MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE COSTA RICA

2023 - 2027

RESUMEN EJECUTIVO

La transformación digital que se está viviendo a nivel global es un poderoso facilitador de un desarrollo sostenible e inclusivo, pero también puede presentar una nueva fuente de riesgos si la infraestructura subyacente y los servicios que dependen de ella no son seguros ni están protegidos frente a las amenazas cibernéticas que pueden traer graves consecuencias de tipo económico y social. Situación que los gobiernos alrededor del mundo han venido atendiendo de varias maneras, una de ellas mediante la formulación e implementación de políticas o estrategias nacionales de ciberseguridad.

El Gobierno de Costa Rica formuló su Estrategia Nacional de Ciberseguridad 2017-2021 permitiendo crear una institucionalidad que ha adelantado sus funciones y actividades en cabeza del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR). Si bien esta estrategia también ha permitido un avance significativo en asuntos de cooperación, de educación y de socialización frente al uso seguro de las Tecnologías de la Información y las Comunicaciones (TIC), es importante reforzar los esfuerzos para cerrar brechas en capacidades de ciberseguridad con el fin de que las múltiples partes interesadas aprovechen las oportunidades actuales y futuras que ofrece la Cuarta Revolución Industrial.

Durante el año 2022, el país experimentó ciberataques de índole extorsivo de gran escala contra un conjunto de instituciones públicas afectando la estructura de sistemas de información mediante el uso de ransomware. Esta experiencia junto con el incremento de nuevas amenazas y riesgos de ciberseguridad ha generado impactos en la economía digital, así como en la seguridad y defensa nacional, por lo que el Gobierno nacional ha decidido replantear su posición frente a la ciberseguridad en todos los niveles.

La nueva Estrategia Nacional de Ciberseguridad 2023-2027 articula una visión estratégica bajo un modelo institucional eficiente robusteciendo el liderazgo del Gobierno nacional y la vinculación de todas las partes interesadas bajo un enfoque de derechos humanos y en línea con la construcción de una sociedad incluyente en todos los ámbitos de la vida costarricense.

Esta estrategia cuenta con un plan de acción para reforzar la gobernanza de ciberseguridad, adecuar el marco normativo jurídico cibernético, mejorar la protección de infraestructuras y la ciber resiliencia nacional, fortalecer el ecosistema de ciberseguridad y cooperar activamente en el entorno digital. Estos documentos han sido elaborado y concertados con el ecosistema de ciberseguridad y están articulados estratégicamente con otros instrumentos de política vigentes con el fin de que el país alcance los objetivos establecidos en el Plan Nacional de Desarrollo e Inversión Pública 2023-2026, en la Política Nacional para la Igualdad efectiva entre mujeres y hombres 2018-2030, en el Plan Nacional de Ciencia, Tecnología e Innovación 2022-2027 y en la Estrategia Nacional de Transformación Digital 2023-2027.

Para aprovechar los actuales beneficios que brinda la tecnología y gestionar los desafíos a los que conlleva la digitalización y la transformación digital del país bajo una visión holística y una atención multisectorial, 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 y agradece el apoyo técnico especializado del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE).

TABLA DE CONTENIDO

LISTA DE GRÁFICAS

LISTA DE CUADROS

SIGLAS Y ACRÓNIMOS

APC	Association for Progressive Communications
BID	Banco Interamericano de Desarrollo
CGI	Global Cybersecurity Index
CGR	Contraloría General de la República
CISTE	Consejo Interinstitucional sobre Terrorismo
CMM	Cybersecurity Capacity Maturity Model for Nations
CNE	Comisión Nacional de Prevención de Riesgos y Atención de Emergencias
CNSL	Comisión Nacional de Seguridad en Línea
CSIRT	Centro de Respuesta de Incidentes de Seguridad Informática
CSIRT-CR	Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica
Cyber4Dev	Cyber Resilience for Development
DIS	Dirección de Inteligencia y Seguridad
FNE	Fondo Nacional de Emergencias
GFCE	Global Forum on Cybersecurity Expertise
GPD	Global Partners Digital
INAMU	Instituto Nacional de la Mujer de Costa Rica
INTERPOL	International Criminal Police Organization
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
MCJ	Ministerio de Cultura y Juventud
MCM	Ministerio de la Condición de la Mujer
MDHIS	Ministerio de Desarrollo Humano e Inclusión Social
MEIC	Ministerio de Economía, Industria y Comercio
MEP	Ministerio de Educación Pública
MH	Ministerio de Hacienda
MNA	Ministerio de la Niñez y Adolescencia
MP	Ministerio de la Presidencia
MTSS	Ministerio de Trabajo y Seguridad Social
MREC	Ministerio de Relaciones Exteriores y Culto
NCSI	National Cyber Security Index
OEA	Organización de Estados Americanos
OEA/CICTE	Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos
OIJ	Organismo de Investigación Judicial
PICTTI	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
PNDIP	Plan Nacional de Desarrollo e Inversión Pública 2023-2026
SOC	Centro de Operaciones de Seguridad
SUTEL	Superintendencia de Telecomunicaciones
TIC	Tecnologías de la Información y las Comunicaciones
UEI	Unidad Especial de Intervención
UIT	Unión Internacional de Telecomunicaciones
UNIDIR	United Nations Institute for Disarmament Research
WEF	World Economic Forum

1. CONTEXTO ACTUAL DE CIBERSEGURIDAD

La pandemia de COVID-19 y la postpandemia han generado un fuerte impacto en la economía global, apresurados procesos de digitalización y transformación digital[1], una expansión del panorama de amenazas y riesgos y un cambio importante en la forma de trabajar en las organizaciones. Además, hay un envejecimiento de la población, existen grandes problemas debidos al alto desempleo y se ha presentado una reversión en el progreso de paridad de género[2] (OEA, 2023). Bajo este escenario, la ciberseguridad se ha convertido en una prioridad y es esencial para garantizar la seguridad y la estabilidad económica.

Este panorama de amenazas[3] y riesgos está en constante expansión[4] debido a una serie de factores, como la creciente interconectividad, la alta complejidad de las nuevas tecnologías y el aumento de la sofisticación de los actores malignos[5]. La adopción de tecnologías emergentes[6] ha conducido a una serie de riesgos de ciberseguridad, que incluyen nuevos vectores de ataque y dificulta la implementación y el mantenimiento de controles de seguridad.

El ransomware, el phishing, las estafas en línea y la intrusión informática (es decir, la piratería) son las tendencias de ciberdelincuencia que perciben los países con mayor frecuencia como amenazas “altas” o “muy altas” a nivel mundial (INTERPOL, 2022), conllevando a la indisponibilidad de servicios ofrecidos virtualmente, el robo de información, o incluso la afectación a servicios esenciales generando consecuencias negativas en el bienestar económico de la ciudadanía[7] o en el eficaz funcionamiento de las organizaciones privadas o públicas.

El costo de recuperarse de un ciberataque, basado en factores como tiempo de inactividad, costos de red, horas de trabajo, oportunidades perdidas y más, es cada vez más alto. Por ejemplo, el costo total promedio global de una violación de datos alcanzó los US$4,5 millones de dólares en 2023, mientras que este costo promedio para la región Latinoamérica alcanzó los US$2,8 millones de dólares (IBM, 2023).

Los eventos geopolíticos recientes también han influido significativamente en la estrategia cibernética y las operaciones tácticas de ciberseguridad en todo el mundo. Se están realizando esfuerzos para fortalecer las políticas y procesos internos, así como para aumentar la efectividad de los controles de ciberseguridad con terceros. Estas tensiones

[1] La transformación digital está llamada a ser una fuerza que potencie el ejercicio de los derechos y responsabilidades ciudadanas, y acelere la productividad, la competitividad y el desarrollo socioeconómico (MICITT, 2023).
[2] Según el Foro Económico Mundial, la brecha global de género en 2023 está cerrada en un 68,6% y se necesitarán otros 131 años para cerrar la brecha global de género y 53 años en América Latina y el Caribe (WEF, 2023a).
[3] Las ocho amenazas más frecuentes a la ciberseguridad actualmente son: ransomware, malware, ingeniería social, amenazas contra los datos, amenazas contra la disponibilidad - denegación de servicio, amenazas contra la disponibilidad - amenazas contra internet, desinformación/mal uso de la información y ataques a la cadena de suministro (PARLAMENTO EUROPEO, 2023).
[4] América Latina y el Caribe sufrió más de 360 mil millones de intentos de ciberataques en 2022, según datos del laboratorio de análisis e inteligencia de amenazas de FORTINET. México recibió la mayor cantidad de intentos de ataques (187 mil millones), seguido de Brasil (103 mil millones), Colombia (20 mil millones) y Perú (15 mil millones) (FORTINET, 2023).
[5] Los ataques de ransomware y extorsión continúan creciendo con nuevos intentos de comprometer las cadenas de suministro de Tecnologías de la información. Los grupos de ransomware se están volviendo más sofisticados y los ataques se están volviendo más específicos, y ciertas industrias e infraestructuras críticas están particularmente en riesgo.
[6] (MCKINSEY, 2023) presenta las tendencias tecnológicas más significativas en 2023.
[7] La Explotación y el Abuso Sexual Infantil en Línea se clasificó entre las diez principales tendencias delictivas percibidas como una amenaza 'alta' o 'muy alta' por los países miembros y el 62 por ciento de los países miembros esperaban firmemente que estos delitos 'aumentaran' o 'aumentar significativamente' en el futuro (INTERPOL, 2022).

geopolíticas han sido responsables de una mayor volatilidad en el carácter de las ciberamenazas, con una mayor variación en los tipos de malware ampliamente disponibles, así como cambios en el tipo de activos o procesos de creación de valor a los que apuntan los ciberatacantes (WEF, 2023b).

Los gobiernos alrededor del mundo trabajan juntos para desarrollar y ejecutar estrategias nacionales de ciberseguridad efectivas, invirtiendo en nuevas tecnologías para mejorar su defensa cibernética, como inteligencia artificial, aprendizaje automático y blockchain. De igual manera, están trabajando para educar, formar y concientizar a la sociedad sobre los riesgos de ciberseguridad, así como para proporcionarle las herramientas y recursos que necesita para protegerse.

Los procesos de formulación de este tipo de estrategias nacionales están incorporando nuevas temáticas asociadas a las nuevas condiciones y tendencias de ciberseguridad a nivel internacional, tales como la ciber diplomacia y seguridad internacional, la seguridad de la cadena de suministro, la seguridad en la nube, la seguridad por diseño y por defecto, la adopción segura de tecnologías emergentes y el desarrollo de fuerza laboral de ciberseguridad bajo enfoques de derechos humanos y de igualdad de género, diversidad e inclusión social [8] [9].

Finalmente, las organizaciones abordan prioridades clave como la creación de ecosistemas receptivos que mejoran la preparación organizacional, la reestructuración de puntos de acercamiento a soluciones y mayor cobertura de ataques, las prácticas de reequilibrio para centrarse en las personas, los procesos y la tecnología y el diseño de programas de ciberseguridad sostenibles y equilibrados (GARTNER, 2023).

2. MARCO NORMATIVO

Costa Rica cuenta con un marco jurídico y reglamentario para proteger a la sociedad contra la ciberdelincuencia y promover un entorno cibernético seguro, de conformidad con los principios de inclusión y de entorno de confianza.

El país ha suscrito convenios y tratados internacionales asumiendo varios compromisos internacionales que tienen relación con la ciberseguridad, por ejemplo instrumentos: i) para proteger y garantizar los derechos humanos, en especial los derechos humanos básicos que deben disfrutar los niños, las niñas y adolescentes, ii) para eliminar la discriminación contra la mujer, iii) para prevenir, sancionar y erradicar toda forma de violencia contra la mujer, iv) para impulsar el desarrollo sostenible, v) para desarrollar legislación nacional integral sobre ciberdelitos, vi) para combatir la impunidad de quienes han cometido crímenes de extrema gravedad, vi) para prevenir y combatir más eficazmente la delincuencia organizada transnacional, entre otros.

También ha formalizado instrumentos jurídicos de cooperación en asuntos de ciberseguridad con organismos internacionales (transcontinentales / regionales),

[8] Se resaltan los aportes realizados a estos temáticas de organizaciones internacionales como United Nations Institute for Disarmament Research (UNIDIR, 2023), Association for Progressive Communications (APC, 2023), Global Partners Digital (GPD, 2023), Global Forum on Cybersecurity Expertise (GFCE, 2023), Chatham House (CHATHAM HOUSE, 2023) y organizaciones nacionales como la Cooperativa Sulá Batsú.

[9] El Programa de Ciberseguridad de OEA/CICTE adelanta, con el apoyo del Gobierno de Canadá, el proyecto "*Cerrando la Brecha de Género en la Agenda de Ciberseguridad de las Américas y el Caribe 2022-2026*" promoviendo la incorporación de perspectiva de género y diversidad en las políticas / estrategia nacionales de ciberseguridad en la región.

organismos multilaterales de desarrollo, y con otros Estados independientes y jurídicamente iguales.

Cuadro 1. Principales instrumentos internacionales relacionado con la Estrategia Nacional de Ciberseguridad 2023-2027

Compromisos Internacionales	Agenda para el Desarrollo Sostenible	Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) y Segundo Protocolo Adicional	Estatuto de Roma	Acuerdo de Asociación Unión Europea - Centroamérica	Declaraciones y Resoluciones del OEA/CICTE	Otros acuerdos multilaterales y bilaterales en la materia
	Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo)	Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer	Agenda Mujeres, Paz y Seguridad y sus resoluciones	Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer	Convención de las Naciones Unidas sobre los Derechos del Niño	Pacto Internacional de Derechos Civiles y Políticos

Fuente: Elaboración propia (2023) tomando en cuenta (APC, 2022)

En relación con la lucha contra el ciberdelito, una vez promulgada la Ley No. 9452 en donde la Asamblea Legislativa aprueba su adhesión, Costa Rica firmó el 22 de septiembre de 2017 el acceso al Convenio sobre Ciberdelincuencia (Convenio de Budapest), el cual entró en vigor desde el 1 de enero de 2018[10]. En el mismo año 2018, Costa Rica fue elegido beneficiario del Programa GLACY+, una iniciativa de apoyo del Consejo de Europa para la implementación del Convenio. Esto refleja el compromiso del país para fortalecer su capacidad en la prevención y combate de delitos informáticos, mejorar la cooperación internacional en este ámbito y proteger a la ciudadanía en el entorno digital. Adicionalmente, el 13 de junio de 2022, Costa Rica firmó el Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest) destinado a mejorar la cooperación y la divulgación de pruebas electrónicas.

