Informe 2021

REVISIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE COSTA RICA (2017)

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

micitt
MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

El presente informe fue elaborado con el apoyo técnico del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA). Las opiniones expresadas en esta publicación corresponden a los autores y no necesariamente las de la Secretaría General de la OEA ni de sus Estados Miembros.

La publicación se realizó con el apoyo financiero del Departamento de Estado Unidos. Las opiniones expresadas en este documento pertenecen a los autores y no reflejan necesariamente las del Departamento de Estado de los Estados Unidos de América.

Adicionalmente, esta publicación contó con la contribución de Cyber4Dev como experto internacional, organización financiada por la Unión Europea.

OEA Más derechos para más gente

CYBER4Dev

ÍNDICE

Resumen Ejecutivo 01

Contexto Actual 02

Marco Nacional de Ciberseguridad 04

Metodología 07

Análisis Situacional 08

Coordinación Nacional 08
- Línea Estratégica 1.1 Coordinador Nacional 08
- Línea Estratégica 1.2 Colaboración del Sector Público y Sector Privado 09
- Nivel de implementación 10

Conciencia Pública 10
- Línea Estratégica 2.1 Concienciación - Público en General 10
- Línea Estratégica 2.2 Sector Público 12
- Línea Estratégica 2.3 Micro, Pequeña y Mediana Empresa 13
- Nivel de implementación 14

Desarrollo de la Capacidad Nacional de Seguridad Cibernética 15
- Línea Estratégica 3.1 Formación de recurso humano especializado 16
- Línea Estratégica 3.2 Investigación y Desarrollo 17
- Nivel de implementación 18

Fortalecimiento del marco jurídico en Ciberseguridad y TIC 19
- Línea Estratégica 4.1 Fortalecer el marco normativo y procesal en ciberdelincuencia 20
- Línea Estratégica 4.2 Crear capacidades en Ciberseguridad para la aplicación de la ley en el sistema penal de justicia 21
- Línea Estratégica 4.3 Fomentar redes de confianza para el intercambio de información entre los socios interesados en el sistema penal de justicia 22
- Nivel de implementación 24

Protección de Infraestructuras Críticas 24
- Línea Estratégica 5.1 Identificación y Clasificación de las Infraestructuras Críticas 24
- Línea Estratégica 5.2 Implementación de medidas de seguridad de los Sistemas de Información y Telecomunicaciones de la Administración Pública 25
- Nivel de implementación 26

Gestión de Riesgo 27
- Línea Estratégica 6.1 Mejorar la seguridad de los productos y servicios vinculados con la seguridad de la información 27
- Línea Estratégica 6.2 Implementación de mejores prácticas y definición de requisitos mínimos de seguridad de la información en el Sector Financiero 28
- Línea Estratégica 6.3 Adopción de medidas de seguridad de referencia 28

Línea Estratégica 6.4 Establecimiento de una red de intercambio de información para las entidades gubernamentales 29
Línea Estratégica 6.5 Fortalecimiento del Centro de Respuesta a Incidentes de Seguridad Informática CSIRT-CR 30
Nivel de implementación 30

Cooperación y Compromiso Internacional 30
Línea Estratégica 7.1 Involucrar a la comunidad internacional en el apoyo de los objetivos de la Estrategia Nacional 30
Nivel de implementación 31

Implementación, Seguimiento y Evaluación 31
Línea Estratégica 8.1 Realizar el seguimiento de la aplicación de la Estrategia Nacional de Ciberseguridad, y evaluar el grado de éxito de cumplimiento de sus objetivos 32
Línea Estratégica 8.2 Realizar una revisión y actualización de la Estrategia Nacional de Ciberseguridad cada dos años o según sea necesario 32
Nivel de implementación 32

Contribución de Expertos 33

Introducción 33

Principios, estructura y objetivos de la estrategia de 2017 34

Recomendaciones 37

Reflexiones Finales 41

Implementación General de la ENC 41

Éxitos 41

Oportunidades 42

Prioridades para la próxima ENC 43

ANEXO I – Resumen Ejecutivo del Estado de Madurez Mibernética de Costa Rica (2016-2020) 44

