Stiftung Neue Verantwortung

Material de base para el ejercicio

Costa Rica

Perfil del País

Puntos de contacto: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

Advertencia:

Descargo de responsabilidad: La investigación solo representa la política de ciberseguridad de un país de forma limitada y no es un análisis o evaluación profunda o completa de la política actual. Para adaptar los ejercicios a países concretos, es importante comprender las líneas generales de las políticas de ciberseguridad de otros países. Nuestro equipo, por lo tanto, investiga la información disponible públicamente sobre las políticas de ciberseguridad de los países para adaptar los ejercicios a las necesidades específicas de cada país. La investigación se comparte con los participantes como material de base para preparar el ejercicio. Por lo tanto, los documentos tienen una indicación de tiempo y contemplan la política hasta la fecha de publicación. Para evitar el ánimo de lucro, hemos decidido poner a disposición del público los antecedentes de la investigación. Si utiliza este material, incluya el descargo de responsabilidad. Tampoco dude en ponerse en contacto con nosotros.

Esta investigación ha sido posible gracias al apoyo financiero de la Konrad-Adenauer-Stiftung Costa Rica.

Puntos de contacto:

Rebecca Beigel

Gerente de Proyecto para la Política de Ciberseguridad Internacional

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Gerente de Proyecto Junior para la Política de Ciberseguridad Internacional

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Apoyo a la investigación:

Christina Rupp

Estudiante asistente para la Política de Ciberseguridad Internacional

crupp@stiftung-nv.de

índice de contenidos

Sistema político y antecedentes sociopolíticos

Hechos clave

- Nombre oficial del país: República de Costa Rica, la capital es San José.[1]
- Población: la población es de aproximadamente 5,15 millones de personas (2021).[2]
- Idioma oficial: Español.[3]
- Moneda: colón de Costa Rica.[4]

Sistema politico

- Forma de gobierno: República presidencial democrática.[5]
  - Jefe de estado y gobierno: Carlos Alvarado Quesada, Presidente de la República de Costa Rica desde mayo del 2018, miembro del Partido Acción Ciudadana (PAC).[6]
    - Según el Artículo 139 de la constitución de Costa Rica, El presidente está facultado, entre otras cosas, para nombrar y destituir a los ministros del gabinete, así como para actuar como comandante en jefe de las fuerzas del orden.[7]
    - El gobierno de Costa Rica está conformado por 21 ministerios.[8] La principal entidad gubernamental de Costa Rica encargada de desarrollar, coordinar y aplicar la política nacional de ciberseguridad es el Ministerio de Ciencias, Tecnología y Telecomunicaciones (MICITT), dirigido por la ministra Paola Vega Castillo (en la sección 2.3 se puede encontrar más información sobre el MICITT).
- Legislatura: consiste de una asamblea legislativa unicameral (La Asamblea Legislativa).[9]

Desde 1948, la constitución de Costa Rica no contempla mantener una fuerza militar permanente. Desde entonces la responsable de las acciones defensivas es la Fuerza Pública de la República de Costa Rica.[10]

Contexto socio-político

Muchos comentaristas describen a Costa Rica como un "bastión de estabilidad política y económica en una región a menudo turbulenta"[11] o " "historia de éxito de desarrollo".[12] Estas evaluaciones se basan, entre otros, en la condición de Costa Rica de:

- país de ingreso medio,
- una de las tasas de pobreza más bajas de Latinoamérica (10.6%, 2019[13]),
- crecimiento económico (un crecimiento promedio del PIB de 4.13% anual 2000-2019[14]),
- así como un enfoque temprano en las políticas medioambientales.[15]

Reporteros Sin Fronteras se refiere a Costa Rica como el país latinoamericano "con el mejor historial en respeto a los derechos humanos y la libertad de expresión" [...y] notable excepción en una región caracterizada por la corrupción, los delitos violentos y la violencia constante contra los medios de comunicación"[16], que está respaldado por su muy alta ubicación en el Índice Mundial de Libertad de Prensa 2021 (5to lugar de un total de 180 países).[17]

En el Informe de Competitividad Global del Foro Económico Mundial del 2019, la Adopción de Tecnologías de Comunicación por Internet (TICs) de Costa Rica ocupa el puesto 63 de 141 países.

- En 2019, aproximadamente el 81.2% de los adultos usaba Internet.[18]
- El informe evaluó además un nivel de 97,2 suscripciones de banda ancha móvil y 16,6 fijas por cada 100 personas en Costa Rica.[19]
- En cuanto a las competencias digitales de su actual mano de obra, Costa Rica ocupa el puesto 33 a nivel mundial.[20]
- Entre 2020 y 2021, el "número de usuarios de internet en Costa Rica aumentó en 397.000 (+ 11%)".[21]

Si se compara con otros países latinoamericanos, la desigualdad de ingresos en Costa Rica es elevada, con un índice de Gini de 48,2 (2019).[22]

Desde mayo de 2021, Costa Rica es miembro de la Organización para la Cooperación y el Desarrollo Económico (OCDE).[23]

La pandemia de COVID-19 plantea retos socioeconómicos a los logros alcanzados por Costa Rica en el pasado. En el año 2020, se observa que su PIB ha disminuido en un 4,6%, su tasa de pobreza ha aumentado al 13%, y en el cuarto trimestre del año, su tasa de desempleo ha aumentado al 20%.[24]