Costa Rica también cuenta con un marco constitucional, legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes. Por una parte, algunos fundamentos constitucionales en torno a la ciberseguridad se encuentran en la Constitución de la República de Costa Rica resaltando aquellos relacionados con los derechos y garantías individuales y sociales, el orden, defensa y seguridad del país, y la soberanía.

Por otra parte, se destaca la legislación expedida en el país en torno a: i) la promoción del desarrollo científico y tecnológico, ii) la protección y privacidad de datos personales, iii) la protección infantil en línea, iv) la promoción de la igualdad social de la mujer, v) la defensa del consumidor, vi) la intervención legal de las comunicaciones, vii) la adopción de certificados, firmas digitales y documentos electrónicos, entre otros. Respecto a la legislación integral a nivel de derecho sustantivo y de derecho procesal frente a la cibercriminalidad, se destaca la promulgación de varias leyes que reforman y adicionan varios delitos informáticos y conexos a la legislación penal costarricense.

[10] Costa Rica presentó dos (2) observaciones interpretativas sobre los artículos 10 y 24 del Convenio sobre Ciberdelincuencia (Convenio de Budapest).

Cuadro 2. Marco constitucional y legal relacionado con la Estrategia Nacional de Ciberseguridad 2023-2027

Marco constitucional y legal	Constitución Política de 1949	Ley 4573 Código Penal	Ley 6683 de Derechos de Autor y Derechos Conexos	Ley 7142 de Promoción de la Igualdad Social de la Mujer	Ley 7169 de Promoción del Desarrollo Científico y Tecnológico	Ley 7425 sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones
	Ley 7472 de Promoción de la Competencia y Defensa Efectiva del Consumidor	Ley 7594 Código Procesal Penal	Ley 7975 de Información no divulgada	Ley 8039 de Procedimientos de Observancia de los Derechos de Propiedad Intelectual	Ley 8148 para reprimir y sancionar los delitos informáticos	Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos
	Ley 8488 de Emergencias y Prevención del Riesgo	Ley 8642 Ley General de Telecomunicaciones	Ley 8660 de Fortalecimiento y Modernización de Entidades Públicas del sector de Telecomunicaciones	Ley 8719 de Fortalecimiento de la Legislación contra el Terrorismo	Ley 8934 de Protección de la Niñez y Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos	Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales
	Ley 9048 sobre Delitos Informáticos y Conexos	Ley 9135 que reforma y adiciona delitos informáticos	Ley 9162 sobre Expediente Digital Único en Salud	Ley 9452 adhiere al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001)	Ley 9738 para regular el teletrabajo	Ley 9975 de Penalización de la Violencia Contra las Mujeres
	Ley 10235 para prevenir, atender, sancionar y erradicar la violencia contra las mujeres en la política	Ley 10238 de protección de la imagen, la voz y los datos personales de las personas menores de edad				

Fuente: Elaboración propia (2023) tomando en cuenta (SULA BATSU & GPD, 2023)

Frente al marco normativo relacionado con ciberseguridad se destaca aquella en donde se otorga al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) la rectoría en temas de ciencia, tecnología, telecomunicaciones y gobernanza digital en el país, se establecen normas técnicas y se crean varias instancias que abordan temas relacionados como el Consejo Interinstitucional sobre Terrorismo (CISTE), la Comisión Nacional de Seguridad en Línea (CNSL) y el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) bajo el MICITT[11].

Cuadro 3. Marco normativo relacionado con la Estrategia Nacional de Ciberseguridad 2023-2027

Marco Normativo	Decreto 31659-MP-RE Creación de la Comisión Interinstitucional	Decreto 33018-MICIT Reglamento a la Ley de Certificados,	Decreto 36274-MICIT Creación de la Comisión Nacional de	Decreto 37052-MICIT Creación del CSIRT-CR	Decreto 37554-JP Reglamento a la Ley de	Decreto 40199-MP Apertura de Datos Públicos

[11] El Decreto Nº 37052-MICIT crea el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) 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 ciberseguridad e informática que afecten a las instituciones gubernamentales

sobre Terrorismo (CISTE)	Firmas Digitales y Documentos Electrónicos	Seguridad en Línea (CNSL)		Protección de la Persona frente al Tratamiento de sus Datos Personales	
Decreto 40546 - RREE Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001)	Decreto 41187-MP-MIDEPLAN Reglamento Orgánico del Poder Ejecutivo	Decreto 43542-MP-MICITT Estado de Emergencia debido a los cibercrímenes de 2022	Directriz 133-MP-MICITT Recomendaciones y medidas técnicas de MICITT y CSIRT-CR	Código Nacional de Tecnologías Digitales	Normas técnicas para el gobierno y gestión de las tecnologías de la información

Fuente: Elaboración propia (2023)

Finalmente, el Gobierno ha emitido directrices que imparten instrucciones a las entidades de la Administración Pública Central para reportar incidentes de ciberseguridad al CSIRT-CR y para promover la implementación de medidas y mecanismos de seguridad.

3. DIAGNÓSTICO

Costa Rica ha vivido una profunda transformación digital durante la última década. Según la Superintendencia de Telecomunicaciones (SUTEL), Internet se ha convertido en un servicio esencial para los consumidores tanto a través de redes fijas como móviles. El aumento ha sido significativo tanto en la cantidad de usuarios como en las velocidades y el volumen de tráfico de la información (SUTEL, 2023).

Cuadro 4. Evolución en suscriptores y tráfico de telefonía móvil y fija en Costa Rica

		2019	2020	2021	2022
Telefonía móvil	Suscriptores de Telefonía Móvil / 100 habitantes	145%	147%	152%	151%
	Suscriptores de Acceso a Internet Móvil / 100 habitantes	92%	93%	95%	96%
	Tráfico, acceso a Internet en la red móvil (miles de TB)	160	223	269	332
Telefonía fija	Suscriptores de Telefonía Fija / 100 habitantes	13%	11%	10%	9%
	Suscriptores de Acceso a Internet Fijo / 100 habitantes	18%	19.4%	20.5%	21.2%
	Tráfico, acceso a Internet en la red fija (miles de TB)	1162	2212	3280	3557

Fuente: (SUTEL, 2023)

En el país, la evolución del entorno digital ha traído consigo un aumento en la participación de la sociedad en actividades económicas y sociales soportadas en las Tecnologías de la Información y las Comunicaciones (TIC), generando mayor inclusión de la población, reduciendo barreras, aumentos en productividad y competitividad y, por tanto, crecimiento económico. No obstante, la mayor presencia de la sociedad costarricense en el entorno digital ha generado mayores riesgos e incertidumbres durante los últimos años. Consiente de esta situación, el Gobierno de Costa Rica expidió la Estrategia Nacional de Ciberseguridad 2017-2021.

3.1. Implementación de la Estrategia Nacional de Ciberseguridad 2017-2021

Costa Rica ha llevado un proceso y ejecución de acciones, para mejorar la ciberseguridad nacional contribuyendo a cerrar brechas digitales[12], lo cual llevó al país en el año 2017 a

[12] En particular, el MICITT ha documentado la persistencia de una brecha de género digital de acceso, uso y profesionalización que debe abordarse a través de la articulación de políticas públicas, agendas de gobierno, planes de acción e intervenciones diversas (MICITT, 2017). Durante el periodo de implementación de la Estrategia Nacional de Ciberseguridad 2017-2021, Costa Rica avanzó en la reducción de su brecha digital, de acuerdo con el Índice de Brecha Digital (IBD) 2016-2018 del MICITT (MICITT, 2019).

establecer un norte común, desarrollando su Estrategia Nacional de Ciberseguridad 2017-2021. El objetivo general de esta estrategia nacional era desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.

Para lograr dicho objetivo, se implementarían acciones en torno a ocho (8) ejes de trabajo: i) coordinación nacional, ii) conciencia pública, iii) capacidades, iv) marco jurídico, v) infraestructuras críticas, vi) gestión del riesgo, vii) cooperación internacional, y viii) implementación, seguimiento y evaluación.

Teniendo en cuenta las condiciones particulares para el periodo de formulación e implementación, el país logró avances en la materia. El MICITT se consolidó como la entidad líder en ciberseguridad a nivel nacional. Se creó y consolidó al CSIRT-CR como una instancia líder de los temas de ciberseguridad y coordinador del resto de organismos del país como institución responsable de la mejora de las capacidades de las instituciones. Se articularon esfuerzos con la Comisión Nacional de Seguridad en Línea (CNSL). Se implementaron algunas iniciativas de intercambio de buenas prácticas e información, capacitaciones y programas de estudio. Se ejecutaron valiosas iniciativas de capacitaciones centradas en buenas prácticas de higiene digital y ciberseguridad para menores y adolescentes y algunas campañas de concienciación consolidando una cultura de ciberseguridad en el país. Se adelantaron diversos proyectos de colaboración por una parte mediante algunas alianzas público-privadas y por otra con socios internacionales en distintas áreas distintivas de ciberseguridad, demostrando el compromiso de cooperación internacional del país.

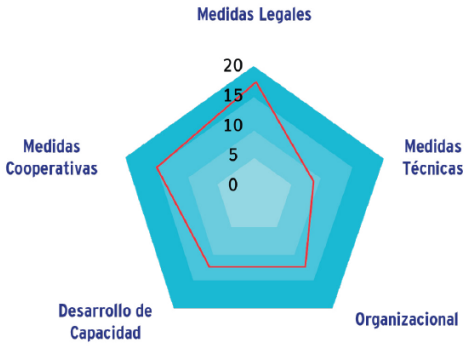
Estos avances lograron posicionar al país mejorando varios aspectos en relación con la madurez de capacidades de ciberseguridad. La medición para el año 2020 del *Global Cybersecurity Index (CGI)*[13] de la Unión Internacional de Telecomunicaciones (UIT) situó a Costa Rica en la posición 76 a nivel global mejorando 39 lugares respecto de la medición del 2018. Los reportes sobre el estado de la ciberseguridad en la región América Latina y el Caribe de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) aplicando el Modelo de Madurez de Capacidades de Seguridad Cibernética[14] también reflejaron mejoras del país entre las mediciones del 2016 y del 2020 (OEA & BID, 2020), especialmente frente a los marcos legales y regulatorios y a los marcos de capacitación profesional.

Gráfica 1. Costa Rica en mediciones internacionales de capacidades de ciberseguridad

Mediciones CMM de OEA & BID (2016 y 2020) **Mediciones GCI de UIT (2020)**

[13] El Global Cybersecurity Index (GCI) es un referente de confianza que mide el compromiso de los países con la ciberseguridad a nivel global (UIT, 2023).

[14] El Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM, por sus siglas en inglés, Cybersecurity Capacity Maturity Model for Nations) es un marco metódico diseñado por el Centro de Capacidad de Seguridad Cibernética Global del Departamento de Ciencias de la Computación de la Universidad de Oxford para revisar la capacidad de ciberseguridad de un país (GCSCC, 2023).



Fuente: Elaboración propia a partir de (OEA & BID, 2020) y (UIT, 2023)

Una vez completado el periodo establecido para la implementación de la Estrategia Nacional de Ciberseguridad 2017-2021, se adelantó una revisión de esta, bajo el liderazgo del MICITT y con el apoyo técnico especializado del Programa de Ciberseguridad de OEA/CICTE y del proyecto Cyber Resilience for Development (Cyber4Dev) de la Unión Europea. Los resultados de la revisión se plasmaron en un reporte (MICITT, 2021) que presenta un análisis situacional por cada uno de los objetivos establecidos junto con unas recomendaciones (ver Anexo 1) respecto de implementar medidas organizacionales, jurídicas, técnicas, de fortalecimiento de capacidades y de cooperación para mejorar las capacidades del país.

3.2. Desafíos recientes a nivel nacional

En el 2022, el Gobierno de Costa Rica experimentó ciberataques de índole extorsivo de gran escala contra un conjunto de instituciones públicas afectando la estructura de los sistemas de información mediante el uso de ransomware. Algunos daños identificados fueron la pérdida de operatividad de los sistemas informáticos, el robo de información y la fuga de datos.

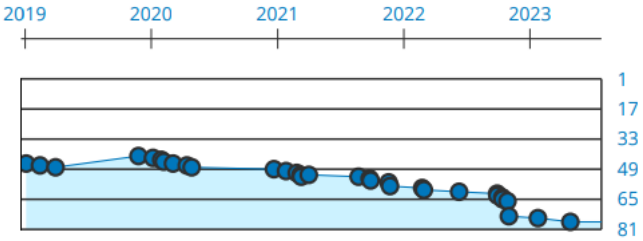
Como medida de respuesta, el Gobierno nacional emitió el Decreto Ejecutivo No. 43542-MP-MICITT de 2022, donde se declaró Estado de Emergencia Nacional en todo el sector público del Estado costarricense y rápidamente reconoció el valor de la cooperación internacional para abordar el desafío. Esta situación derivó en la elaboración de un Plan General de la Emergencia (CNE, 2022) facilitando la disponibilidad de recursos y los actos administrativos necesarios para su atención. En este plan se establece que el costo de respuesta estimado para atender los ciberataques ascendió a ₡15.949 millones, de los cuales ₡11.158 millones corresponden a recursos propios de las instituciones y ₡4.791 millones aportados por el Fondo Nacional de Emergencias (FNE).