ANEXO II – Lista de los Actores Principales 47

UNO

Resumen Ejecutivo

La siguiente revisión de la Estrategia Nacional de Ciberseguridad (ENC) de Costa Rica, publicada en 2017, fue liderada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de Costa Rica y contó con el apoyo técnico especializado del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE). Debido a las restricciones de desplazamiento derivadas de la pandemia de COVID-19, la metodología y las fases de trabajo descritas en este documento se desarrollaron de manera remota, optimizando herramientas en línea, facilitando la consulta y los aportes recibidos de las partes interesadas.

El análisis presentado en este informe está basado en la recopilación de información obtenida por representantes de los sectores interesados. Se distribuyeron dos cuestionarios complementarios en línea, un cuestionario general abarcando todos los objetivos específicos de la estrategia, al igual que un cuestionario para actores específicos. Ambos cuestionarios fueron distribuidos con el propósito de evaluar el nivel de implementación de la Estrategia Nacional de Ciberseguridad de Costa Rica 2017 (ENC 2017), a fin de obtener un documento robusto y consensuado. La evaluación de la información adquirida se extrajo en base a los ocho objetivos específicos que contempla la ENC 2017, los cuales son:

- Coordinación Nacional
- Conciencia Pública
- Desarrollo de la Capacidad Nacional de la Seguridad Cibernética
- Fortalecimiento del Marco Jurídico en Ciberseguridad y TIC
- Protección de Infraestructura Críticas
- Gestión del Riesgo
- Cooperación y Compromiso Internacional
- Implementación, Seguimiento y Evaluación

El marco de análisis presentado en este informe tiene como propósito evaluar el nivel de implementación de la ENC 2017, de acuerdo con los objetivos específicos y sus respectivas líneas estratégicas que contempla. En base a la información recopilada, se derivaron conclusiones y recomendaciones pertinentes, las cuales aportarán en la elaboración del marco de revisión de la actual estrategia, así como en el desarrollo de la siguiente estrategia de ciberseguridad que se anticipa se llevará a cabo durante el año 2022. Por ende, este documento constituye el primer paso en la formulación de una segunda Estrategia Nacional de Ciberseguridad de Costa Rica.

El Gobierno de Costa Rica quisiera agradecer la contribución invaluable de los distintos actores nacionales quienes proporcionaron su amplio conocimiento e información para la finalización de este instrumento que será un referente en la planificación de una hoja de ruta en materia de ciberseguridad nacional para los próximos años. Adicionalmente, extiende su agradecimiento a la Organización de los Estados Americanos por su apoyo técnico especializado durante la revisión de la Estrategia Nacional de Ciberseguridad 2017 y en el desarrollo de este informe.

DOS

Contexto Actual

En un panorama cibernético altamente dinámico y de naturaleza interdependiente, ningún sector puede asegurar el ciberespacio de forma aislada. En este sentido, los gobiernos tienen una responsabilidad compartida, y entrelazada con todos los sectores, en la promoción de marcos legislativos que proporcionen políticas públicas e iniciativas nacionales hacia un ciberespacio confiable. Dada la creciente dependencia del ciberespacio para realizar actividades cotidianas, económicas y sociales, progresivamente la prosperidad y bienestar de los países depende de garantizar la seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC), haciendo imperativo el incrementar el nivel de madurez nacional. A este entorno cambiante, se le suma en 2020 la pandemia de COVID-19, una emergencia sanitaria que ha acelerado la dependencia de las plataformas digitales para realizar actividades diarias y esenciales, haciéndolas cada vez más susceptibles a las ciberamenazas.

De acuerdo con el Índice de Seguridad de Unisys, desde el inicio de la pandemia, los delitos cibernéticos se han incrementado hasta en 74% en América Latina.