Panorama de vulnerabilidad y amenazas

En los últimos años, se sabe que Costa Rica ha sido víctima de múltiples operaciones e intrusiones cibernéticas. Para el primer semestre del 2020, la firma de ciberseguridad Fortinet reportó la detección de "más de 51 millones de ataques informáticos contra sistemas y dispositivos institucionales, empresariales y personales [...] en Costa Rica".[25] Este elevado número está relacionado con nuevos vectores de intrusión estrechamente vinculados a la pandemia de COVID 19, como el aumento del trabajo a distancia o los informes sobre la aplicación de ransomware COVIDLock, que afirma a ayudado a mitigar la propagación del virus mediante el suministro de mapas interactivos.[26]

Al echar un vistazo a los incidentes cibernéticos conocidos públicamente antes de COVID, se hace evidente que particularmente las instituciones financieras y los sitios web del gobierno parecen constituir objetivos deseados y frecuentemente explotados en Costa Rica.

La empresa de ciberseguridad Kaspersky sitúa a Costa Rica en el quinto puesto en cuanto a la mayor proporción de usuarios afectados por amenazas financieras a nivel mundial.[27] Un informe de prensa sugiere además que el sistema bancario costarricense es el principal objetivo de los delincuentes cibernéticos en Costa Rica[28]. Los casos conocidos de robo financiero por medios cibernéticos en Costa Rica provienen tanto de actores estatales como no estatales.

- En 2020, se reveló que entidades del sector privado costarricense han estado entre las presuntas víctimas de una operación atribuida al Grupo Lazarus con vínculos con el régimen norcoreano, que ha apuntado a los cajeros automáticos "manipulando el software de procesamiento de transacciones para iniciar retiros de efectivo fraudulentos"[29].

- Además, autores no estatales desconocidos, que operan mediante el uso del ransomware Maze, han podido acceder a las redes del banco estatal costarricense Banco BCR en 2019 y 2020, lo que les ha permitido robar un conjunto de datos que contiene, entre otros, 11 millones de datos de tarjetas de crédito.[30] La primera intrusión tuvo lugar en agosto de 2019. Entonces el grupo de ransomware Maze no se abstuvo de cifrar archivos y dispositivos porque según ellos "el posible daño era demasiado"[31]. En 2020, el mismo grupo volvió a acceder al sistema del BCR tras comprobar que el banco no había asegurado su red tras su primera operación. En mayo de 2020, el grupo de ransomware Maze afirmó públicamente que no vendería los datos de los usuarios ni utilizaría sus credenciales para adquirir dinero, sino que intentaría "alertar a la gente y a las instituciones financieras sobre la escasa seguridad"[32]. El grupo amenazó además con publicar este conjunto de datos si no recibía información sobre los elementos de seguridad informática recién instalados por parte del BCR. Ante la falta de respuesta del BCR, el grupo de ransomware Maze publicó de forma continuada filtraciones de los datos adquiridos y amenazó además con exponer información sobre los métodos de procesamiento y la estructura de la red del BCR.[33]

- El Grupo Silencio puso en riesgo otras entidades financieras del sector financiero de Costa Rica en agosto de 2019 y en enero de 2018[34].

En los últimos años, muchas entidades gubernamentales costarricenses también han sido objeto de operaciones cibernéticas.

- Más recientemente, en abril de 2021, se reveló que cerca de 4.500 contraseñas asociadas a direcciones de correo electrónico de organismos gubernamentales de Costa Rica estaban entre los 3.000 millones de credenciales publicadas de la filtración Compilation of Many Breaches (COMP) o Compilación de muchas brechas.[35]
- En 2018, el grupo paquistaní Pak Monster Cyber Thunders habría sido capaz de hacer caer los sitios web de, entre otros, la **Presidencia de la República de Costa Rica**, el **Ministerio de Ambiente y Energía** (MINAE), el **Ministerio de Seguridad Pública de Costa Rica** (MSP), el **Organismo de Investigación Judicial** (OIJ), así como de múltiples municipalidades.[36] Los informes sospechan que hay un motivo político detrás del incidente y lo perciben como una posible "respuesta a la salida de Estados Unidos del acuerdo nuclear"[37] (en referencia al Plan de Acción Integral Conjunto), entre otros.

Otras operaciones en el pasado han tenido como objetivo y, en consecuencia, han comprometido una página web interna del **MINAE** en diciembre de 2015[38], la página web del **Ministerio de Relaciones Exteriores y Culto** (MREC) de Costa Rica en marzo de 2019[39], así como la página web de la **Dirección General de Migración y Extranjería** (DGME) de Costa Rica en febrero de 2020.[40]

Política de ciberseguridad de Costa Rica

Política de ciberseguridad

Según el Índice de Ciberseguridad Global (ICG) 2020, Costa Rica ocupa el octavo lugar en la región de las Américas, compuesta por 35 países, en cuanto a su compromiso con la política de ciberseguridad.[41] El ICG es calculado por la Unión Internacional de Telecomunicaciones (UIT) sobre la base de cinco pilares que contienen, por ejemplo, medidas legales o cooperación internacional. A nivel mundial, Costa Rica ocupa el puesto 76 de 182 países.[42]