Según la Contraloría General de la República (CGR, 2023), los ciberataques afectaron las labores ordinarias de al menos 45.535 personas funcionarias, afectando 49 tipos de trámites y servicios; y provocando pérdida de ingresos institucionales; así como la pérdida de información, o bien, su calidad o disponibilidad, lo cual incidió en la toma de decisiones, la transparencia y la rendición de cuentas. La CGR analizó las implicaciones y los costos de los ciberataques para la Hacienda Pública y la sociedad en general y presentó recomendaciones (ver Anexo 2) tanto al poder ejecutivo como al poder legislativo en el país,

respecto de la necesidad de implementar medidas organizacionales, jurídicas, técnicas, de fortalecimiento de capacidades y de cooperación.

De esta forma, estos ciberataques han influido significativamente en la forma en que el Gobierno ve la ciberseguridad y la gestión de riesgos en organizaciones tanto públicas como privadas. Al considerar el importante impacto socioeconómico que pueden tener incidentes de ciberseguridad como estos, existe una voluntad al más alto nivel de invertir el capital político, el tiempo, el dinero y los recursos para tener un ciberespacio más seguro para la ciudadanía costarricense. Sin embargo, esta voluntad debe sopesarse con la realidad de la reducida capacidad de seguridad cibernética que existe a nivel nacional y que debe abordarse. Por ejemplo, en el *National Cyber Security Index (NCSI)*, Costa Rica pasa del puesto 42 a nivel mundial en 2020 al puesto 77 en 2023, es decir, pierde 35 puestos.

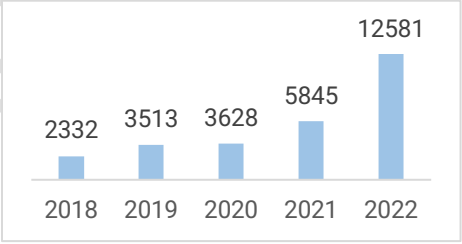
Gráfica 2. Evolución de la medición del *National Cyber Security Index (NCSI)* del e-Governance Academy de Estonia para Costa Rica



Fuente: (e-Governance Academy, 2023)

Las condiciones para desarrollar actividades socioeconómicas en el país cambiaron drásticamente después de los ciberataques del año 2022. El incremento de amenazas y riesgos de ciberseguridad digitales ha generado impactos en el Estado, en la economía y en la sociedad que deben ser abordados bajo una nueva estrategia nacional que integre una nueva visión estratégica con nuevos enfoques acogiendo buenas prácticas internacionales.

Gráfica 3. Evolución de las denuncias de delitos informáticos en Costa Rica



Fuente: (SEMINARIO UNIVERSIDAD, 2023) & (LA NACION, 2023)

Durante los años 2022 y 2023, MICITT y CSIRT-CR continúan ejerciendo la coordinación y liderando iniciativas nacionales de ciberseguridad haciendo esfuerzos significativos bajo un marco dinámico de cooperación a nivel nacional con otras ramas del poder público y a nivel internacional, con el fin de mejorar las capacidades de ciberseguridad de las instituciones de la Administración Pública Central y del resto de partes interesadas en el país.

4. MARCO ESTRATÉGICO

La Estrategia Nacional de Ciberseguridad 2023-2027[15] proporciona una visión cohesiva y convincente construida con todas las múltiples partes interesadas, incluidos los sectores público y privado, las organizaciones de la sociedad civil, la academia y la comunidad en general, abordando las necesidades y los desafíos únicos de la ciudadanía costarricense, promoviendo la igualdad de oportunidades y la participación inclusiva en las iniciativas de ciberseguridad.

También el gobierno construye sobre los logros, objetivos y criterios de la Estrategia Nacional de Ciberseguridad 2017-2021 y de las experiencias atendidas durante los años 2022 y 2023. Las instituciones e iniciativas desarrolladas durante los últimos años han ayudado a establecer en Costa Rica unas importantes capacidades de ciberseguridad que son necesarias potenciar.

Para mitigar las múltiples amenazas y proteger los intereses de Costa Rica en el ciberespacio, se necesita un enfoque estratégico que guíe todas las acciones colectivas e individuales en el ámbito digital durante los próximos cuatro años. Esta sección establece el marco estratégico, teniendo en cuenta las diversas perspectivas y experiencias de la ciudadanía costarricense para garantizar una estrategia de ciberseguridad integral y equitativa.

4.1. Alineación estratégica

La Estrategia Nacional de Ciberseguridad 2023-2027 está alineada estratégicamente con varios instrumentos de política pública y de planificación nacional. Por una parte, con el marco estratégico relacionado con los sectores de ciencia, innovación, tecnología y telecomunicaciones que hace énfasis en el desarrollo de la sociedad y economía costarricense. Por otra parte, con el marco estratégico que promueve el cese de toda desigualdad y la integración de una perspectiva de género en el quehacer de las instituciones públicas para la construcción de una sociedad incluyente en todos los ámbitos de la vida costarricense[16].

Cuadro 5. Políticas, Planes y Estrategias nacionales relacionados con la Estrategia Nacional de Ciberseguridad 2023-2027

Políticas Públicas	Política Nacional de Sociedad y Economía Basada en el Conocimiento 2022-2050	Política Nacional para la Igualdad efectiva entre mujeres y hombres (PIEG) 2018-2030	Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de la Ciencia, la Tecnología, las Telecomunicaciones	Política Nacional para una sociedad libre de racismo, discriminación racial y xenofobia 2014-2025	Política Nacional para la atención, prevención y protección de la violencia contra las mujeres de todas las edades (PLANOVI) 2017-2032	Política Nacional de Gestión del Riesgo 2016-2030

[15] La Estrategia Nacional de Ciberseguridad 2023-2027 tiene en cuenta los lineamientos de planificación nacional establecidos en los siguientes documentos estratégicos: i) Lineamientos para incorporar la Planificación Prospectiva Estratégica en el Sistema Nacional de Planificación (SNP) (MIDEPLAN, 2023b), ii) Guía de la Teoría de la Intervención (MIDEPLAN, 2018a), iii) Guía de Indicadores - Orientaciones básicas para su elaboración (MIDEPLAN, 2018b), iv) Guía sobre el enfoque de igualdad de género y derechos humanos (MIDEPLAN, 2017b), v) Política Nacional para la atención, prevención y protección de la violencia contra las mujeres de todas las edades (PLANOVI) 2017-2032 (INAMU, 2018) y vi) Manual de Planificación con Enfoque para Resultados en el Desarrollo – Marco Teórico y Práctico (MIDEPLAN, 2016).

[16] En concordancia con los desafíos a nivel nacional en relación con la prevención y atención de aquellos riesgos en línea que enfrentan menores de edad, personas y grupos históricamente discriminados y que viven en condiciones de vulnerabilidad, así como la violencia de género en línea que afecta a mujeres con identidades múltiples y a miembros de la comunidad LGBTI (Lesbianas, Gays, Bisexuales, Transexuales y de género diverso e Intersexuales), cuya incidencia tuvo un aumento considerable en toda Latinoamérica a partir del acelerado uso de las tecnologías digitales ante la pandemia del COVID-19 (OEA, 2021) (OEA & ONU Mujeres, 2021) (CEPAL, 2022).

	y la Innovación (PICTTI) 2018-2027			
Planes	Plan Nacional de Desarrollo e Inversión Pública (PNDIP) 2023-2026	Plan Nacional de Ciencia, Tecnología e Innovación (PNCTI) 2022-2027	Plan Nacional Desarrollo de las Telecomunicaciones (PNT) 2022-2027	Ruta de la Educación 2022-2026
Estrategias	Estrategia Nacional de Transformación Digital[17] 2023-2027 *	Estrategia Nacional para la Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea 2021-2027	Estrategia nacional para el combate del acoso y hostigamiento sexual contra las mujeres 2022-2026	

Nota: * Documento bajo Consulta Pública no vinculante durante el mes de junio de 2023[18]
Fuente: Elaboración propia (2023)

La Estrategia Nacional de Ciberseguridad 2023-2027 incluirá intervenciones públicas con el fin de que se alcancen objetivos establecidos en el *Plan Nacional de Desarrollo e Inversión Pública (PNDIP) 2023-2026* (MIDEPLAN, 2023a) que tienen relación con la ciberseguridad como, por ejemplo, la meta de 25.938 personas que participen en espacios de fomento de la ciberseguridad[19] entre 2023 y 2026 así como la meta de 40 actividades de diplomacia de seguridad y desarme[20] a implementarse en el mismo periodo.

De igual manera, intervenciones públicas para apoyar la creación de ciberespacios seguros que reduzcan los factores de riesgo y la condición de vulnerabilidad de ciertos grupos de mujeres, en particular las capacitaciones para la atención y prevención de la violencia de género, riesgo y vulnerabilidad digital al personal de la sección de delitos informáticos, meta establecida en la *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 (PICTTI) 2018-2027* (MIDEPLAN, 2017a).

4.2. Enfoques rectores

La Estrategia Nacional de Ciberseguridad 2023-2027 se formula para ser implementada bajo enfoques estratégicos nacionales que fundamentan el accionar de las actuaciones que se realicen y ayuden a guiar la toma de decisiones:

[17] En la Estrategia Nacional de Transformación Digital 2023-2027 establece a la *Ciberseguridad* como un pilar para el desarrollo de *Gobierno Digital*.
[18] Ver https://www.micitt.go.cr/consultas-publicas/
[19] El PNDIP 2023-2026 define Espacios de Fomento de la Ciberseguridad como *"espacios actividades como eventos, webinars, charlas, cursos o talleres"*. También define Fomento de ciberseguridad como temas *"que van desde cultura informática en ciberseguridad, alfabetización digital, consejos, buenas prácticas, vida en línea, incluyendo acciones especializadas en temas de incidentes, respuestas, redes, desarrollo de software, analítica y aspectos legales."* (subrayado fuera de texto)
[20] El PNDIP 2023-2026 define actividades de diplomacia de seguridad y desarme como *"actividades implementadas se refiere a las actividades realizadas en coordinación con los entes rectores, las misiones diplomáticas, organismos internacionales y sociedad civil organizada, en las áreas de: Desarme, desarme nuclear, comercio de armas, seguridad, lucha contra el crimen organizado, lucha contra el narcotráfico, lucha contra la corrupción, lucha contra el terrorismo, uso nuclear para fines pacíficos, ciberdelito, ciberseguridad, paz, prevención de conflictos, entre otros."* (subrayado fuera de texto)

- **Enfoque de Toda la Sociedad** en donde se propende por la coordinación efectiva entre actores estatales y no estatales tales como proveedores de servicios esenciales, proveedores de servicios de internet, ecosistema digital, academia, organizaciones de la sociedad civil, etc.

- **Enfoque de Gestión y Mitigación de Riesgos** en donde se reconoce la necesidad de garantizar que las medidas adoptadas aborden o mantengan las amenazas a medida que evolucionan y aseguran que haya una fuerza laboral adecuada y capacitada con agilidad para responder.

- **Enfoque de Derechos Humanos**[21] en donde se pone a las personas en Costa Rica en el centro y se garantiza el ejercicio pleno de los derechos de las personas, demostrando que los resultados de la implementación de las intervenciones públicas de ciberseguridad no van a generar discriminación debido a la diversidad étnica, etaria, sexo, credo religioso, lugar de residencia, condición de discapacidad, entre otros.

- **Enfoque centrado en el ser humano**[22] en donde se abordan los riesgos e impactos diferenciados de las amenazas cibernéticas para que la ciberseguridad responda a necesidades, complejas, diferenciadas e interseccionales de las personas en Costa Rica en función del género, la orientación sexual, la raza, la religión, la etnia, la capacidad, la clase, la nacionalidad, la ruralidad y la afiliación política, entre otros factores.

4.3. Visión

Para 2027, el ecosistema digital de Costa Rica es confiable y contribuye al esfuerzo global para asegurar el ciberespacio, al brindar intercambio de conocimientos y experiencias de una fuerza laboral de ciberseguridad bien desarrollada.

4.4. Misión

Establecer un marco de acción integral que permita prevenir y mitigar los riesgos y amenazas en el entorno digital, fomentar la innovación y el desarrollo de soluciones en ciberseguridad, fortalecer la capacidad de respuesta ante incidentes de ciberseguridad, promover una cultura de seguridad sólida, con el fin ayudar a garantizar la estabilidad del país y su economía, proteger la información personal y crítica del Estado y de la ciudadanía, y mantener la confianza en el uso de los sistemas digitales.

4.5. Principios orientadores

La Estrategia Nacional de Ciberseguridad 2023-2027 aplica los siguientes principios orientadores:

- **Gestión integral de riesgos**. Todas las partes interesadas deben comprender los riesgos de ciberseguridad y evaluar el impacto potencial de sus decisiones de

[21] En línea con el enfoque de Derechos Humanos de la PICTTI 2018-2027 (MIDEPLAN, 2017a)
[22] En línea con el enfoque de Género y Diversidades de la PICTTI 2018-2027 (MIDEPLAN, 2017a)

gestión integral de riesgos de ciberseguridad en sus actividades socio económicas y el entorno digital en general.

- **Respeto a los Derechos Humanos y los valores fundamentales**. Todas las partes interesadas deben gestionar los riesgos de ciberseguridad de forma transparente y coherente con los derechos humanos y los valores fundamentales del Estado costarricense.

- **Responsabilidad compartida.** Todas las partes interesadas deben asumir la responsabilidad de la gestión integral de riesgos de ciberseguridad observando el rol que poseen bajo el marco de gobernanza de ciberseguridad del país.

- **Cooperación.** Todas las partes interesadas deben cooperar, incluso más allá de las fronteras del país, promoviendo un entorno cibernético seguro.