Frente a los retos que ha generado la ampliación y el uso de las tecnologías digitales en Costa Rica, y a su vez los procesos de modernización de la transformación digital en el país con base a la Estrategia de la Trasformación Digital Hacia la Costa Rica del Bicentenario 4.0, que ha generado que tanto los servicios digitales de las instituciones y empresas se ampliaran, esto dentro del contexto de pandemia mundial; sumando la valiosa información del reporte del 2020: "Ciberseguridad: Riesgos, avances, y el camino a seguir en América Latina y el Caribe", desarrollado con el apoyo de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), así como insumos valiosos recibidos por medio de la Embajada de los Estados Unidos e Israel en temas de estrategia en materia de seguridad digital, el Gobierno de Costa Rica, dentro del marco del proceso gestado desde la primera Estrategia Nacional de Ciberseguridad 2017, por medio del Ministerio de Ciencia, Innovación Tecnologías y Telecomunicaciones, la Dirección de Gobernanza Digital y el CSIRT Nacional, y con la valiosa colaboración de la OEA y el Cyber4Dev de la Unión Europea, hemos realizado una revisión integral de la misma, para examinar las fortalezas y debilidades de la ciberseguridad nacional.

Con este trabajo, iniciamos el proceso para actualizar la Estrategia Nacional de Ciberseguridad de Costa Rica, con el fin de poder responder a las necesidades actuales de la cibersociedad costarricense que nos genere una hoja de ruta de trabajo común que permita desarrollar nuevos ejes como educación, oportunidad de actividades económicas, desarrollo seguro del turismo y fortalecimiento de la ciberseguridad país.

Con el objetivo de contribuir a que los países garanticen que las inversiones en ciberseguridad nacional sean lo más eficaz, eficiente y sostenible posible, se han creado una serie de marcos metodológicos para facilitar la toma de decisiones para los gobiernos. La evaluación de la ENC a través del fomento del intercambio de experiencias, recomendaciones y retroalimentación facilita contribuir al avance de soluciones de ciberseguridad basadas en la colaboración reciproca. Cuando la visión de un país se materializa en una ENC, sirve como hoja de ruta hacia un objetivo de madurez de seguridad cibernética deseable.

En virtud de este contexto, en septiembre de 2020, el Gobierno de Costa Rica solicitó la asistencia técnica especializada del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE) para llevar a cabo una revisión y elaboración oportuna de la actual ENC y en vistas de renovar el marco de ciberseguridad. Debido a los desafíos y las restricciones de viaje derivadas de la pandemia de COVID-19, la OEA/CICTE acordó brindar asesoramiento y orientación técnica, así como asistencia en la elaboración de un marco de recomendaciones específicas que emanan de la revisión de la ENC 2017 de manera virtual.

TRES

Marco Nacional de Ciberseguridad

La ENC de Costa Rica 2017 brindó una política gubernamental de ciberseguridad que proporciona un marco estratégico para lograr los objetivos socioeconómicos que dependen de la seguridad del ciberespacio. A medida que aumenta la necesidad de proteger el espacio digital para contribuir a la prosperidad del país, una estrategia de ciberseguridad se convierte en una herramienta esencial para diseñar e implementar políticas frente a los riesgos emergentes que amenazan el funcionamiento básico de la sociedad. Teniendo en cuenta que la naturaleza de la estrategia está arraigada en una perspectiva digital nacional, la misma debe ser actualizada de acuerdo con la realidad y el contexto del país. La revisión oportuna y de manera holística de la actual ENC permite reforzar la formulación y continuidad de políticas públicas en materia de ciberseguridad. Asimismo, sirve como paradigma para la mejora de la actual y futura formulación de la políticas públicas e iniciativas en ciberseguridad a nivel nacional.

De acuerdo con el Índice de Ciberseguridad Global 2020, Costa Rica ocupa el puesto 76 a nivel mundial, en comparación con el puesto 115 en el informe de 2018. Adicionalmente, en 2020 Costa Rica ingresó a los diez países más seguros en línea, ocupando el octavo lugar, una mejora de 10 lugares con respecto a la medición anterior realizada en 2018.

Considerando los avances a nivel nacional en la madurez cibernética, es imperativo revisar y actualizar el marco político, a fin de que refleje las oportunidades y desafíos actuales y futuros del país en el ámbito de la ciberseguridad.