Los intereses y las políticas de Costa Rica sobre el ciberespacio están definidos principalmente por su **Estrategia Nacional de Ciberseguridad**[43]. La estrategia fue adoptada en 2017 como marco orientador de las actividades del país y fue desarrollada con el apoyo de la Organización de Estados Americanos (OEA). La estrategia fue aprobada en 2017 como marco orientador de las actividades del país y fue elaborada con el apoyo de la Organización de Estados Americanos (OEA).[44] Actualmente, Costa Rica está en proceso de evaluación y actualización de su Estrategia Nacional de Ciberseguridad.[45]

La estrategia pretende orientar la actuación del país en materia de seguridad en el uso de las TIC, fomentar la coordinación y la cooperación entre las distintas partes interesadas, así como promover medidas de educación, prevención y mitigación en relación con el uso de las TIC para conseguir un entorno más seguro y fiable para sus ciudadanos.[46]

Los principales principios definidos de la estrategia y por tanto de la política de ciberseguridad de Costa Rica son:

1. un enfoque centrado en el ser humano
2. respeto por los derechos humanos y la privacidad
3. necesidad de coordinación y corresponsabilidad de las partes interesadas
4. participación en la cooperación internacional.

De conformidad, los objetivos políticos del país en el ámbito de la ciberseguridad son:

- Incrementar la coordinación nacional mediante la asignación de un coordinador nacional (ubicado en el MICITT), que no solo se encargue de coordinar las acciones, sino también de vigilar el cumplimiento en la implementación de la estrategia y las colaboraciones público-privadas continuas[47];
- Implementar campañas públicas de sensibilización y educación en ciberseguridad entre los ciudadanos costarricenses, el sector público y los funcionarios públicos, así como en las micro, pequeñas y medianas empresas[48];

- Impulsar la creación de capacidades nacionales en materia de ciberseguridad mediante la realización de formación para el sector público con el fin de apoyar una cultura de ciberseguridad, compartir las mejores prácticas y participar en alianzas con las universidades para fomentar la investigación y el desarrollo[49];
- Reforzar el marco jurídico de la ciberseguridad y las TIC mediante la consolidación del marco aplicable a la ciberdelincuencia, la creación de las capacidades respectivas para la aplicación de la ley y el fomento del intercambio de información en el ámbito de la justicia penal[50];
- Proteger las infraestructuras críticas, entre otras cosas, identificándolas, adoptando una clasificación de infraestructuras críticas y promoviendo mecanismos así como políticas públicas para su protección, que incluyan también la ejecución de medidas de seguridad para los sistemas de información y telecomunicaciones de la Administración Pública[51];
- Promover la gestión de riesgos, por ejemplo, fortaleciendo el Equipo Costarricense de Seguridad Informática y Respuesta a Incidentes, estableciendo una red de intercambio de información para las entidades gubernamentales y definiendo requisitos mínimos de seguridad de la información en el sector financiero[52];
- Participar en la cooperación internacional, por ejemplo, mediante la asistencia mutua y la colaboración en materia penal, técnica y educativa[53];
- Comprometerse a hacer un seguimiento y evaluar la aplicación de la estrategia[54].

Además, el gobierno costarricense ha publicado un **Plan Nacional de Desarrollo de las Telecomunicaciones** (PNDT) para los años 2015-2021, que contribuirá a perfilar la visión de Costa Rica en 2021 como una "sociedad conectada, basada en un enfoque integral sobre el acceso, uso y apropiación de las tecnologías de la información y la comunicación, de forma segura, responsable y productiva".[55]

Marco legal

En Costa Rica, la **Ley General de Telecomunicaciones**, No. 8642, 2008[56], así como la **Ley para el Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones**, No. 8660, 2008[43] así como la **Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones** (Nº 8660, 2008)[57] constituyen el marco regulatorio del país en materia de Telecomunicaciones. Entre otras cosas, designan al MICITT como ente rector principal y establecen la Superintendencia de Telecomunicaciones (SUTEL), autoridad reguladora que garantiza la protección de los derechos de los usuarios y la universalización de los servicios.[58]

Otra ley reguladora de importancia para el ámbito de la ciberseguridad y la ciberdelincuencia en Costa Rica es el **Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales** (Nº 37554, 2012)[59], que ha creado la Agencia de Protección de Datos de los Habitantes (PRODHAB).

El marco jurídico nacional de Costa Rica que facilita la persecución e investigación de los delitos cibernéticos se centra en su **Código Penal** (nº 4573) y en la **Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones** (nº 7425, 1994)[60].

En la última década, el código penal del país se modificó a través de la Ley Nº 9048 (2012)[61] y la Ley Nº 9135 (2013)[62], permitiendo la inclusión de "nuevos tipos de delitos [...] entre los que se encuentran los cometidos mediante el uso de sistemas y tecnologías informáticas"[63] y, por tanto, "introduciendo formalmente la ciberdelincuencia en el código penal del país"[64] Entre otros, prohíben la "instalación y difusión de programas informáticos y códigos maliciosos en ordenadores, sistemas de información y servidores" (Art. 232 Código Penal) o el "phishing y la usurpación de sitios web de Internet y la obtención de información confidencial de personas físicas y jurídicas con fines de lucro propio para el beneficio de terceros" (Art. 233 Código Penal)[65].