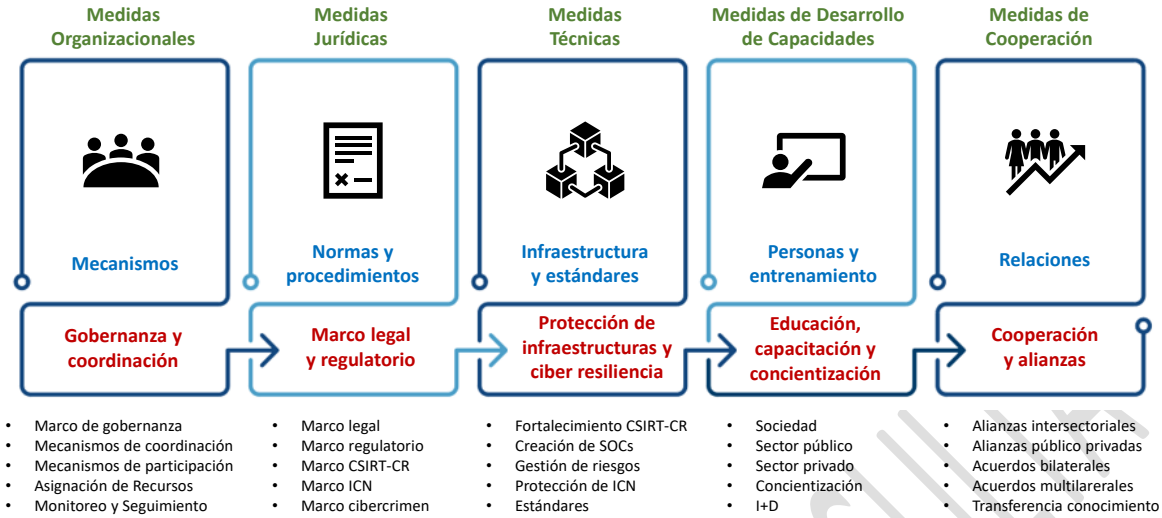
- **Innovación.** Los líderes y tomadores de decisiones que representan a las partes interesadas deben asegurarse de que la innovación sea considerada durante la implementación de iniciativas de ciberseguridad.

4.6. Pilares

La Estrategia Nacional de Ciberseguridad 2023-2027 establece cinco "*acciones prioritarias*" que establecen objetivos estratégicos y se utilizan como pilares del marco estratégico, orientando y organizando las líneas de acción específicas que se tomarán y los resultados que se pretenden lograr para 2027:

- **Pilar 1: Reforzar la gobernanza de ciberseguridad**, optimizando la inversión pública y profundizando en la coordinación entre gobierno, industria, academia, sociedad y comunidad internacional (MAS CIBERCOORDINAD@S)
- **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 (MAS CIBERACTUALIZAD@S)
- **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. (MAS CIBERSEGUR@S)
- **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. (MAS CIBERPREPARAD@S)
- **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. (MAS CIBERINTEGRAD@S)

Gráfica 4. Pilares de la Estrategia Nacional de Ciberseguridad 2023-2027



Fuente: Elaboración propia (2023)

4.7. Objetivo general

Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas.

4.8. Objetivos Específicos y Líneas de Acción

La Estrategia Nacional de Ciberseguridad 2023-2027 establece acciones que se dedican a todos los sectores de la economía y la sociedad, desde las instituciones de la administración pública central hasta los líderes de toda la industria y la ciudadanía, con el fin de alcanzar objetivos estratégicos y el objetivo general. La estrategia busca aumentar la ciberseguridad en todos los niveles para el beneficio colectivo y será la base a partir de la cual participará Costa Rica a nivel internacional para promover un ciberespacio más seguro.

4.8.1. Reforzar la gobernanza de ciberseguridad

Costa Rica establecerá un marco de gobernanza que defina roles, responsabilidades y mecanismos de coordinación, colaboración y comunicación entre entidades gubernamentales, organizaciones del sector privado, academia, organizaciones de la sociedad civil y comunidad internacional. Este pilar se centra en la coordinación general, el liderazgo y los procesos de toma de decisiones en ciberseguridad.

- **Línea de Acción 1.1. Consolidar la instancia de coordinación nacional de ciberseguridad**
    - Establecer y poner en marcha una hoja de ruta para reestructurar el MICITT consolidando y centralizando los esfuerzos y actividades relacionados con la ciberseguridad a nivel nacional
    - Fortalecer la instancia de coordinación nacional para dirigir la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027 y

hacer seguimiento continuo, dotándola de herramientas jurídicas y técnicas que le permitan desempeñar sus funciones con la mayor efectividad
- Asegurar que la instancia de coordinación nacional cuente con un equipo de personal especializado, calificado y técnico dedicado a las acciones de ciberseguridad promoviendo la igualdad de género y la diversidad.

- **Línea de Acción 1.2. Establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad**

  - Diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
  - Renovar la instancia de máximo nivel intergubernamental e intersectorial de planeación estratégica para orientar la gestión de la ciberseguridad en el país, promoviendo la igualdad de género y la diversidad.
  - Crear instancias de planeación táctica para asesorar la implementación de acciones establecidas y priorizadas teniendo en cuenta la cooperación con los líderes tecnológicos y personas expertas en el campo.
  - Crear y poner en marcha mecanismos dinámicos de coordinación, colaboración e intercambio de información intergubernamental e intersectorial vinculando a las múltiples partes interesadas.
  - Crear una figura de enlace (persona responsable de ciberseguridad) en instituciones públicas, en gobiernos locales y en otras organizaciones a nivel operativo.
  - Desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
  - Establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
  - Adelantar evaluaciones de impacto socio económico respecto de la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027.

- **Línea de Acción 1.3. Asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad**

  - Establecer y poner en marcha una hoja de ruta para la transición al cese de estado de emergencia declarado mediante el Decreto Ejecutivo No. 43542-MP-MICITT de 2022.
  - Desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad.

- Reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad.
- Promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad.
- Establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad.
- Promover el diseño de estímulos a la inversión del sector privado para la financiación de proyectos de ciberseguridad.

4.8.2. Adecuar el marco jurídico cibernético

Costa Rica desarrollará legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad. Este pilar asegura la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.

- **Línea de Acción 2.1. Fortalecer el marco legal y regulatorio cibernético**

  - Apoyar a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.
  - Apoyar a los reguladores sectoriales en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco regulatorio relacionado con la ciberseguridad, así como en el ejercicio de supervisión y verificación del cumplimiento de las disposiciones de los marcos regulatorios sectoriales relacionadas con la ciberseguridad.
  - Revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.

- **Línea de Acción 2.2. Fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad**

  - Actualizar el marco normativo para fortalecer los procesos de gestión administrativa y técnica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR).
  - Establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional, incluyendo:
    - Guías para la evaluación de los programas interinstitucionales en materia de seguridad de TIC.
    - Planes de contingencia en materia de seguridad de las TIC en el sector público.
    - Guías para reducir el impacto y la probabilidad de incidentes de ransomware y extorsión de datos en organizaciones públicas y

privadas, incluyendo mejores prácticas internacionales para prepararse, prevenir y mitigar estos incidentes.

- Desarrollar un marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales, adoptando normas y estándares internacionales, incluyendo:
  - Protocolo nacional de gestión y respuesta a crisis y emergencias cibernéticas.
  - Planes de contingencia y recuperación para las infraestructuras críticas nacionales y los servicios esenciales.
  - Manual para adelantar ejercicios y simulacros nacionales de ciberseguridad.
- Impulsar el cumplimiento del marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad.

4.8.3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional

Costa Rica establecerá un marco de gestión integral de riesgos de ciberseguridad que permita la detección, el reporte, el análisis y la respuesta oportuna a incidentes de ciberseguridad. Este pilar se enfoca en desarrollar capacidades para la respuesta a incidentes de ciberseguridad, así como la coordinación y la comunicación efectiva entre las partes interesadas durante las crisis cibernéticas.

- **Línea de Acción 3.1. Adoptar un marco para la gestión integral de riesgos de ciberseguridad**

  - Elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades.
  - Establecer procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos de ciberseguridad adaptándolo a las nuevas amenazas, vulnerabilidades y tendencias en el ámbito de la ciberseguridad.
  - Garantizar que los procesos de gestión de riegos de ciberseguridad y de gestión de riesgos de la seguridad de la información se integren en los procesos de planificación estratégica, operativa, y presupuestaria de las instituciones públicas.

- **Línea de Acción 3.2. Fortalecer las capacidades nacionales de monitoreo, detección y respuesta a incidentes de ciberseguridad**

  - Crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad.
  - Proveer una solución de Centro de Operaciones de Seguridad (SOC) para monitorear, detectar y responder a incidentes de ciberseguridad en instituciones públicas priorizadas.

- Proveer a las instituciones públicas priorizadas de soluciones tecnológicas para detección y prevención de amenazas.
- Crear y poner en marcha un Centro de Operaciones de Seguridad nacional (SOC-CR) permanente encargado de la gestión preventiva, reactiva y proactiva de riesgos de ciberseguridad a nivel nacional.
- Implementar sistemas avanzados de alerta y respuesta intersectorial ante incidentes de ciberseguridad en instituciones públicas.
- Crear y ejecutar una estrategia para promover la creación y el fortalecimiento de SOC sectoriales.

Línea de Acción 3.3. Proteger y defender las infraestructuras críticas nacionales y los operadores de servicios esenciales

- Definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades.
- Identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales.
- Identificar y categorizar las infraestructuras críticas nacionales y los operadores de servicios esenciales.
- Adelantar evaluaciones de riesgos de ciberseguridad de las infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales.
- Coordinar ejercicios y simulacros nacionales de ciberseguridad para probar el estado de preparación de los operadores de infraestructuras críticas nacionales y de servicios esenciales.

Línea de Acción 3.4. Fortalecer el tratamiento de la información relacionada con incidentes de ciberseguridad

- Crear un Registro Nacional de Incidentes de Ciberseguridad haciendo énfasis en el reporte de incidentes de ciberseguridad en infraestructuras críticas nacionales.
- Establecer mecanismos eficientes asegurando el correcto procesamiento, administración, almacenamiento, compartición e intercambio de información sobre incidentes de ciberseguridad entre las múltiples partes interesadas incluyendo la aplicación de estándares recomendados por la industria y la participación en redes regionales e internacionales como la Red CSIRT Américas de la OEA/CICTE.
- Crear y poner en marcha un mecanismo de notificación a autoridades competentes de la aplicación de la ley.
- Crear y poner en marcha un mecanismo de notificación a personas u organizaciones afectadas por incidentes de ciberseguridad.
- Divulgar información oportuna y confiable sobre riesgos de ciberseguridad que afectan a la sociedad costarricense resaltando aquellos debidos al género y otras interseccionalidades.

4.8.4. Reforzar las capacidades del ecosistema de ciberseguridad

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.

- **Línea de Acción 4.1. Mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles**

  - Elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
  - Formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
  - Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas.
  - Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y personas en cargos directivos en organizaciones privadas, haciendo énfasis en MIPYMES.
  - Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales que ejercen la protección de infraestructuras críticas nacionales y en operadores de servicios esenciales
  - Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales de autoridades competentes de aplicación de la ley, incluyendo un enfoque sensible a la víctima para los delitos en línea, como el ciberacoso, la violencia de género en línea y el abuso y explotación sexual en línea de menores de edad.
  - Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para la sociedad costarricense en general reconociendo las necesidades de seguridad diferenciadas e interseccionales de las personas y comunidades.

- **Línea de Acción 4.2. Fomentar una cultura ciudadana responsable en ciberseguridad**

  - Desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
  - Desarrollar herramientas y recursos en línea, como tutoriales, videos y guías, que permitan a la ciudadanía costarricense adquirir y fortalecer habilidades en ciberseguridad.

- Crear e implementar un programa de concientización en prácticas de ciberhigiene y uso responsable de la tecnología para la población en general, y para las infancias y adolescencias en particular.
- Divulgar información sobre el estado del cibercrimen a nivel nacional desagregando datos basados en el perfil de la víctima que informarán estrategias específicas para abordar los desafíos que enfrentan esos perfiles.

Línea de Acción 4.3. Promover la investigación, el desarrollo y la innovación

- Establecer e implementar un programa para impulsar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad especialmente en el ámbito de la protección y resiliencia de infraestructuras críticas nacionales.
- Elaborar estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas junto con su impacto en la ciberseguridad.
- Crear e implementar un plan para fomentar la creación de nuevas empresas, en alianza con incubadoras y aceleradoras de emprendimiento.
- Promover la investigación y el desarrollo en ciberseguridad basado en análisis de género e interseccionalidad para proteger a las personas más vulnerables a tipos específicos de ciberataques.

4.8.5. Cooperar en el entorno digital

Costa Rica impulsará la cooperación nacional e internacional, la colaboración y el intercambio de información sobre cuestiones de ciberseguridad. Este pilar enfatiza la participación en iniciativas, alianzas y foros internacionales para abordar las amenazas cibernéticas transfronterizas y promover normas de seguridad cibernética global.

Línea de Acción 5.1. Fortalecer la cooperación, colaboración y asistencia en ciberseguridad entre las múltiples partes interesadas a nivel nacional

- Promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
- Fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
- Establecer mecanismos específicos de cooperación con operadores de infraestructuras críticas nacionales y operadores de servicios esenciales.

Línea de Acción 5.2. Maximizar los beneficios de la cooperación cibernética internacional

- Nombrar responsabilidades organizativas para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político / estratégico.
- Promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.

- Fortalecer la participación del CSIRT-CR en redes regionales e internacionales de equipos de respuesta a incidentes como la Red CSIRTS Américas de la OEA/CICTE.
- Promover alianzas con instituciones de otras ramas del poder público, en especial con aquellas instancias que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional en materia de ciberseguridad y de lucha contra la ciberdelincuencia.
- Establecer mecanismos de cooperación en la investigación y persecución de delitos cibernéticos con organismos de seguridad y justicia internacionales.
- Participar en operaciones conjuntas y colaborativas para desmantelar redes de cibercriminales y proteger a las víctimas de ciberdelitos.
- Participar en la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio estable, seguro y confiable comprendiendo el impacto de las operaciones cibernéticas maliciosas en los grupos vulnerables.
- Promover la consideración de aspectos de género y diversidad y una participación activa y efectiva de las mujeres en los debates internacionales sobre cuestiones de seguridad internacional relacionadas con el comportamiento responsable de los Estados en el ciberespacio, así como la incorporación del componente cibernético en los esfuerzos estatales para la implementación de la Resolución 1325 del Consejo de Seguridad de Naciones Unidas sobre “Mujer, Paz y Seguridad”.