Al evaluar el nivel de implementación de la ENC, también se consideró el estado de madurez de Costa Rica a través de un análisis de los hallazgos del informe OEA-BID 2020 "Riesgos, avances y el camino a seguir en América Latina y el Caribe", así como el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU por sus siglas en ingles). **Estas herramientas permiten a los gobiernos realizar una revisión y evaluación de sus capacidades nacionales de ciberseguridad**, identificar áreas para el desarrollo e informar la asignación adecuada de recursos.

La siguiente tabla es resume los objetivos específicos y sus respectivas líneas estratégicas de la NCS 2017, los cuales fueron analizados en este informe:

Figura 1: Objetivos y líneas estratégicas de la ENC de Costa Rica 2017

OBJETIVO 1
Coordinación Nacional

Coordinar con todas las partes interesadas para establecer su papel y línea de acción tanto en el proceso de mitigación como gestión, recuperación y continuidad en caso de un incidente de seguridad cibernética.

- 1.1 Coordinador Nacional
- 1.2 Colaboración del Sector Público y Privado

OBJETIVO 2
Conciencia Pública

Desarrollar y/o implementar campañas de concienciación y educación sobre seguridad cibernética que fomenten la responsabilidad de la protección digital como un deber de todos los usuarios de las tecnologías digitales.

- 2.1 Concienciación - Público General
- 2.2 Sector público
- 2.3 Micro, Pequeña y Mediana Empresa

OBJETIVO 3
Desarrollo de la Capacidad Nacional de Seguridad Cibernética

Realizar campañas de capacitación exclusivas para el sector público que tengan como objetivo educar a los usuarios finales en conceptos y buenas prácticas sobre seguridad cibernética y preparar a usuarios expertos (desarrolladores, administradores, directivos) en técnicas de seguridad cibernética.

- 3.1 Formación de recurso humano especializado
- 3.2 Investigación y Desarrollo

OBJETIVO 4
Fortalecimiento del Marco Jurídico en Ciberseguridad y TIC

Realizar una revisión del marco jurídico existente y proponer los ajustes necesarios para llevar a cabo procedimientos legales y medidas institucionales que garanticen una adecuada investigación y el enjuiciamiento efectivo.

- 4.1 Fortalecer el marco normativo y procesa en ciberdelincuencia
- 4.2 Crear capacidades en Ciberseguridad para la aplicación de la ley en el sistema penal de justicia
- 4.3 Fomentar redes de confianza para el intercambio de información entre los socios interesados en el sistema penal de justicia

OBJETIVO 5
Protección de Infraestructuras Críticas

Promover mecanismos para la identificación y protección de las infraestructuras críticas, así como la creación de políticas públicas específicas, como paso crucial para prevenir y/o mitigar incidentes de seguridad cibernética dirigidos a dañar o descontinuar operaciones sensibles.

- **5.1** Identificación y clasificación de las Infraestructuras Críticas
- **5.2** Implementación de medidas de seguridad de los Sistemas de Información y Telecomunicaciones de la Administración Pública

OBJETIVO 6
Gestión de Riesgo

Promover la implementación de un modelo de gestión de riesgo que se adapte a las necesidades propias de cada institución u organización.

- **6.1** Mejorar la seguridad de los productos y servicios vinculados con la seguridad de la información
- **6.2** Implementación de mejores prácticas y definición de requisitos mínimos de seguridad de la información en el Sector Financiero
- **6.3** Adopción de medidas de seguridad de referencia
- **6.4** Establecimiento de una red de intercambio de información para las entidades gubernamentales
- **6.5** Fortalecimiento del Centro de Respuesta a Incidentes de Seguridad Informática CSIRT-CR

OBJETIVO 7
Cooperación y Compromiso Internacional

Participar de la cooperación internacional a través de la asistencia y colaboración mutua en materia penal, técnica, educativa y el desarrollo de medidas de seguridad para abordar asuntos relacionados en materia de ciberseguridad.