Además, Costa Rica ratificó el **Convenio de Budapest sobre la Ciberdelincuencia** (Tratado n.º 185) en 2017 tras finalizar el proceso de adhesión designado.[66] El Convenio de Budapest es el primer tratado internacional que persigue una política penal común mediante la cooperación y la adopción de legislación contra la ciberdelincuencia.[67] La convención, entre otras cosas, obliga a las entidades firmantes a adoptar una legislación que penalice las distintas formas de ciberdelincuencia y posibilite la investigación de los delitos relacionados con el ciberespacio.[68]

Arquitectura de ciberseguridad - Instituciones seleccionadas

Varios actores gubernamentales trabajan en la mejora de la ciberseguridad en Costa Rica. La mayoría de ellos se encuentran institucionalmente en el ámbito del **Ministerio de Ciencia, Tecnología y Telecomunicaciones** (MICITT) de Costa Rica.

El **Ministerio de Ciencia, Tecnología y Telecomunicaciones** (MICITT) constituye la principal entidad gubernamental de Costa Rica encargada de desarrollar, coordinar e implementar la política de ciberseguridad del país.[69] El MICITT alberga al Coordinador Nacional de Ciberseguridad, así como al Equipo de Seguridad Informática y Respuesta a Incidentes del país (CSIRT-CR). Además, la Estrategia Nacional de Ciberseguridad encomendó al MICITT la creación de un Consejo Asesor de Ciberseguridad interdepartamental y multisectorial, que, entre otras cosas, elaborará planes de acción para cada uno de los objetivos de la estrategia.

El Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) de Costa Rica se constituyó en 2012 dentro del MICITT como "organismo encargado de coordinar todo lo relacionado con los temas de seguridad informática y cibernética"[70]. Cuando se redactó la estrategia nacional de ciberseguridad, se describió que las tareas del CSIRT-CR se centraban principalmente en las medidas de creación de capacidades en el sector público y en la concienciación. Además, el Decreto de creación del CSIRT-CR nº 37052- MICIT[71] también le otorgó autoridad para crear un equipo de expertos encargado de "prevenir y responder

a los incidentes cibernéticos contra las instituciones gubernamentales"[72]. En julio de 2018 se acordó un protocolo nacional de gestión de incidentes de ciberseguridad.[73] El CSIRT-CR está compuesto por los jefes de los ministerios nacionales seleccionados y supervisa la Dirección de Gobernanza Digital del MICITT.[74]

Las investigaciones relacionadas con el cibercrimen y la tecnología en Costa Rica se llevan a cabo principalmente dentro de una **Sección Especializada contra el Cibercrimen en el Organismo de Investigación Judicial** (OIJ), que está subordinada a la Corte Suprema de Justicia de Costa Rica. La Sección Especializada contra el Cibercrimen fue creada en 1997 y se le sumó una Sección de Delitos Informáticos en 2004[75]. En su totalidad, la división es capaz de llevar a cabo investigaciones a partir de la recolección de pruebas y métodos de análisis forense[76].

En 2010, se creó una **Comisión Nacional de Seguridad en Línea** (CNSL) mediante el Decreto nº 36274-MICIT[77] bajo la dirección del MICITT. Se encarga de "diseñar las políticas necesarias para el buen uso de Internet y las Tecnologías Digitales" y de establecer un Plan Nacional de Seguridad en Línea[78].

La Estrategia Nacional de Ciberseguridad encomendó al MICITT convocar un **Comité Consultivo en Ciberseguridad** en los tres meses siguientes a la publicación de la estrategia. Está integrado por representantes del MICITT, el Poder Judicial, la SUTEL, así como representantes de la sociedad civil, la academia y el sector privado.[79] La Junta Consultiva tiene el mandato de ser la entidad responsable de la operatividad de la Estrategia Nacional de Ciberseguridad de Costa Rica. Junto con el Coordinador Nacional de Ciberseguridad del MICITT, la Junta Asesora es responsable de "disponer todas las acciones necesarias para iniciar el proceso de implementación, con planes de acción para cada uno de los objetivos propuestos en esta estrategia"[80] a partir de una definición previa de objetivos, plazos y actores responsables. Su primera reunión tuvo lugar en enero de 2018.[81] En marzo de 2019, el MICITT y el Consejo Asesor de Ciberseguridad lanzaron una Campaña Nacional de Alfabetización en Seguridad de la Información.[82]

Tras el ataque a los sitios web del gobierno costarricense en mayo de 2018 por parte de un grupo pakistaní, el gobierno de Costa Rica decidió establecer una **Red de Enlaces de Ciberseguridad**, que comenzó su trabajo en julio de 2018.[83] Se creó como un mecanismo que permite conectar a los responsables de la ciberseguridad de las instituciones del sector público y facilita la coordinación en materia de seguridad de la información en general, pero también en materia de incidentes. El CSIRT-CR comunica a la red alertas periódicas sobre vulnerabilidades, así como información relacionada con incidentes.[84] Está integrado por un grupo de expertos del MICITT, el OIJ, el Ministerio de Seguridad Pública (MSP), la Dirección de Inteligencia y Seguridad Nacional (DIS), el Instituto Costarricense de Electricidad (ICE) y el NIC Costa Rica. Está integrado por un grupo de expertos del MICITT, el OIJ, el Ministerio de Seguridad Pública (MSP), la Dirección de Inteligencia y Seguridad Nacional (DIS), el Instituto Costarricense de Electricidad (ICE) y NIC Costa Rica.[85] En el pasado, también asistieron a las reuniones representantes del Instituto de Fomento y Asesoría Municipal (IFAM), de la Agencia de Protección de datos de los Habitantes (PRODHAB), así como del Centro de Información de la Red de América Latina y el Caribe (LACNIC).[86]