5. INTERVENCIONES PÚBLICAS

Costa Rica continuará avanzando en su desarrollo y empleará las oportunidades de optimización para reforzar su estrategia en la lucha contra los ataques informáticos, fomentando de esta manera una sociedad y economía estable y segura al definir áreas clave para la implementación de su Estrategia Nacional de Ciberseguridad 2023-2027.

Mediante la ejecución metódica de acciones específicas, Costa Rica aspira a mantener su liderazgo en investigación y desarrollo en TIC, además de ser un referente en la formación de profesionales especializados en ciberseguridad e informática. A nivel nacional, la ciberseguridad solo puede implementarse mediante un enfoque multifacético y diverso, garantizando así el desarrollo simultáneo de áreas clave para fortalecer la resiliencia cibernética del país.

Costa Rica, consciente de que las amenazas informáticas son una realidad presente y no un riesgo futuro, asignará los recursos gubernamentales necesarios para garantizar el éxito de esta estrategia. Además, establecerá alianzas con todos los actores relevantes para avanzar en sus objetivos y metas. El Gobierno impulsará una cultura de ciberseguridad en el sector público y fomentará la asignación de recursos para este propósito.

A continuación, se presentan las intervenciones públicas teniendo en cuenta el marco estratégico de la Estrategia Nacional de Ciberseguridad 2023-2027.

Nota: (*) Las entidades públicas que se mencionan en los siguientes cuadros como entidades responsables o entidades de apoyo serán contactadas por el MICITT de manera oficial con el fin de solicitar su apoyo y, si es del caso, oficializar durante el proceso de consulta pública el nivel de compromiso en el marco de sus funciones y competencias.

Objetivo Estratégico 1. Reforzar la gobernanza de ciberseguridad
Línea de Acción 1.1. Consolidar la instancia de coordinación nacional de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
1	Hoja de Ruta para reestructurar el MICITT	Establecer y poner en marcha una hoja de ruta para reestructurar el MICITT consolidando y centralizando los esfuerzos y actividades relacionados con la ciberseguridad a nivel nacional	Hoja de ruta para reestructurar el MICITT implementada	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Recursos propios de las entidades	MICITT Apoyo de MH y otros Ministerios	Financiero Económico Operativo Tecnológico
2	Instancia de coordinación nacional de ciberseguridad	Fortalecer la instancia de coordinación nacional para dirigir la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027 y hacer seguimiento continuo, dotándola de herramientas jurídicas y técnicas que le permitan desempeñar sus funciones con la mayor efectividad	Cantidad de nuevas herramientas técnicas en funcionamiento en la Instancia de coordinación nacional de ciberseguridad	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MICITT Apoyo de MH y otros Ministerios	Financiero Operativo Tecnológico
3	Recurso humano para la coordinación nacional de ciberseguridad	Asegurar que la instancia de coordinación nacional cuente con un equipo de personal especializado, calificado y técnico dedicado a las acciones de ciberseguridad promoviendo la igualdad de género y la diversidad	Cantidad de personas trabajando en la instancia de coordinación nacional	4	Meta del indicador para el periodo: 25 Meta del indicador por año: 2024: 10 2025: 5 2026: 5 2027: 5	Recursos propios de las entidades	MICITT Apoyo de MH, MCM, INAMU y otros Ministerios	Financiero Operativo

Objetivo Estratégico 1. Reforzar la gobernanza de ciberseguridad
Línea de Acción 1.2. Establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
4	Marco de gobernanza nacional de ciberseguridad	Construir y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.	Acto administrativo para la creación del marco de gobernanza nacional de ciberseguridad	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Cooperación internacional y recursos propios de las entidades	MICITT Apoyo de CNSL, CISTE, MCM, INAMU y todos los Ministerios MICITT Apoyo de MP, MIDEPLAN, DIS, UEI, SUTEL, MCM, INAMU MICITT Apoyo de MP, MIDEPLAN, DIS, UEI, SUTEL	Político Financiero Económico Operativo Social
5	Instancia de planeación estratégica de ciberseguridad	Renovar la instancia de máximo nivel intergubernamental e intersectorial de planeación estratégica para orientar la gestión de la ciberseguridad en el país, promoviendo la igualdad de género y la diversidad						
6	Instancia de planeación táctica de ciberseguridad	Crear instancias de planeación táctica para asesorar la implementación de acciones establecidas y priorizadas teniendo en cuenta la cooperación con los líderes tecnológicos y personas expertas en el campo.						
7	Mecanismos dinámicos de coordinación y colaboración	Crear y poner en marcha mecanismos dinámicos de coordinación, colaboración e intercambio de información intergubernamental e intersectorial vinculando a las múltiples partes interesadas.	Cantidad de mecanismos de coordinación, colaboración e intercambio de información intergubernamental e intersectorial creados y puestos en marcha	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MP y MIDEPLAN	Operativo Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
8	Figuras de enlace institucional	Crear una figura de enlace (persona responsable de ciberseguridad) en instituciones públicas, en gobiernos locales y en otras organizaciones a nivel operativo.	Porcentaje de organizaciones públicas con figuras de enlace de ciberseguridad	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de todas las organizaciones públicas	Financiero Operativo
9	Estrategias, protocolos y mecanismos de comunicación	Desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.	Cantidad de mecanismos de comunicación creados y puestos en marcha	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MP y MIDEPLAN	Financiero Operativo Social
10	Mecanismos de seguimiento y control	Establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.	Cantidad de reportes sobre el cumplimiento de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad	4	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MP, MCM, INAMU y MIDEPLAN	Financiero Operativo Social
11	Evaluaciones de impacto socio económico	Adelantar evaluaciones de impacto socio económico respecto de la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027.	Cantidad de evaluaciones de impacto socio económico respecto de la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 0 2025: 0 2026: 0 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MP, MCM, INAMU y MIDEPLAN	Financiero Operativo Social

Objetivo Estratégico 1. Reforzar la gobernanza de ciberseguridad
Línea de Acción 1.3. Asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
12	Hoja de ruta para la transición al cese de estado de emergencia	Establecer y poner en marcha una hoja de ruta para la transición al cese de estado de emergencia declarado mediante el Decreto Ejecutivo No. 43542-MP-MICITT de 2022	Hoja de ruta para la transición al cese de estado de emergencia implementada	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Recursos propios de las entidades	MICITT Apoyo de MH, CNE, MIDEPLAN, CGR	Geopolítico Político Financiero Económico Operativo Tecnológico Emergente Social
13	Plan de inversión para iniciativas de ciberseguridad	Desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad	Plan de inversión para la asignación de recursos en instituciones públicas para llevar a cabo iniciativas de ciberseguridad	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Recursos propios de las entidades	MICITT Apoyo de MH y todas las instituciones públicas	Financiero Económico Operativo Tecnológico
14	Recurso humano de ciberseguridad en instituciones públicas	Reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad	Porcentaje de instituciones públicas con recurso humano destinado específicamente a la ciberseguridad	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de MCM, INAMU y todas las instituciones públicas	Financiero Operativo Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
15	Presupuesto anual en instituciones públicas	Promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad	Porcentaje de instituciones públicas con presupuesto integrado para llevar a cabo iniciativas de ciberseguridad	0	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 40% 2025: 30% 2026: 30% 2027: 0%	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Financiero Operativo Tecnológico
16	Procesos de adquisición y compra de recursos tecnológicos en instituciones públicas	Establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad	Porcentaje de instituciones públicas implementando procesos para la adquisición y compra de recursos tecnológicos para la gestión integral de los riesgos de ciberseguridad	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 40% 2025: 30% 2026: 30% 2027: 0%	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Financiero Operativo Tecnológico
17	Programa de estímulos a la inversión privada	Promover el diseño de estímulos a la inversión del sector privado para la financiación de proyectos de ciberseguridad	Cantidad de programas para estimular la inversión del sector privado implementados	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 0 2025: 1 2026: 0 2027: 0	Recursos propios de las entidades	MICITT Apoyo de MH, MEIC, MIDEPLAN	Financiero Operativo Tecnológico

Objetivo Estratégico 2. Adecuar el marco jurídico cibernético
Línea de Acción 2.1. Fortalecer el marco legal y regulatorio cibernético

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
18	Trámites de iniciativas o proyectos legislativos	Apoyar a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.	Porcentaje de trámites de iniciativas o proyectos legislativos apoyados al año	100%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de MP	Geopolítico Político Financiero Económico Social
19	Trámite de iniciativas o proyectos regulatorios	Apoyar a los reguladores sectoriales en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco regulatorio relacionado con la ciberseguridad, así como en el ejercicio de supervisión y verificación del cumplimiento de las disposiciones de los marcos regulatorios sectoriales relacionadas con la ciberseguridad.	Porcentaje de trámites de iniciativas o proyectos regulatorios apoyados al año	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de reguladores sectoriales	Financiero Económico Operativo
20	Revisión del marco legal y regulatorio cibernético	Revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales	Cantidad de revisiones del marco legal y regulatorio cibernético	0	Meta del indicador para el periodo: 2 Meta del indicador por año: 2024: 0 2025: 1 2026: 0 2027: 1	Cooperación internacional	MICITT Apoyo de MCM, INAMU, DIS y UEI	Operativo

Objetivo Estratégico 2. Adecuar el marco jurídico cibernético
Línea de Acción 2.2. Fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
21	Marco normativo del CSIRT-CR	Actualizar el marco normativo para fortalecer los procesos de gestión administrativa y técnica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)	Cantidad de actos administrativos (decretos, resoluciones u otros) fortaleciendo el CSIRT-CR	0	Meta del indicador para el periodo: 2 Meta del indicador por año: 2024: 1 2025: 1 2026: 0 2027: 0	Cooperación internacional	MICITT	Financiero Económico Operativo Tecnológico Emergente Social
22	Estándares, protocolos y procedimientos técnicos: Guías y Plan	Establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional, incluyendo: □ Guías para la evaluación de los programas interinstitucionales en materia de seguridad de TIC □ Planes de contingencia en materia de seguridad de las TIC en el sector público □ Guías para reducir el impacto y la probabilidad de incidentes de ransomware y extorsión de datos en organizaciones públicas y privadas, incluyendo mejores prácticas internacionales para prepararse, prevenir y mitigar estos incidentes.	Cantidad de estándares, protocolos y procedimientos técnicos establecidos	0	Meta del indicador para el periodo: 10 Meta del indicador por año: 2024: 3 2025: 3 2026: 2 2027: 2	Cooperación internacional	MICITT	Operativo Tecnológico
23	Marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales	Desarrollar un marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales, adoptando normas y estándares internacionales, incluyendo: □ Protocolo nacional de gestión y respuesta a crisis y emergencias cibernéticas. □ Planes de contingencia y recuperación para las infraestructuras críticas nacionales y los servicios esenciales □ Manual para adelantar ejercicios y simulacros nacionales de ciberseguridad	Cantidad de normas técnicas relacionadas específicamente con infraestructuras críticas nacionales y de operadores de servicios esenciales establecidos	0	Meta del indicador para el periodo: 6 Meta del indicador por año: 2024: 2 2025: 2 2026: 1 2027: 1	Cooperación internacional	MICITT	Operativo Tecnológico
24	Mecanismos de supervisión al cumplimiento	Impulsar el cumplimiento del marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad.	Porcentaje de instituciones públicas cumpliendo el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad.	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de reguladores sectoriales SUTEL	Operativo

Objetivo Estratégico 3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional
Línea de Acción 3.1. Adoptar un marco para la gestión integral de riesgos de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
25	Marco de gestión integral de riesgos de ciberseguridad	Elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades.	Marco de gestión integral de riesgos de ciberseguridad elaborado	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 0 2025: 1 2026: 0 2027: 0	Cooperación internacional	MICITT Apoyo de MIDEPLAN, MCM, INAMU	Operativo Tecnológico Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
26	Procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos	Establecer procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos de ciberseguridad adaptándolo a las nuevas amenazas, vulnerabilidades y tendencias en el ámbito de la ciberseguridad	Porcentaje de instituciones públicas implementando el marco de gestión integral de riesgos de ciberseguridad	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 0% 2025: 20% 2026: 30% 2027: 50%%	Recursos propios de las entidades	MICITT Apoyo de MIDEPLAN y OIJ	Operativo Tecnológico
27	Integración de la gestión de riesgos de ciberseguridad en procesos institucionales	Garantizar que los procesos de gestión de riegos de ciberseguridad y de gestión de riesgos de la seguridad de la información se integren en los procesos de planificación estratégica, operativa, y presupuestaria de las instituciones públicas	Proceso de integración de la gestión de riesgos de ciberseguridad en procesos institucionales	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 0 2025: 1 2026: 0 2027: 0	Recursos propios de las entidades	MICITT Apoyo de MIDEPLAN	Operativo Tecnológico