- **7.1** Involucrar a la comunidad internacional en el apoyo de los objetivos de la Estrategia Nacional

OBJETIVO 8
Implementación, Seguimiento y Evaluación

Diseñar y aplicar una metodología de implementación y seguimiento que permita evaluar el cumplimiento de las líneas de acción y proponer los ajustes según se requiera.

- **8.1** Realizar el seguimiento de la aplicación de la Estrategia Nacional de Ciberseguridad, y evaluar el grado de éxito de cumplimiento de sus objetivos
- **8.2** Realizar una revisión y actualización de la Estrategia Nacional de Ciberseguridad cada dos años o según sea necesario

CUATRO

Metodología

El Gobierno de Costa Rica, con el apoyo técnico especializado del Programa de Ciberseguridad de la OEA/CICTE, desarrolló dos cuestionarios con el objetivo de recopilar datos de evaluación de la implementación de la ENC 2017 y ofrecer la oportunidad para que las partes interesadas brindarán sus comentarios y recomendaciones para la próxima ENC a desarrollar en 2021.

El primer cuestionario, que se distribuyó a través de una herramienta en línea, se abrió la semana del 10 de junio de 2021 y se cerró oficialmente el 30 de julio de 2021. En total se recibieron 25 cuestionarios, los cuales respondieron a preguntas en base a los objetivos y sus respectivas líneas de acción contempladas en la ENC 2017 (Figura 1). En cada sección se pidió a los encuestados que respondieran preguntas basadas en los objetivos, actividades, cronogramas y roles principales establecidos en NCS 2017. Al responder a estas preguntas, se solicitó que proporcionaran evidencias de implementación como enlaces a sitios web o descripción de iniciativas, entre otros.

Este primer cuestionario consideró componentes tanto cuantitativos como cualitativos. Cada sección contó con una tabla cuantitativa, solicitando calificar el grado de cumplimiento de las actividades previstas en la ENC 2017, de acuerdo con la siguiente escala del 1 al 5:

Rubrico:

1	2	3	4	5
Totalmente de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente desacuerdo

De igual manera, el segundo cuestionario se elaboró para ser distribuido entre actores específicos e instituciones de gobierno y fue distribuido por correo electrónico a fin de complementar y adquirir información relacionada con los siguientes temas:

- **Investigación Cibercriminal**
- **Importancia Económica de la Ciberseguridad e Infraestructura Crítica**
- **Expansión de las Fronteras de la Ciberseguridad**

CINCO

Análisis Situacional

La siguiente sección resume las respuestas recopiladas de acuerdo con los objetivos, líneas estratégicas y actividades establecidas en la ENC 2017. Adicionalmente, cada sección cita áreas de interés específicas identificadas por los encuestados y recomendaciones para consideración en el desarrollo de la nueva Estrategia Nacional de Ciberseguridad de Costa Rica.

Coordinación Nacional

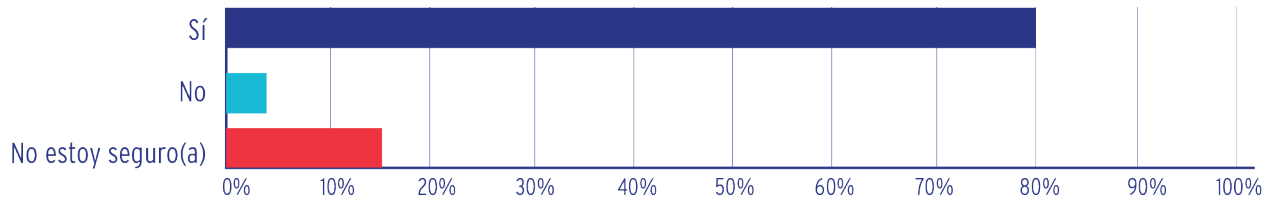
Esta sección tiene como propósito evaluar el nivel de implementación del marco de coordinación propuesto en la ENC 2017. Considerando que el objetivo general de la ENC 2017 se centra en el fomento de coordinación y cooperación de múltiples partes interesadas, es importante identificar los avances derivados de la implementación de la estrategia, así como identificar los desafíos actuales y oportunidades con miras al desarrollo de la siguiente Estrategia Nacional de Ciberseguridad de Costa Rica.