Cooperación bilateral y multilateral

Costa Rica es un Estado miembro de la Organización de Estados Americanos (OEA), de la Unión Internacional de Telecomunicaciones (UIT) y de las Naciones Unidas (ONU).[87] Todas estas organizaciones internacionales tratan y debaten temas relacionados con la ciberseguridad. En el pasado, la OEA ha redactado, entre otras cosas, declaraciones tituladas "Fortalecimiento de la cooperación hemisférica para combatir el terrorismo y promover la seguridad, la cooperación y el desarrollo en el ciberespacio" (2016)[88], "Protección de las infraestructuras críticas frente a las amenazas emergentes"[89]. Además, los Estados miembros de la OEA han acordado un conjunto de medidas de fomento de la confianza (MFC) relacionadas con la cibernética en marzo de 2018.[90] En el ámbito de la ciberseguridad, la OEA también mantiene memorandos de entendimiento con España (2015) y Estonia.[91]

Además, Costa Rica participó en el recientemente concluido primer **Grupo de Trabajo de Composición Abierta (GTCA) sobre los avances en el campo de las TIC en el contexto de la seguridad internacional,** que fue establecido en 2018 bajo los auspicios de la Primera Comisión de la Asamblea General de la ONU. En su informe final[92], el GTCA confirmó la noción de que el derecho internacional y la Carta de la ONU son aplicables en el ciberespacio y que los Estados deben identificar y cooperar voluntariamente en las medidas de fomento de la confianza en sus contextos locales. La aportación de Costa Rica en las sesiones giró, entre otras cosas, en torno a las cuestiones de los derechos humanos y la privacidad, que, a su juicio, deberían constituir el "enfoque del trabajo del grupo".[93] Costa Rica también se encuentra entre los 32 Estados miembros de la **Coalición para la Libertad en Línea** (FOC, por sus siglas en inglés), que busca "coordinar [...] los esfuerzos diplomáticos [de sus miembros] y comprometerse con la sociedad civil y el sector privado para apoyar la libertad de Internet [...] en todo el mundo"[94].

Además de la OEA, Costa Rica participa a nivel regional en la **Red de Gobierno Electrónico de América Latina y el Caribe** (Red GEALC), cuyo objetivo principal es el "apoyo al desarrollo de políticas públicas de gobierno digital".[95] En el marco de la Red GEALC, Costa Rica ha propuesto, por ejemplo, la posteriormente adoptada Declaración de San José[96] noviembre de 2020), que ha incorporado el tema de la ciberseguridad como una línea de trabajo dentro de la red.[97]

El CSIRT-CR está representado en la **Red de CSIRT de las Américas**, así como en **la Alianza de Ciberseguridad para el Progreso Mutuo** (CAMP, por sus siglas en inglés). El CAMP sirve de plataforma de red para mejorar el nivel de ciberseguridad de sus miembros mediante el intercambio de experiencias de desarrollo y tendencias de ciberseguridad.[98]

Asimismo, Costa Rica se encuentra entre los nueve países prioritarios del proyecto **Resiliencia Cibernética para el Desarrollo** (Cyber4Dev), financiado por la UE, cuyo objetivo es, entre otros, aumentar la resiliencia cibernética y la política de ciberseguridad.[99] El Cyber4Dev lo han implementado agencias gubernamentales británicas, holandesas y estonias.[100]

En el marco de su adhesión al Convenio de Budapest, Costa Rica ha sido designada además como uno de los quince "países prioritarios y centrales" del proyecto conjunto **GLACY+** de la Unión Europea (UE) y el Consejo de Europa (CdE). GLACY+ busca "reforzar las capacidades de los Estados de todo el mundo para aplicar la legislación sobre ciberdelincuencia y pruebas electrónicas y mejorar sus capacidades para una cooperación internacional eficaz en este ámbito".[101]

En cuanto a la cooperación bilateral en materia de ciberseguridad, Costa Rica mantiene varios acuerdos con terceros Estados:

- En mayo de 2021 se celebró con el Estado de **Israel** un **Memorando de Entendimiento para la Cooperación en materia de Ciberseguridad** como continuación de un Acuerdo de Cooperación en materia de Cooperación Económica, Cultural, Técnica y Científica celebrado anteriormente. Entre otros, fortalecerá la implementación de la Estrategia de Transformación Digital de Costa Rica y ayudará a digitalizar las instituciones públicas costarricenses.[102]
- En septiembre de 2019, Costa Rica y **Estonia** firmaron un **Memorando de Entendimiento sobre Cooperación en el ámbito del Gobierno Digital y la "Cuarta Revolución Industrial"**. Incluye, entre otras, la formación y el intercambio de experiencias en materia de ciberseguridad, protección de infraestructuras críticas, así como el desarrollo de soluciones eficaces para la economía y el gobierno digital como objetivos mutuos.[103]
- En septiembre de 2017 se celebró un **acuerdo de cooperación con China en materia económica y técnica**. Entre otras cuestiones, se hace referencia a la ciberseguridad como ámbito de actuación prioritario.[104]

Por otra parte, el Ministerio de Relaciones Exteriores de Costa Rica ha informado de las relaciones de cooperación e intercambios en materia de ciberseguridad que se mantienen con representantes gubernamentales de **Austria, Singapur** y **Corea del Sur**.[105]