Objetivo Estratégico 3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional
Línea de Acción 3.2. Fortalecer las capacidades nacionales de monitoreo, detección y respuesta a incidentes de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
28	Plan de fortalecimiento de capacidades de CSRT-CR	Crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad	Plan de fortalecimiento de capacidades del CSIRT-CR implementado	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 0 2025: 1 2026: 0 2027: 0	Cooperación internacional	MICITT	Financiero Económico Operativo Tecnológico
29	Solución de Centro de Operaciones de Seguridad (SOC)	Proveer una solución de Centro de Operaciones de Seguridad (SOC) para monitorear, detectar y responder a incidentes de ciberseguridad en instituciones públicas priorizadas	Porcentaje de avance en la implementación de la solución de Centro de Operaciones de Seguridad (SOC)	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 50% 2025: 50% 2026: 0% 2027: 0%	Cooperación internacional	MICITT Apoyo de instituciones públicas priorizadas	Financiero Operativo Tecnológico
30	Instituciones públicas priorizadas	Proveer a las instituciones públicas priorizadas de soluciones tecnológicas para detección y prevención de amenazas	Porcentaje de instituciones públicas priorizadas conectadas a la solución de Centro de Operaciones de Seguridad (SOC)	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 50% 2025: 50% 2026: 0% 2027: 0%	Cooperación internacional	MICITT Apoyo de instituciones públicas priorizadas	Financiero Operativo Tecnológico
31	Centro de Operaciones de Seguridad nacional (SOC-CR) permanente	Crear y poner en marcha un Centro de Operaciones de Seguridad nacional (SOC-CR) permanente encargado de la gestión preventiva, reactiva y proactiva de riesgos de ciberseguridad a nivel nacional	Porcentaje de avance en la implementación y puesta en marcha del Centro de Operaciones de Seguridad nacional (SOC-CR) permanente	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 0% 2025: 0% 2026: 50% 2027: 50%	Cooperación internacional	MICITT Apoyo de todas las instituciones públicas	Financiero Operativo Tecnológico
32	Sistemas avanzados de alerta y respuesta intersectorial	Implementar sistemas avanzados de alerta y respuesta intersectorial ante incidentes de ciberseguridad en instituciones públicas	Porcentaje de instituciones públicas con sistemas avanzados de alerta y respuesta intersectorial implementados	0%	Meta del indicador para el periodo: 50% Meta del indicador por año: 2024: 10% 2025: 10% 2026: 15% 2027: 15%	Cooperación internacional	MICITT Apoyo de todas las instituciones públicas	Financiero Operativo Tecnológico

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
33	Estrategia para promover SOC sectoriales	Crear y ejecutar una estrategia para promover la creación y el fortalecimiento de SOC sectoriales	Cantidad de nuevos SOC sectoriales creados y puestos en marcha	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Cooperación internacional	MICITT Apoyo de todas las instituciones públicas	Financiero Operativo Tecnológico

Objetivo Estratégico 3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional
Línea de Acción 3.3. Proteger y defender las infraestructuras críticas nacionales y los operadores de servicios esenciales

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
34	Criterios para designar infraestructuras críticas nacionales	Definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades.	Porcentaje de instituciones públicas que aplican los criterios para designar infraestructuras críticas nacionales	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Cooperación internacional	MICITT Apoyo de MCM, INAMU y todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico
35	Identificación de operadores de infraestructuras críticas nacionales y que prestan servicios esenciales	Identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Porcentaje de operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales identificados	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 60% 2025: 20% 2026: 10% 2027: 10%	Cooperación internacional	MICITT Apoyo de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico
36	Catálogo de infraestructuras críticas nacionales	Identificar y categorizar las infraestructuras críticas nacionales y los operadores de servicios esenciales	Cantidad de actualizaciones al catálogo de infraestructuras críticas nacionales y los operadores de servicios esenciales	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Cooperación internacional	MICITT Apoyo de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico
37	Evaluaciones de riesgos de ciberseguridad de infraestructuras críticas nacionales	Adelantar evaluaciones de riesgos de ciberseguridad de infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales	Cantidad de evaluaciones de riesgos de ciberseguridad de infraestructuras críticas nacionales y servicios esenciales adelantadas	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Cooperación internacional	MICITT Apoyo de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico
38	Ejercicios y simulacros nacionales de ciberseguridad	Coordinar ejercicios y simulacros nacionales de ciberseguridad para probar el estado de preparación de los operadores de infraestructuras críticas nacionales y de servicios esenciales	Cantidad de ejercicios y simulacros nacionales de ciberseguridad ejecutados	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Cooperación internacional	MICITT Apoyo de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Financiero Operativo Tecnológico

Objetivo Estratégico 3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional

Línea de Acción 3.4. Fortalecer el tratamiento de la información relacionada con incidentes de ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
39	Registro Nacional de Incidentes de Ciberseguridad	Crear un Registro Nacional de Incidentes de Ciberseguridad haciendo énfasis en el reporte de incidentes de ciberseguridad en infraestructuras críticas nacionales	Porcentaje de instituciones públicas que reportan incidentes de ciberseguridad al Registro Nacional	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Cooperación internacional	MICITT Apoyo de todas las instituciones públicas	Operativo Tecnológico
40	Mecanismos eficientes para el tratamiento de la información de incidentes de ciberseguridad	Establecer mecanismos eficientes asegurando el correcto procesamiento, administración, almacenamiento, compartición e intercambio de información sobre incidentes de ciberseguridad entre las múltiples partes interesadas incluyendo la aplicación de estándares recomendados por la industria y la participación en redes regionales e internacionales como la Red CSIRT Américas de la OEA/CICTE.	Porcentaje de instituciones públicas usando los mecanismos para el tratamiento de la información de incidentes de ciberseguridad	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Operativo Tecnológico
41	Mecanismo de notificación a autoridades competentes de la aplicación de la ley	Crear y poner en marcha un mecanismo de notificación a autoridades competentes de la aplicación de la ley	Porcentaje de instituciones públicas usando el mecanismo de notificación a autoridades competentes de la aplicación de la ley	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Operativo Tecnológico
42	Mecanismo de notificación a personas u organizaciones afectadas	Crear y poner en marcha un mecanismo de notificación a personas u organizaciones afectadas por incidentes de ciberseguridad.	Porcentaje de instituciones públicas usando el mecanismo de notificación a personas u organizaciones afectadas	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Operativo Tecnológico
43	Mecanismo de divulgación de información sobre riesgos de ciberseguridad	Divulgar información oportuna y confiable sobre riesgos de ciberseguridad que afectan a la sociedad costarricense resaltando aquellos debidos al género y otras interseccionalidades.	Cantidad de reportes divulgados sobre riesgos de ciberseguridad que afectan a la sociedad costarricense	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MICITT Apoyo de MCM, INAMU	Operativo Tecnológico Social

Objetivo Estratégico 4. Reforzar las capacidades del ecosistema de ciberseguridad
Línea de Acción 4.1. Mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles con enfoque centrado en el ser humano y de género con perspectiva interseccional

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
44	Plan nacional de educación y formación en ciberseguridad	Elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.	Plan nacional de educación y formación en ciberseguridad elaborado	0	Meta del indicador para el periodo: 0 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Cooperación internacional	MEP Apoyo de MICITT, MCM, INAMU, MNA, MDHIS, MCJ	Financiero Económico Operativo Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
45	Estrategia nacional de desarrollo de fuerza laboral de ciberseguridad	Formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.	Estrategia de desarrollo de fuerza laboral de ciberseguridad formulada	0	Meta del indicador para el periodo: 1 Meta del indicador por año: 2024: 1 2025: 0 2026: 0 2027: 0	Cooperación internacional	MICITT Apoyo de MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Financiero Económico Operativo Social
46	Programas de capacitación a sector público	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas	Porcentaje de personas en instituciones públicas capacitadas en ciberseguridad	0%	Meta del indicador para el periodo: 50% Meta del indicador por año: 2024: 10% 2025: 10% 2026: 15% 2027: 15%	Recursos propios de las entidades	MICITT Apoyo de MEP y todas las instituciones públicas	Operativo Social
47	Programas de capacitación a sector privado	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y personas en cargos directivos en organizaciones privadas, haciendo énfasis en MIPYMES	Cantidad de personas en organizaciones privadas capacitadas en ciberseguridad	0	Meta del indicador para el periodo: 10.000 Meta del indicador por año: 2024: 2.500 2025: 2.500 2026: 2.500 2027: 2.500	Recursos propios de las entidades	MICITT Apoyo de MEP	Operativo Social
48	Programas de capacitación a infraestructuras críticas nacionales	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales que ejercen la protección de infraestructuras críticas nacionales y en operadores de servicios esenciales	Porcentaje de profesionales que ejercen la protección de infraestructuras críticas nacionales y en operadores de servicios esenciales capacitados	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 60% 2025: 20% 2026: 10% 2027: 10%	Recursos propios de las entidades	MICITT Apoyo MEP y de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico
49	Programas de capacitación al sector de aplicación de la ley	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales de autoridades competentes de aplicación de la ley, incluyendo un enfoque sensible a la víctima para los delitos en línea, como el ciberacoso, la violencia de género en línea y el abuso y explotación sexual en línea de menores de edad.	Porcentaje de profesionales en autoridades competentes de aplicación de la ley	0%	Meta del indicador para el periodo: 70% Meta del indicador por año: 2024: 20% 2025: 20% 2026: 15% 2027: 15%	Recursos propios de las entidades	MICITT Apoyo MEP, MCM, INAMU y de todas las autoridades de aplicación de la ley	Operativo Tecnológico
50	Programas de capacitación a la ciudadanía	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para la sociedad costarricense en general reconociendo las necesidades de seguridad diferenciadas e interseccionales de diversas personas.	Cantidad de personas que participan en los espacios de fomento de la ciberseguridad	4.429	Meta del indicador para el periodo: 31.000 Meta del indicador por año: 2024: 5.693 2025: 6.959 2026: 8.857 2027: 9.491	Recursos propios de las entidades	MICITT Apoyo de MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operativo Social

Objetivo Estratégico 4. Reforzar las capacidades del ecosistema de ciberseguridad
Línea de Acción 4.2. Fomentar una cultura ciudadana responsable en ciberseguridad

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
51	Campañas nacionales de concientización	Desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples	Cantidad de campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad ejecutadas	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1	Cooperación internacional	MICITT Apoyo de MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operativo Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
		partes interesadas con enfoque de género y con perspectiva interseccional			2026: 1 2027: 1			
52	Herramientas y recursos en línea de concientización	Desarrollar herramientas y recursos en línea, como tutoriales, videos y guías, que permitan a la ciudadanía costarricense adquirir y fortalecer habilidades en ciberseguridad	Cantidad de personas usando herramientas y recursos en línea para adquirir y fortalecer habilidades en ciberseguridad	0	Meta del indicador para el periodo: 7.000 Meta del indicador por año: 2024: 1.000 2025: 1.500 2026: 2.000 2027: 2.500	Cooperación internacional	MICITT Apoyo de MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operativo Social
53	programa de concientización sobre ciberhigiene y uso responsable de tecnologías	Crear e implementar un programa de concientización en prácticas de ciberhigiene y uso responsable de la tecnología en la población en general	Cantidad de campañas nacionales de concientización en prácticas de ciberhigiene y uso responsable de la tecnología ejecutadas	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operativo Social
54	Mecanismos de divulgación sobre estado de cibercrímen	Divulgar información sobre el estado del cibercrímen a nivel nacional desagregando datos basados en el perfil de la víctima que informarán estrategias específicas para abordar los desafíos que enfrentan esos perfiles.	Cantidad de reportes sobre el estado del cibercrímen a nivel nacional publicados	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MICITT Apoyo de OIJ, MCM y INAMU	Operativo Social

Objetivo Estratégico 4. Reforzar las capacidades del ecosistema de ciberseguridad
Línea de Acción 4.3. Promover la investigación, el desarrollo y la innovación

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
55	Programa para impulsar la innovación y el desarrollo tecnológico	Establecer e implementar un programa para impulsar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad especialmente en el ámbito de la protección y resiliencia de infraestructuras críticas nacionales	Cantidad de proyectos para impulsar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad	0	Meta del indicador para el periodo: 20 Meta del indicador por año: 2024: 2 2025: 4 2026: 6 2027: 8	Recursos propios de las entidades	MICITT Apoyo de MH y de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Financiero Operativo Tecnológico
56	Estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas	Elaborar estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas junto con su impacto en la ciberseguridad	Cantidad de estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Cooperación internacional	MICITT	Financiero Operativo Tecnológico Emergente
57	Plan de fomento a la creación de nuevas empresas	Crear e implementar un plan para fomentar la creación de nuevas empresas, en alianza con incubadoras y aceleradoras de emprendimiento	Cantidad de empresas creadas bajo el plan de fomento a la creación de nueva empresa implementado	8	Meta del indicador para el periodo: 20 Meta del indicador por año: 2024: 5 2025: 5 2026: 5 2027: 5	Recursos propios de las entidades	MICITT Apoyo de MH y MEIC	Financiero Operativo Tecnológico
58	Estudios para promover investigación y desarrollo	Promover la investigación y el desarrollo en ciberseguridad basado en análisis de género e interseccionalidad para proteger a las personas	Cantidad de estudios para promover la investigación y el desarrollo en ciberseguridad	0	Meta del indicador para el periodo: 2 Meta del indicador por año: 2024: 0	Recursos propios de las entidades	MICITT Apoyo de MCM, INAMU, MNA, MDHIS, MCJ	Operativo Tecnológico Social

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
		más vulnerables a tipos específicos de ciberataques.			2025: 1 2026: 0 2027: 1			

Objetivo Estratégico 5. Cooperar en el entorno digital
Línea de Acción 5.1. Fortalecer la cooperación, colaboración y asistencia en ciberseguridad entre las múltiples partes interesadas a nivel nacional

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
59	Iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial	Promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial	Cantidad de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial firmadas	0	Meta del indicador para el periodo: 12 Meta del indicador por año: 2024: 3 2025: 3 2026: 3 2027: 3	Recursos propios de las entidades	MICITT Apoyo de instituciones públicas	Operativo Tecnológico
60	Alianzas con sector privado, organizaciones de la sociedad civil y academia	Fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.	Cantidad de alianzas con sector privado, organizaciones de la sociedad civil y academia firmadas	0	Meta del indicador para el periodo: 20 Meta del indicador por año: 2024: 5 2025: 5 2026: 5 2027: 5	Recursos propios de las entidades	MICITT Apoyo de MEP, MEIC	Operativo Tecnológico
61	Mecanismos de cooperación con operadores de infraestructuras críticas nacionales	Establecer mecanismos específicos de cooperación con operadores de infraestructuras críticas nacionales y operadores de servicios esenciales.	Porcentaje de operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales usando el mecanismo de cooperación establecido	0%	Meta del indicador para el periodo: 100% Meta del indicador por año: 2024: 60% 2025: 20% 2026: 10% 2027: 10%	Recursos propios de las entidades	MICITT Apoyo de todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales	Operativo Tecnológico

Objetivo Estratégico 5. Cooperar en el entorno digital
Línea de Acción 5.2. Maximizar los beneficios de la cooperación cibernética internacional