Línea Estratégica 1.1 Coordinador Nacional

Dado que la designación de un coordinador nacional fue uno de los objetivos principales de la ENC 2017, resulta alentador el nivel de conocimiento que se manifiesta por parte de los encuestados sobre la existencia de este coordinador nacional para articular acciones en materia de ciberseguridad y asegurar la continuidad de la estrategia, ya que el **80%** de los encuestados respondieron afirmativamente sobre la existencia de una figura de coordinación nacional. Adicionalmente, como pregunta de seguimiento, se planteó **¿qué institución cree que debería alojar esta iniciativa?**, la respuesta fue abrumadora al señalar a MICITT como institución encargada de supervisar la implementación de la estrategia. A pesar de este dato, el hecho de que todavía el 20% de los encuestados no conozcan la figura del coordinador nacional indica que existe una oportunidad de mejorar e incrementar los esfuerzos de concientización y alcance en esta línea.

Q3 1.1.1 ¿Existe un coordinador nacional para articular acciones enmateria de ciberseguridad y hacer la estrategia?

Respuestas: 25



Opciones respondidas	Respuestas	
Sí	80.00%	20
No	4.00%	1
No estoy seguro(a)	16.00%	4
Total		**25**

Línea Estratégica 1.2 Colaboración del Sector Público y Sector Privado

Las respuestas acerca de esta línea estratégica sugieren que es necesario incrementar esfuerzos para reforzar un diálogo con el sector privado y generar más visibilidad de esta colaboración puesto que, pese a que la mitad de los encuestados afirman conocer sobre diálogos entre los dos sectores, la otra mitad de los encuestados lo desconoce.

RECOMENDACIÓN

Se recomienda que la próxima ENC contemple una línea estratégica designada para la planificación de comunicaciones con el objetivo de aumentar la visibilidad de las distintas iniciativas que se están implementando a través del MICITT. Es evidente que una estrategia de comunicación adecuada contribuiría no solo a una mayor visibilidad de los esfuerzos de seguridad cibernética que se están implementando, sino también a la adquisición de mayor apoyo que podría conducir en la asignación de recursos.

Aquellos, no obstante, que respondieron afirmativamente señalaron distintas iniciativas público-privado de las cuales tienen conocimiento, entre ellos el intercambio de buenas prácticas e información, capacitaciones y programas de estudio en especialidad técnica de ciberseguridad. Dado que mayoritariamente cada respuesta señalaba distintas iniciativas, esto sugiere que si bien existen distintas iniciativas que se realizan de manera conjunta con el sector privado, el conocimiento de estas iniciativas varía dependiendo de la entidad, aludiendo a la necesidad de mejorar los mecanismos de comunicación para dar a conocer las iniciativas que se realizan de manera multisectorial.

RECOMENDACIÓN

La coordinación público-privada puede mejorar e incrementar mediante el Clúster de ciberseguridad, es por ello por lo que se recomienda asignar responsabilidades y un marco de gobernanza al Clúster de Ciberseguridad.

Una observación recurrente por parte de los encuestados se refería al fomento de la coordinación multisectorial y que esta no sea únicamente enfocada en el sector privado, si no incluyente de otros sectores. Una persona tenía conocimiento de que, en el pasado, como parte de la ENC, se estableció un *"modelo de coordinación multiactor, con la conformación de un Comité Consultivo integrado por representantes institucionales, de sector privado, académico y sociedad civil. Lamentablemente, ese no volvió a reunirse desde el mes de mayo de 2019".* Este comentario podría tomarse en cuenta en la actualización de la estrategia, a fin de evaluar la posibilidad de revitalizar el comité señalado y mediante este mecanismo impulsar el establecimiento e implementación de líneas estratégicas y actividades concretas que involucren a todos los sectores.