El CSIRT de Costa Rica recibió el apoyo del **Reino Unido** en materia de formación y asesoramiento entre 2014 y 2015.[106] Además, el personal de la División Especializada en Delitos Cibernéticos del Organismo de Investigación Judicial de Costa Rica ha recibido formación en los **Estados Unidos de América** y **Canadá** en el pasado.[107]

Fuentes

1 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

2 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

3 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

4 Global Exchange: The Costa Rica colon. https://www.globalexchange.es/en/currencies-of-the-world/costa-rica-colon

5 Auswärtiges Amt (2021): Costa Rica: Steckbrief. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/costarica-node/costarica/224814

6 Auswärtiges Amt (2021): Costa Rica: Steckbrief. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/costarica-node/costarica/224814

7 Republic of Costa Rica: Constitution of The Republic of Costa Rica. https://www.wipo.int/edocs/lexdocs/laws/en/cr/cr039en.pdf

8 Presidencia de la República de Costa Rica: El Gabinete. https://www.presidencia.go.cr/autoridades/el-gabinete/

9 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

10 Alejandro Zúñiga (2020): Costa Rica celebrates 72 years without an army. https://ticotimes.net/2020/11/30/costa-rica-celebrates-72-years-without-an-army

11 Congressional Research Service (2021): Costa Rica: An Overview. https://sgp.fas.org/crs/row/IF10908.pdf

12 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

13 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

14 The World Bank (2019): GDP growth (annual %) - Costa Rica. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2019&locations=CR&start=2009&view=chart

15 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

16 Reporters Without Borders: Costa Rica. https://rsf.org/en/costa-rica

17 Reporters Without Borders (2021): 2021 World Press Freedom Index. https://rsf.org/en/ranking

18 The World Bank (2020): Individuals using the Internet (% of population) - Costa Rica. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CR

19 World Economic Forum (2019): The Global Competitiveness Report 2019. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

20 World Economic Forum (2019): The Global Competitiveness Report 2019. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

21 Simon Kemp (2021): Digital 2021: Costa Rica. https://datareportal.com/reports/digital-2021-costa-rica

22 Organisation for Economic Co-Operation and Development (2016): Costa Rica Policy Brief. https://www.oecd.org/policy-briefs/costa-rica-towards-a-more-inclusive-society.pdf

The World Bank (2019): Gini index (World Bank estimate) - Costa Rica. https://data.worldbank.org/indicator/SI.POV.GINI?locations=CR

23 Organisation for Economic Co-operation and Development: OECD welcomes Costa Rica as its 38th Member. https://www.oecd.org/costarica/oecd-welcomes-costa-rica-as-its-38th-member.htm

24 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

25 TCRN Staff (2020): More than 51 Million Attacks by Hackers During the Pandemic in Costa Rica. https://thecostaricanews.com/more-than-51-million-attacks-by-hackers-during-the-pandemic-in-costa-rica/

26 Anastasia Austin (2020): Latin America Under Threat of Cybercrime Amid Coronavirus. https://insightcrime.org/news/analysis/threat-cyber-crime-coronavirus/

27 Kaspersky (2020): Kaspersky Security Bulletin 2020. Statistics. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

28 Julieta Cambronero (2020): Una cuarta parte de ciberataques al sector financiero son únicamente destructivos sin ningún beneficio económico. https://costaricamedios.cr/2020/06/04/una-cuarta-parte-de-ciberataques-al-sector-financiero-son-unicamente-destructivos-sin-ningun-beneficio-economico/

29 Council on Foreign Relations: Targeting of automated teller machines worldwide. https://microsites-live-backend.cfr.org/cyber-operations/targeting-automated-teller-machines-worldwide

30 Carnegie Endowment for International Peace (2021): Timeline of Cyber Incidents Involving Financial Institutions. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

The Tico Times (2020): BCR confirms financial information has leaked after cybercrime group claims to publish private data. https://ticotimes.net/2020/05/24/bcr-confirms-financial-information-has-leaked-after-cyber-crime-group-claims-to-publish-private-data-updated

31 Lawrence Abrams (2020): Hackers say they stole millions of credit cards from Banco BCR. https://www.bleepingcomputer.com/news/security/hackers-say-they-stole-millions-of-credit-cards-from-banco-bcr/

32 Cyble (2020): Maze Ransomware Operators Targets Banco de Costa Rica, One of the Strongest Banking Companies in Both Costa Rica and Central America. https://blog.cyble.com/2020/05/01/maze-ransomware-operators-targets-banco-de-costa-rica-one-of-the-strongest-banking-companies-in-both-costa-rica-and-central-america/

33 Cyble (2020): Maze Ransomware Operators Release the Banco De Costa Rica Data Leak Part 3. https://blog.cyble.com/2020/05/22/maze-ransomware-operators-release-the-banco-de-costa-rica-data-leak-part-3/

Cyble (2020): Maze Ransomware Operators Release the Banco de Costa Rica Data Leak Part 2. https://blog.cyble.com/2020/05/05/maze-ransomware-operators-targets-banco-de-costa-rica-for-the-second-consecutive-time/

34 Carnegie Endowment for International Peace (2021): Timeline of Cyber Incidents Involving Financial Institutions. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

35 Erick Murillo (2021): Se filtran miles de claves de correo electrónicos del Gobierno. https://www.crhoy.com/tecnologia/se-filtran-miles-de-claves-de-correos-electronicos-del-gobierno/