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
62	Responsable de ciber diplomacia	Nombrar responsabilidades organizativas para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político / estratégico.	Cantidad de reportes sobre el estado de la cooperación internacional a nivel político / estratégico	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MREC Apoyo de MP y MICITT	Geopolítico Político Operativo
63	Convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales	Promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.	Cantidad de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales firmados	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MREC Apoyo de MP, MICITT, OIJ e instancias que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional	Geopolítico Político Operativo

#	Intervención pública	Objetivo	Indicador	Línea Base	Meta	Recursos requeridos	Responsable	Riesgos
64	Fortalecimiento de la participación del CSIRT-CR en redes internacionales	Fortalecer la participación del CSIRT-CR en redes regionales e internacionales de equipos de respuesta a incidentes como la Red CSIRTS Américas de la OEA/CICTE.	Cantidad de acuerdos con redes de CSIRT regionales e internacionales firmados	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MICITT Apoyo de MREC	Operativo Tecnológico Emergente
65	Alianzas con instituciones de otras ramas del poder público en torno a la cooperación internacional	Promover alianzas con instituciones de otras ramas del poder público, en especial con aquellas instancias que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional en materia de ciberseguridad y de lucha contra la ciberdelincuencia.	Cantidad de alianzas firmadas con instituciones de otras ramas del poder público que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional en materia de ciberseguridad y de lucha contra la ciberdelincuencia	0	Meta del indicador para el periodo: 8 Meta del indicador por año: 2024: 2 2025: 2 2026: 2 2027: 2	Recursos propios de las entidades	MICITT Apoyo de MP, MREC e instancias que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional	Político Operativo
66	Mecanismos de cooperación con organismos de seguridad y justicia internacionales	Establecer mecanismos de cooperación en la investigación y persecución de delitos cibernéticos con organismos de seguridad y justicia internacionales	Cantidad de mecanismos de cooperación para la investigación y persecución de delitos cibernéticos establecidos creados y puestos en marcha	0	Meta del indicador para el periodo: Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de todas las instituciones públicas	Político Operativo
67	Participación del país en operaciones internacionales	Participar en operaciones conjuntas y colaborativas para desmantelar redes de cibercriminales y proteger a las víctimas de ciberdelitos	Cantidad de reportes con el resultado de operaciones conjuntas y colaborativas para desmantelar redes de cibercriminales y proteger a las víctimas de ciberdelitos	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MICITT Apoyo de MP, MREC y OIJ	Geopolítico Operativo Tecnológico
68	Participación del país en discusión y desarrollo de normativas internacionales	Participar en la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio estable, seguro y confiable comprendiendo el impacto de las operaciones cibernéticas maliciosas en los grupos vulnerables.	Cantidad de eventos internacionales asistidos para la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio estable, seguro y confiable	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MREC Apoyo de MP y MICITT	Geopolítico Político Operativo
69	Participación del país sobre comportamiento responsable de los Estados e implementación de la Resolución 1325	Promover la consideración de aspectos de género y diversidad y una participación activa y efectiva de las mujeres en los debates internacionales sobre cuestiones de seguridad internacional relacionadas con el comportamiento responsable de los Estados en el ciberespacio, así como la incorporación del componente cibernético en los esfuerzos estatales para la implementación de la Resolución 1325 del Consejo de Seguridad de Naciones Unidas sobre "Mujer, Paz y Seguridad".	Cantidad de eventos internacionales asistidos sobre cuestiones de seguridad internacional relacionadas con el comportamiento responsable de los Estados en el ciberespacio y la incorporación del componente cibernético en los esfuerzos estatales para la implementación de la Resolución 1325	0	Meta del indicador para el periodo: 4 Meta del indicador por año: 2024: 1 2025: 1 2026: 1 2027: 1	Recursos propios de las entidades	MREC Apoyo de MP y MICITT	Geopolítico Político Operativo

6. SEGUIMIENTO, EVALUACIÓN Y GESTIÓN DE RIESGOS

El seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los Objetivos Estratégicos se realizará a través de un *Plan de Acción* que señala las entidades responsables de cada acción, los periodos de ejecución de estas, los recursos necesarios y disponibles para llevarlas a cabo, y la importancia de cada acción para el cumplimiento del propósito general y los objetivos específicos bajo cada pilar de la Estrategia.

La instancia de Coordinación Nacional de Ciberseguridad adelantará trimestralmente actividades de monitoreo y evaluación de la implementación de la Estrategia y presentará reportes anuales a la instancia de máximo nivel intergubernamental e intersectorial de planeación estratégica.

Costa Rica adelantará monitoreo del nivel de madurez en ciberseguridad y evaluación de las capacidades de las múltiples partes interesadas con el fin de asegurar una mejora continua, haciendo énfasis en el corto y mediano plazo. Adicionalmente, se soportará en el desarrollo de auditorías sobre los procesos que llevan a cabo las instituciones públicas y el desarrollo de ejercicios de eficiencia comparativa basada en la recolección y análisis de información estadística relevante a nivel nacional, así como en la elaboración de reportes situacionales sobre el estado de la ciberseguridad.

Finalmente, se prevé también la revisión y la actualización de la Estrategia cada año o según sea necesario.

Los indicadores claves de rendimiento serán monitoreados y evaluados por la instancia de Coordinación Nacional de Ciberseguridad trimestralmente y presentará reportes anuales a la instancia de máximo nivel intergubernamental e intersectorial de planeación estratégica.

7. PARTICIPACIÓN SOCIAL Y CIUDADANA

La construcción de la Estrategia Nacional de Ciberseguridad 2023-2027 se soporta en el análisis de insumos fundamentales provistos por todas las múltiples partes interesadas en Costa Rica que permiten construir una propuesta que se pone a consideración de los interesados mediante un proceso de Consulta Pública quienes presentaron consideraciones en un plazo prudencial de tiempo, las cuales fueron revisadas y atendidas por el Gobierno nacional.

8. DIVULGACIÓN

En línea con lo dispuesto en el Plan Nacional de Desarrollo e Inversiones Públicas 2023-2026 (MIDEPLAN, 2023a), esta Estrategia Nacional está dirigida tanto al público interno (institucionalidad del Estado) como al público externo (todos que tienen un determinado interés por la importancia y relevancia de la ciberseguridad).

Para la divulgación de la Estrategia Nacional de Ciberseguridad 2023-2027 se utilizan las herramientas y mecanismos disponibles en el MICITT (comunicados de prensa, página web, redes sociales, foros y charlas en diversos ámbitos, talleres y mesas de diálogo, centros y

medios de documentación, entre otros), para facilitar la transparencia y rendición de cuentas a la ciudadanía costarricense.

9. GLOSARIO

A continuación, algunas definiciones:

Alertas técnicas: Tienen como objetivo comunicar a un usuario información referente a la ocurrencia de eventos de su interés en un sistema informático.

Amenazas cibernéticas: Se refiere a cualquier posible ataque malicioso que busca acceder ilegalmente a los datos, interrumpir las operaciones digitales o dañar la información.

Análisis de vulnerabilidades: Es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas o identificadas, como exploits, fallas, brechas de seguridad, puntos de entrada de acceso inseguros y los errores de configuración del sistema.

Centro de Operaciones en Seguridad (SOC): Equipo cualificado específicamente en ciberseguridad con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.

Ciberataque: Son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos.

Cibercrimen: Es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos.

Ciberespacio: Es el entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física.

Ciberseguridad: Es la capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos.

Cibernética: Es la ciencia que relaciona las entradas y salidas de un sistema, sus inputs y outputs.

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.

Código Fuente: Conjunto de instrucciones que debe seguir un sistema y que está escrito por programadores, en uno o varios lenguajes de programación para que sea entendible por las personas.

Confidencialidad: Preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, incluidos los medios para proteger la privacidad personal y la información de manejo restringido, limitado o patentado.

Control de seguridad: Son mecanismos de la seguridad para la protección que abarcan desde el acceso a los datos y los sistemas, hasta la gestión de los dispositivos y la protección de las redes.

Delito cibernético: Es el acto ilícito en el que se usan como medio o como fin para realizarlos, las Tecnologías de la Información y la Comunicación, tales como recursos informáticos, electrónicos, tecnológicos, Internet, entre otros. Es decir, en la comisión de estos delitos se usan las computadoras, los teléfonos inteligentes, software, etcétera, como por ejemplo la falsificación de documentos a través de una computadora o destrucción de información contenida en una computadora.

Estándares de Ciberseguridad: Son técnicas generalmente establecidas en materiales publicados que buscan establecer las mejores prácticas para prevenir, detectar, responder a las amenazas de ciberseguridad, con el fin de proteger el entorno cibernético de un usuario u organización para reducir los riesgos, incluyendo prevención o atenuación de ciberataques.

Género: conjunto de valores socialmente construidos que definen las diferentes características (emocionales, afectivas, intelectuales o físicas) y los comportamientos que cada sociedad asigna a los hombres o a las mujeres. A diferencia del sexo, que viene determinado con el nacimiento, el género se aprende y se puede modificar (INAMU, 2018).

Gestión de incidente de ciberseguridad: Actuación ante incidentes de ciberseguridad implantando los controles y los mecanismos necesarios para su monitorización e identificación, así como las líneas de actuación a seguir.

Igualdad de género: Hace referencia a la existencia de un "piso a partir del cual las mujeres pueden ser reconocidas como iguales y ser tratadas normativamente como iguales no en el sentido de identidad, sino en el sentido axiológico: cada persona vale igual que cualquier otra. Cada mujer vale igual que otra mujer y cada hombre, en tanto que cada hombre vale igual que cada hombre y cada mujer. Es el principio de la igual valía de las personas, que es uno de los derechos humanos universales fundamentales (MIDEPLAN, 2017a)

Incidente: Un suceso que real o potencialmente resulta en consecuencias adversas a efectos adversos que representa una amenaza para un sistema de información o la información que el sistema procesa, almacena o transmite y que puede requerir una acción de respuesta para mitigar las consecuencias.

Incidente de Ciberseguridad: Infracción digital o física que amenace la privacidad, el acceso restringido, la integridad o la disponibilidad de los sistemas de información o datos personales sensibles o restringidos, así como confidenciales de una organización. Los incidentes engloban desde ciberataques intencionales realizados por hackers o usuarios no autorizados, hasta violaciones no intencionadas de la política de seguridad de parte de usuarios legítimos autorizados.

Información: Conjunto organizado de datos procesados.

Infraestructura: Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Infraestructura crítica: Sistemas y activos informáticos, ya sean físicos o virtuales, tan vitales para la sociedad que la incapacidad o destrucción de los mismos puede tener un impacto debilitante en la seguridad, la economía, la salud o seguridad pública, el medio ambiente o cualquier combinación de estos asuntos.

Infraestructura Crítica de Información: Son los activos, los sistemas y las redes, ya sean físicos o virtuales, que su incapacitación o destrucción tendría un efecto negativo.

Malware: Es software malintencionado que puede inutilizar los sistemas infectados. La mayoría de las variantes de malware destruyen datos al eliminar o limpiar archivos críticos para la capacidad de ejecución del sistema operativo.

Operador de Infraestructuras Críticas de Información: Son todas las organizaciones o entidades que operen sistemas físicos o virtuales, que ofrecen servicios esenciales para dar apoyo a los sistemas básicos a nivel social, educativo, económico, medioambiental y político.

Perspectiva de género: permite enfocar, analizar y comprender las características que definen a mujeres y hombres de manera específica, así como sus semejanzas y diferencias. Desde esta perspectiva se analizan las posibilidades vitales de unas y otros, el sentido de sus vidas, sus expectativas y oportunidades, las complejas y diversas relaciones sociales que se dan entre ambos géneros (MIDEPLAN, 2017a)

Perspectiva interseccional: La perspectiva interseccional identifica un sistema de opresiones diversas e interconectadas, entre ellas el género, pero que incluyen cuestiones como la raza, la religión y la clase, que crea a veces jerarquías sociales, económicas y de otro tipo complejas entre las personas de una sociedad (APC, 2022).

Phishing: Intentan robar las credenciales o los datos confidenciales de los usuarios como, por ejemplo, números de tarjetas de crédito. En este caso, los estafadores envían a los usuarios e-mails o mensajes de texto diseñados para que parezca que provienen de una fuente legítima, utilizando hipervínculos falsos.

Ransomware: Es un malware sofisticado que se aprovecha de las debilidades del sistema y utiliza un cifrado sólido para mantener los datos o la funcionalidad del sistema como rehenes.

Resiliencia: Capacidad de una organización de resistir ante una situación adversa, como, por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.

Regulador sectorial: Entidad pública dentro de cuyas funciones principales se encuentra la regulación y/o supervisión de uno o más sectores regulados específicos.

Respuesta a incidentes: Las actividades que abordan los efectos directos a corto plazo de un incidente y también pueden apoyar la recuperación a corto plazo.

Riesgo: Medida del grado en el que una entidad se ve amenazada por una circunstancia o evento potencial y típicamente una función de los impactos adversos que surgirían si ocurriera la circunstancia o el evento; y la probabilidad de que ocurra.

Riesgos digitales: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado.

Sector regulado: Representa alguna actividad económica estratégica para el país, que se encuentra sometido a la supervisión de un regulador o fiscalizador sectorial.

Servicios esenciales: Todo servicio, prestado por el Estado o por empresas privadas, respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción, no disponibilidad o destrucción de su infraestructura de la información pueda afectar gravemente: la vida o integridad física de las personas; la provisión de servicios sean estos: sanitarios, de seguridad, energéticos, de suministro de agua, educativos o de telecomunicaciones; y al normal funcionamiento de infraestructura vial y medios de transporte; a la generalidad de personas usuarias o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; o de modo general, el normal desarrollo y bienestar de la población.

Sistema informático o Sistema de información: Todo sistema, dispositivo, equipo, red o activo aislado o el conjunto de ellos, interconectados o relacionados entre sí, incluidos sus soportes lógicos, cuya función, o la de alguno de sus elementos, sea la recogida, el almacenamiento, la utilización, el intercambio, la difusión, la transmisión, la eliminación o, en general, el tratamiento de información, en ejecución de un programa.