Nivel de implementación

Tomando en consideración todas las líneas estratégicas, se les pidió a los encuestados, en una escala de 1 a 5 (1-estar muy de acuerdo en que se implementó el objetivo y 5-estar muy en desacuerdo con que se implementó el objetivo), que indicaran su opinión sobre el nivel de implementación de las mismas. La brecha es evidente en cuanto a **la coordinación y colaboración entre el sector público y privado**, tomando en cuanto que casi **61%** respondió de manera indecisa. Sin embargo, los resultados sugieren que hubo un nivel significativo de implementación, reflejado en el nivel promedio de 3 correspondiente para las dos líneas estratégicas correspondientes al objetivo de coordinación nacional.

	1. Totalmente en desacuerdo	2. En desacuerdo	3. Indeciso	4. De acuerdo	5. Totalmente de acuerdo	Total	Promedio
1. La coordinación entre las principales partes interesadas en la ciberseguridad ha sido adecuada	4.35% 1	8.70% 2	34.78% 8	47.83% 11	4.35% 1	23	3.39
2. La coordinación entre el sector público y privado ha sido adecuada	4.35% 1	8.70% 2	60.87% 14	26.09% 6	0.00% 0	23	3.09

Conciencia Pública

Esta sección tiene como propósito evaluar el nivel de implementación de las diversas actividades orientadas a aumentar y fomentar una cultura de ciberseguridad a nivel nacional, principalmente a través de campañas de sensibilización que buscan preservar los beneficios del mundo digital. Por consiguiente, estas campañas sirven como una herramienta invaluable que contribuyen a crear un ciberespacio más seguro y resiliente.

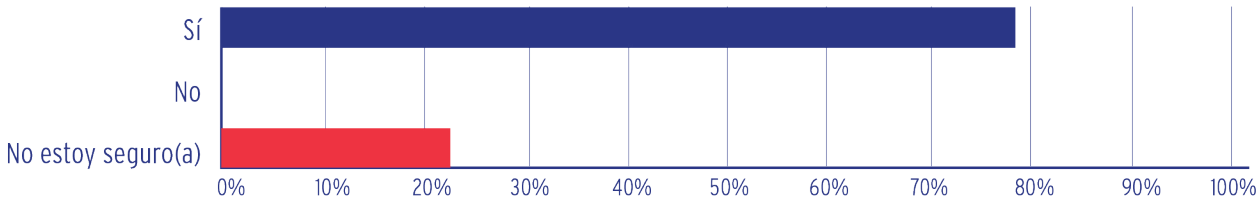
Línea Estratégica 2.1 Concienciación – Público en General

La estrategia nacional estipula el desarrollo de campañas de concienciación para la sociedad civil centradas en el fomento de buenas prácticas de ciberseguridad, particularmente orientadas en la protección de grupos poblacionales en condición de vulnerabilidad como la niñez y adolescencia, adultos mayores, población indígena y población con discapacidad. Asimismo, la estrategia determina que estas campañas y concientización se llevarían a cabo en alianza con el sector privado, sociedad civil y organizaciones no gubernamentales dedicadas a la protección de la infancia y adolescencia.

En lo que se refiere al **desarrollo de campañas de concienciación en ciberseguridad para los habitantes de Costa Rica, 78%** de los encuestados indicaron que sí se han llevado a cabo campañas de esta índole. Del mismo modo, los encuestados confirmaron que existen distintas campañas de concientización para la población, indicando que se han efectuado por diversos medios de comunicación nacionales, como las redes sociales, publicidades, anuncios y reportajes en medios de comunicación como la radio. En particular, varias partes interesadas, mediante sus respuestas, reafirmaron que la finalidad de esta línea estrategia fue implementada, tal y como fue señalando por la siguiente persona indicando que *"se han emitido comunicación sobre buenas prácticas en el uso de la tecnología y alertas sobre ataques a la población general y como resguardar sus datos personales."* Sin embargo, los encuestados no expresaron amplio conocimiento sobre la realización de campañas de concientización en conjunto con distintos sectores.

Q9 2.1.1 ¿Se han desarrollado campañas de concienciación en ciberseguridad para los habitantes de Costa Rica?