36 Rico (2018): Pakistani Hackers In Massive Attack On Costa Rica Government Websites. https://qcostarica.com/pakistani-hackers-in-massive-attach-on-costa-rica-government-websites/

37 Rico (2018): Pakistani Hackers In Massive Attack On Costa Rica Government Websites. https://qcostarica.com/pakistani-hackers-in-massive-attach-on-costa-rica-government-websites/

38 Cf. Jaime Lopez (2015): Costa Rica Government Website Hacked by Pro-ISIS Group. https://news.co.cr/costa-rica-government-website-hacked-by-pro-isis-group/43541/

39 Cf. RedaQted (2019): Chancellery website suffered a “cyber attack”. https://qcostarica.com/chancellery-website-suffered-a-cyber-attack/

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2019): CSIRT-CR atiende alerta de incidente en Ministerio de Relaciones Exteriores. https://www.micit.go.cr/noticias/csirt-cr-atiende-alerta-incidente-ministerio-relaciones-exteriores

40 Cf. The Tico Times (2021): Immigration services impacted by cybersecurity issue. https://ticotimes.net/2021/02/04/immigration-services-impacted-by-cybersecurity-issue

41 International Telecommunication Union (2021): Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

42 International Telecommunication Union (2021): Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

43 MICITT (2017): Estrategia Nacional de Ciberseguridad de CostaRica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

44 Organization of American States (2015): OAS Supports Costa Rica in Development of a National Cyber Security Strategy. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/15

45 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Este lunes se llevó a cabo el III Encuentro de la Red de Enlaces de Ciberseguridad, como parte de las actividades... [Facebook Status Update]. https://www.facebook.com/micitcr/posts/3747180185292345

46 Ministerio de Planificación Nacional y Política Económica (2020): Ciberseguridad en el Sistema de Planificación Nacional. https://www.hacienda.go.cr/Sidovih/uploads/Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

47 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

48 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

49 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

50 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

51 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

52 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

53 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

54 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

55 Viceministerio de Telecomunicaciones (2015): National Telecommunications Development Plan 2015-2021.
https://www.micit.go.cr/sites/default/files/pndt_2015-2021._english_version_web_1_0.pdf

56 La Asamblea Legislativa De La República De Costa Rica: Ley General de Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63431

57 La Asamblea Legislativa De La República De Costa Rica: Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63786

58 La Asamblea Legislativa De La República De Costa Rica: Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63786

SUTEL (2021): Visión y Misión. https://sutel.go.cr/pagina/vision-y-mision

59 La Presidenta De La República Y El Ministro De Justicia Y Paz (2012): Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC

60 Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (1994).
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRM&nValor1=1&nValor2=16466&strTipM=FN

61 La Asamblea Legislativa De La República De Costa Rica (2012): Law No. 9048.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

62 La Asamblea Legislativa De La República De Costa Rica (2013): Law No. 9135.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&strTipM=TC

63 Council of Europe (2020): Costa Rica.
https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

64 Inter-American Development Bank (2016): Cybersecurity Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report.
https://publications.iadb.org/publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf

65 Council of Europe (2020): Costa Rica.
https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

66 Council of Europe (2021): Chart of signatures and ratifications of Treaty 185.
https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean.
https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

El Presidente De La República Y El Ministro A.L. De Relaciones Exteriores Y Culto (2017): Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001).
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84643&nValor3=109293&param2=1&strTipM=TC&lResultado=1&strSim=simp

67 Council of Europe (2021): Details of Treaty No. 185.
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

68 Council of Europe (2021): Convention on Cybercrime.
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

69 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2021): Ciberseguridad.
https://micit.go.cr/tags/ciberseguridad

70 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

71 La Presidenta De La República Y El Ministro De Ciencia Y Tecnología (2012): N 37052-MICIT. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC

72 Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

73 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

74 Council of Europe (2020): Costa Rica. https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

UNIDIR (2020): Costa Rica. https://unidir.org/cpp/en/states/costarica

75 Organismo de Investigación Judicial: Sección Especializada contra el Cibercrimen. https://sitiooij.poder-judicial.go.cr/index.php/oficinas/departamento-de-investigaciones-criminales/delitos-informaticos

76 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

Organismo de Investigación Judicial (2021): Cibercrimen. https://sitiooij.poder-judicial.go.cr/index.php/component/k2/itemlist/search?searchword=cibercrimen&categories=&__ncforminfo=4RGrTo1JVkmEHCjcxREZI7I5sKm1fcc26tZvrBf2P72qcgo2wXeyted3a1riV3R3styBJIGYXXJGBrK8TIitL1-IPQv9ytGWoXwHdEqfubRgFc-aSNa6DCP8iGAKkYUC

77 MICITT, Nº 36274-MICIT.

78 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

79 Ministerio de Planificación Nacional y Política Económica (2020): Ciberseguridad en el Sistema de Planificación Nacional. https://www.hacienda.go.cr/Sidovih/uploads/Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

80 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

81 Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica (2018): MICITT es sede de primera reunión del Comité Consultivo en Ciberseguridad. https://www.micitt.go.cr/portaldos/index.php?option=com_content&view=article&id=10286:micitt-es-sede-de-primera-reunion-del-comite-consultivo-en-ciberseguridad&catid=40&Itemid=1917