Transformación digital: La transformación digital es el proceso de sustitución total de métodos manuales, tradicionales y heredados de hacer negocios con las últimas alternativas digitales. Este tipo de reinvención toca todos los aspectos de un negocio, no solo la tecnología.

Vulnerabilidad de seguridad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

10. REFERENCIAS BIBLIOGRÁFICAS

APC. (2022). *A Framework for Developing Gender-Responsive Cybersecurity Policy - Norms, Standards and Guidelines.* Obtenido de https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf

APC. (2023). *What is a gender approach to cybersecurity?* Obtenido de https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-approach-cybersecurity

CEPAL. (2022). *Digitalización de las mujeres en América Latina y el Caribe. Acción urgente para una recuperación transformadora y con igualdad.* Obtenido de https://repositorio.cepal.org/bitstream/handle/11362/47940/4/S2200375_es.pdf

CGR. (2023). *Opiniones y sugestiones: Emergencia Cibernética: obstáculo para la transformación digital y el bienestar social; retroceso para la transparencia y la rendición de cuentas*. Obtenido de https://sites.google.com/cgr.go.cr/rchp/ma2022/dfoe-cap-os-00001-2023?authuser=0

CHATHAM HOUSE. (2023). *Understanding gender and cybersecurity*. Obtenido de https://www.chathamhouse.org/about-us/our-departments/international-security-programme/understanding-gender-and-cybersecurity

CNE. (2022). *Plan General de la Emergencia Ciberataques.* Obtenido de https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

e-Governance Academy. (2023). *National Cyber Security Index Project.* Obtenido de https://ncsi.ega.ee/ncsi-index/

FORTINET. (2022). *2022 Cybersecurity Skills Gap - Global Research Report.* Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

FORTINET. (2023). *Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022*. Obtenido de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

GARTNER. (2023). *Top Strategic Cybersecurity Trends for 2023*. Obtenido de https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023

GCSCC. (2023). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Obtenido de https://gcscc.ox.ac.uk/the-cmm

GFCE. (2023). *Gender and Cybersecurity: creating a more inclusive digital world*. Obtenido de https://thegfce.org/initiatives/gender-and-cybersecurity-creating-a-more-inclusive-digital-world/

GPD. (2023). *New Guide to Fostering Inclusive Cyber Norm Processes*. Obtenido de https://www.gp-digital.org/news/gpd-unveils-new-guide-to-fostering-inclusive-cyber-policymaking-processes/

IBM. (2023). *Cost of a Data Breach Report 2023.* Obtenido de https://www.ibm.com/reports/data-breach

INAMU. (2018). *Política nacional para la atención y la prevención de la violencia contra las mujeres de todas las edades Costa Rica 2017-2032.* Obtenido de https://planovicr.org/sites/default/files/documentos/planovi_2017-2032_diagramada_2019_0.pdf

INTERPOL. (2022). *2022 INTERPOL Global Crime Trend Report.* Obtenido de https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

LA NACION. (2023). *Expertos advierten sobre riesgos de ciberataques en Costa Rica: ¿cómo defendernos?* Obtenido de https://www.nacion.com/brandvoice/ecosistema/expertos-advierten-sobre-riesgos-de-ciberataques/ESXEPRYA2BAQ3D5PO442XXYMTY/story/

MCKINSEY. (2023). *Technology Trends Outlook 2023.* Obtenido de https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#/

MICITT. (2017). *Un acercamiento a la brecha digital de género en Costa Rica.* Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/04/un-acercamiento-a-la-brecha-digital-de-genero.pdf

MICITT. (2019). *Indice de Brecha Digital IDB 2016-2018* . Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/04/indice_de_brecha_digital_2016-2018_0.pdf

MICITT. (2021). *Revision de la Estrategia Nacional de Ciberseguridad de Costa Rica 2017.* Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/05/Revision-de-la-Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-2017.pdf

MICITT. (2023). *Estrategia de Transformación Digital 2023-2027 de Costa Rica.* Obtenido de https://www.micitt.go.cr/wp-content/uploads/2023/06/ETD-2023-2027-CONSULTA-PUBLICA-02-06-2023.pdf

MIDEPLAN. (2016). *Manual de Planificación con Enfoque para Resultados.* Obtenido de https://documentos.mideplan.go.cr/share/s/Tc1cuf30TOWL8_jBSxdI8Q

MIDEPLAN. (2017a). *Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de los productos de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación, 2018-2027.* Obtenido de https://repositorio-snp.mideplan.go.cr/handle/123456789/92

MIDEPLAN. (2017b). *Guía sobre el enfoque de igualdad de género y derechos humanos.* Obtenido de https://documentos.mideplan.go.cr/share/s/UWG8czewS5-A8GJsx8xBCw

MIDEPLAN. (2018a). *Guia de la Teoría de la Intervención.* Obtenido de https://documentos.mideplan.go.cr/share/s/3hKUn5b6Q5mjqaTeZoKQyg

MIDEPLAN. (2018b). *Guía de Indicadores - Orientaciones básicas para su elaboración.* Obtenido de https://documentos.mideplan.go.cr/share/s/Iny9wiulTiy3QZdWrvq0ew

MIDEPLAN. (2023a). *Plan Nacional de Desarrollo y de Inversión Pública 2023-2026.* Obtenido de https://sites.google.com/expedientesmideplan.go.cr/pndip-2023-2026/pagina_principal

MIDEPLAN. (2023b). *Lineamientos para incorporar la Planificación Prospectiva Estratégica en el Sistema Nacional de Planificación (SNP).* Obtenido de https://documentos.mideplan.go.cr/share/s/Lfq4MTVVQkiEKClspayHuw

OEA & BID. (2020). *Observatorio de la Ciberseguridad en America Latina y el Caribe.* Obtenido de https://observatoriociberseguridad.org/#/home

OEA & ONU Mujeres. (2021). *Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belem Do Pará.* Obtenido de https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf

OEA. (2021). *Ciberseguridad de las mujeres durante la pandemia de COVID-19: Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital.* Obtenido de https://www.oas.org/es/mesecvi/docs/Ciberseguridad_COVID_esp.pdf

OEA. (2023). *Report on Cybersecurity Workforce Development in an Era of Talent and Skills Shortages.* Obtenido de https://www.oas.org/en/sms/cicte/docs/Report_Cyber_WorkForce_Development_in_an_Era_of_Talent_and_Skills_Shortages.pdf

PARLAMENTO EUROPEO. (2023). *Ciberseguridad: amenanzas principales y emergentes*. Obtenido de https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_es.pdf

SEMINARIO UNIVERSIDAD. (2023). *Delitos informáticos en Costa Rica se sextuplican en cinco años y desbordan a policía*. Obtenido de https://semanariouniversidad.com/pais/delitos-informaticos-en-costa-rica-se-sextuplican-en-cinco-anos-y-desbordan-a-policia/#:~:text=No%20se%20trata%20%C3%BAnicamente%20de,cinco%20a%C3%B1os%20(ver%20gr%C3%A1fico).

SULA BATSU & GPD. (2023). *Normativa a contemplar para un adecuado abordaje desde los derechos humanos de la ciberseguridad en Costa Rica*. Obtenido de https://www.yumpu.com/es/document/read/68368596/normativa-a-contemplar-abordaje-de-derechos-humanos-en-ciberseguridad-en-costa-rica

SUTEL. (2023). *Estadísticas del sector de telecomunicaciones.* Obtenido de https://www.sutel.go.cr/sites/default/files/informe_estadisticas_del_sector_de_telecomunicaciones_costa_rica_2022.pdf

UIT. (2023). *Global Cybersecurity Index (GCI)*. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

UNIDIR. (2023). *Gender and Disarmament*. Obtenido de https://unidir.org/programmes/gender-and-disarmament

WEF. (2022). Global Gender Gap Report 2022. Obtenido de https://www.weforum.org/reports/global-gender-gap-report-2022/

WEF. (2023a). *Global Gender Gap Report 2023.* Obtenido de https://www3.weforum.org/docs/WEF_GGGR_2023.pdf

WEF. (2023b). *Global Cybersecurity Outlook 2023.* Obtenido de https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

ANEXO 1

Recomendaciones respecto de la implementación de la Estrategia Nacional de Ciberseguridad 2017-2021 presentadas por MICITT con apoyo de OEA & Cyber4Dev

Recomendación de MICITT con apoyo de OEA & Cyber4Dev	Tipo de medidas
Asignar responsabilidades y un **marco de gobernanza** que promueva la coordinación público-privada.	Medidas organizacionales
Considerar la creación de un **organismo de coordinación de alto nivel** a nivel gubernamental (por ejemplo, Consejo Nacional de Ciberseguridad)	
Generar concientización entre los jefes de entidades gubernamentales sobre el posible impacto que los incidentes de ciberseguridad pueden tener en sus operaciones con el fin de **asignar los recursos** adecuados para abordar las vulnerabilidades de respuesta a incidentes.	
Desarrollar una **estrategia de comunicación** en la que incluya planificación para informar a los departamentos y agencias gubernamentales, las empresas y la sociedad civil sobre iniciativas relevantes	
Incluir un **plan de acción** de alto nivel sobre cómo alcanzar los objetivos deseados, así como **indicadores** con los que medir los logros.	
Establecer un grupo de trabajo específicamente para analizar el **marco legal** y las brechas que deben abordarse a nivel nacional y considerar la posición nacional del Gobierno de Costa Rica al abordar la investigación del delito cibernético tanto dentro como fuera de su jurisdicción, especialmente en lo que se refiere a la investigación y cooperación entre jurisdicciones.	Medidas normativas
Tomar medidas adecuadas que permitan generar la visibilidad del mandato legal del **CSIRT-CR** como coordinador nacional en gestión y respuesta a incidentes de ciberseguridad.	Medidas técnicas
Definir claramente la **Infraestructura de Información Crítica** (IIC).	
Realizar un mapeo de forma horizontal y vertical basado en la independencia intersectorial de la Infraestructura de Información Crítica (CII) de Costa Rica.	
Promover la coordinación entre autoridades para garantizar pruebas y evaluaciones periódicas de las infraestructuras crítica, los **servicios esenciales** y la red gubernamental.	
Diseñar mecanismos para el seguimiento y actualizaciones regulares de la lista de elementos y proveedores de la infraestructura crítica.	
Establecer una metodología común de evaluación de los riesgos de ciberseguridad, evaluaciones periódicas de los riesgos en los sectores, un repositorio de riesgos, un registro de incidentes de ciberseguridad y un informe obligatorio	
Desarrollar **estándares** específicos a cada industria a nivel nacional y establecer campañas de sensibilización, así como talleres para su implementación.	
Abordar la administración de **crisis cibernéticas**, la planificación de contingencias y recuperación ante desastres, y los ejercicios de ciberseguridad.	
Informes periódicos de Análisis de Riesgos y Panorama de Amenazas tanto para el sector público como para el privado.	
Desarrollo de **planes de gestión de incidentes de ciberseguridad** a gran escala como parte de la planificación nacional de emergencia.	
Incrementar y fortalecer la **fuerza laboral** de ciberseguridad.	Medidas de fortalecimiento de capacidades
Desarrollar e incluir programas básicos de **educación en ciberseguridad** para cada nivel educativo.	
Mapear los cursos en ciberseguridad y centralizar el acceso de la información respecto a **ofertas académicas** de profesionalización, así como promover este recurso a nivel nacional.	
Desarrollar, socializar y visibilizar las campañas nacionales de **concientización** al sector público y al público en general, especialmente grupos poblacionales en condición de vulnerabilidad.	
Llevar a cabo acuerdos de **cooperación** con academia y comunidad técnica,	Medidas de cooperación

Fuente: Elaboración propia (2023) a partir (MICITT, 2021)

ANEXO 2.

Recomendaciones respecto de la declaración de estado de emergencia en 2022 presentadas por la Contraloría General de la República

Recomendación de la CGR	Tipo de medidas
Modernizar el **modelo de gobernanza** de la ciberseguridad para consolidar una instancia coordinadora que supervise y gestione de manera efectiva las medidas y prácticas de seguridad de la información y para el desarrollo de una capacidad colectiva que involucre a las instituciones públicas, la sociedad civil, el sector privado, los organismos internacionales y otras partes interesadas.	Medidas organizacionales
No eliminar o reducir las inversiones en ciberseguridad que se realizan desde el Presupuesto de la República y procurar la **habilitación de recursos financieros** de contingencia que permitan dar una respuesta efectiva ante posibles ataques cibernéticos que se materialicen en el futuro.	
Revisar, modernizar y adaptar el **marco normativo** para gestionar los riesgos asociados a la seguridad de la información considerando la ciberseguridad y la definición de estándares mínimos de prácticas para las instituciones públicas.	Medidas normativas
Priorizar la seguridad de la **infraestructura crítica** definiendo en forma precisa cuál es la infraestructura crítica nacional, tanto a nivel del sector público como privado, así como cuales son los mecanismos de protección indispensables que se requieren, para que las instituciones involucradas establezcan la hoja de ruta correspondiente.	Medidas técnicas
Fortalecer la **gestión de riesgos** para identificar y priorizar los activos críticos, la infraestructura crítica y la valoración periódica de riesgos de ciberseguridad. También para asignar recursos y esfuerzos en la protección de aquellos que presenten un mayor nivel riesgo, maximizando así el retorno de la inversión en términos de beneficios económicos y sociales.	
Fortalecer la cultura de ciberseguridad mediante el desarrollo de la **concientización** del personal acerca de la relevancia de la ciberseguridad en el manejo y custodia de la información y la continuidad de los servicios.	Medidas de fortalecimiento de capacidades
Adoptar un enfoque **colaborativo**, en el cual se creen espacios para el aprendizaje conjunto, la socialización de buenas prácticas, compartir experiencias exitosas y el desarrollo de un ecosistema articulado acorde con las necesidades de la institucionalidad.	Medidas de cooperación

Fuente: Elaboración propia (2023) a partir de (CGR, 2023)