82 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2019): MICITT y Comité Consultivo de Ciberseguridad lanzan Campaña en Seguridad de la Información. https://www.micit.go.cr/noticias/micitt-y-comite-consultivo-ciberseguridad-lanzan-campana-seguridad-la-informacionv

83 Johnny Castro (2018): Costa Rica crea alta comisión de seguridad informática. https://www.larepublica.net/noticia/costa-rica-crea-alta-comision-de-seguridad-informatica

Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

84 Erick Murillo (2021): Se filtran miles de claves de correos electrónicos del Gobierno. https://www.crhoy.com/tecnologia/se-filtran-miles-de-claves-de-correos-electronicos-del-gobierno/

85 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

86 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Este lunes se llevó a cabo el III Encuentro de la Red de Enlaces de Ciberseguridad, como parte de las actividades... [Facebook Status Update]. https://www.facebook.com/micitcr/posts/3747180185292345

87 UNIDIR (2020): Costa Rica. https://unidir.org/cpp/en/states/costarica

88 Organisation of American States (2016): Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace. http://www.oas.org/en/sms/cicte/documents/2016/declaration/cicte%20dec%201%20declaration%20english%20cicte01037e04.pdf

89 Organisation of American States (2015): Protection of Critical Infrastructure from Emerging Threats. https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

90 Organization of American States (2018): Regional Confidence-Building Measures (CBMs) To Promote Cooperation And Trust In Cyberspace. https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multilateral/OAS+Regional+Confidence-Building+Measures+%28CBMs%29+to+Promote+Cooperation+and+Trust+in+Cyberspace+%28Agreed+During+the+First+Meeting+of+the+Working+Group+on+Cooperation+and+Confidence-Building+Measures+in+Cyberspace%2C+Held+on+February+28+-+March+1%2C+2018%29.pdf

91 Theresa Hitchens and Nilsu Goren (2017): International Cybersecurity Information Sharing Agreements. https://www.jstor.org/stable/pdf/resrep20426.pdf?refreqid=excelsior%3Aafff0b1a0413ce710ab5b22e-5ae99fd8

92 Open-ended working groupon developments in the field of information and telecommunications in the context of international security (2021): Final Substantive Report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

93 Digital Watch (2019): 2nd Meeting of the third substantive session of the Open-Ended Working Group (OEWG). https://dig.watch/resources/2nd-meeting-third-substantive-session-open-ended-working-group-oewg

94 Freedom Coalition (2021): Aims and Priorities. https://freedomonlinecoalition.com/about-us/

Freedom Online Coalition (2021): Members. https://freedomonlinecoalition.com/members/

95 Network of e-Government of Latin America and the Caribbean: About Red Gealc. https://www.redgealc.org/sobre-red-gealc/que-es-la-red-gealc/

96 VI Reunión Ministerial y XIV Asamblea anual de laRed de Gobierno Electrónico de América Latina y el Caribe (2020): DECLARACIÓN MINISTERIAL DE SAN JOSÉ 2020. https://www.redgealc.org/site/assets/files/12593/declaracionministerialsj2020.pdf

97 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Países miembros de la Red Gealc firman la Declaración de San José que incorpora el tema de Ciberseguridad propuesto por Costa Rica. https://www.micit.go.cr/noticias/paises-miembros-la-red-gealc-firman-la-declaracion-san-jose-que-incorpora-el-tema

Network of e-Government of Latin America and the Caribbean: Cibersecurity. https://www.redgealc.org/lineas-de-trabajo/ciberseguridad/

98 Cybersecurity Alliance for Mutual Progress: About CAMP. https://www.cybersec-alliance.org/camp/about.do

Cybersecurity Alliance for Mutual Progress: Members. https://www.cybersec-alliance.org/camp/membership.do

Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

99 Cybil (2021): EU Cyber Resilience for Development Cyber4Dev (*GFCE Initiative). https://cybilportal.org/projects/eu-cyber-resilience-for-development-cyber4dev-gfce-initiative/

100 Global Forum on Cyber Expertise: Cyber4Dev. https://thegfce.org/initiatives/cyber4dev/

101 Council of Europe (2021): Global Action on Cybercrime Extended (GLACY)+. https://www.coe.int/en/web/cybercrime/glacyplus

102 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Costa Rica e Israel firman Memorándum de Entendimiento para la Cooperación en Ciberseguridad. https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008

103 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2019): Costa Rica y Estonia firman convenios de cooperación en temas de Gobierno Digital y La Cuarta Revolución Industrial. https://www.micit.go.cr/noticias/costa-rica-y-estonia-firman-convenios-cooperacion-temas-gobierno-digital-y-la-cuarta

104 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2017): Costa Rica recibe al Canciller de la República Popular de China y firma convenio de cooperación económica y técnica. https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=3641

105 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2019): MICITT fortalece alianza con Corea en temas de Ciberseguridad. https://www.micit.go.cr/noticias/micitt-fortalece-alianza-corea-temas-ciberseguridad

Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Costa Rica y Austria sostienen diálogo sobre ciberseguridad. https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=5973

Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Smart Nation: Strategies, Opportunities and Cybersecurity Management. https://www.rree.go.cr/index.php?sec=servicios&cat=becas&cont=579&beca=4613

106 Cybil (2015): Support to Costa Rica's CSIRT. https://cybilportal.org/projects/support-to-costa-ricas-csirt/

107 International Telecommunication Union (2015): Cyberwellness Profile Republic of Costa Rica. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Costa_Rica.pdf