Respuestas: 23



Opciones respondidas	Respuestas	
Sí	78.26%	18
No	0.00%	0
No estoy seguro(a)	21.74%	5
Total		**23**

En relación a campañas de concientización dirigidas para grupos poblacionales en condición de vulnerabilidad, hubo limitada indicación de conocimiento sobre el tema. Sin embargo, el CSIRT-CR ha impulsado capacitaciones centradas en buenas prácticas de higiene digital y ciberseguridad para menores y adolescentes. En el 2020 los eventos de capacitación para docentes., beneficiaron a más de 7000 docentes del MEP capacitados en materia de ciberseguridad. Adicionalmente, desde la Comisión Nacional de Seguridad en Línea llevan a cabo acciones que forman parte de los componentes de la iniciativa "Costa Rica dice No a la Explotación y Abuso Sexual en Línea" (CR-NEXST) que surge en el 2018 para garantizar la protección de niñas, niños y adolescentes frente a la explotación y abuso sexual en línea. Esta acción se ha ejecutado bajo el liderazgo de la Fundación Paniamor con el apoyo del Ministerio de Ciencia, Tecnología y Telecomunicaciones, así como otras entidades públicas y privadas, en aras de desarrollar capacidades para que actores claves se conviertan en facilitadores activos en la prevención y respuesta ante estos flagelos. Este proceso de trabajo resultó en que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, la Dirección de Evolución y Mercado en Telecomunicaciones, realizara el lanzamiento de la Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea 2021-2027, lanzada recientemente en agosto 2021, para ello, se llevó a cabo un trabajo interinstitucional liderado por MICITT, desde la Comisión Nacional de Seguridad en Línea que preside y en la que participan el Ministerio de Educación Pública (MEP), Ministerio de Cultura y Juventud (MCJ), Superintendencia de Telecomunicaciones (SUTEL), Poder Judicial (PJ), Patronato Nacional de la Infancia (PANI), Fundación Paniamor, Fundación Omar Dengo (FOD), Cámara Costarricense de Tecnologías de la Información y la Comunicación (CAMTIC) así como otras organizaciones aliadas.

RECOMENDACIÓN

Dado el bajo nivel de conocimiento de las existentes campañas nacionales para la protección de grupos poblacionales en condición de vulnerabilidad, se recomienda desarrollar una campaña nacional de mensajería centralizada que este dirigida a los diferentes grupos identificados en la ENC 2017. La limitada implementación de este objetivo podría atribuirse a la ausencia de asignar una entidad como responsable de la ejecución de esta actividad, por lo tanto, se debe considerar la asignación de una entidad específica como responsable de la implementación de esta línea de acción.

Una observación recurrente fue el comentario de los encuestados sobre las campañas de concientización, las cuales señalan que han consistido mayoritariamente de infografías y por un periodo corto, por lo que una persona señaló que *"es notorio que faltaron recursos para hacer campañas más agresivas que incluyeran producciones audiovisuales".* Consecuentemente, se podría hacer un mayor acercamiento a distintos sectores que actualmente realizan esfuerzos similares, a fin de unir esfuerzos y recursos que permitan expandir el alcance de campañas nacionales de concienciación en materia de ciberseguridad.

RECOMENDACIÓN

A fin de tener conocimiento sobre qué iniciativas son más eficientes y efectivas de utilizar según el grupo poblacional al que se dirigen las campañas de educación y sensibilización, se recomienda desarrollar un mensaje claro y focalizado con indicadores clave sobre la audiencia a la que se pretende llegar. Asimismo, se recomienda medir los niveles de concientización antes y después de que se lleven a cabo las iniciativas.

Herramientas de buenas prácticas a nivel internacional:

- ☑ **"Iniciativas de concienciación sobre la seguridad de la información: práctica actual y medición del éxito" *Agencia Europea de Seguridad de las Redes y de la Información (enisa)*, 2007.[1]**
- ☑ **"Campañas de concienciación sobre seguridad cibernética ¿Por qué no logran cambiar el comportamiento?" *Global Cyber Security Capacity Centre*, 2014.[2]**

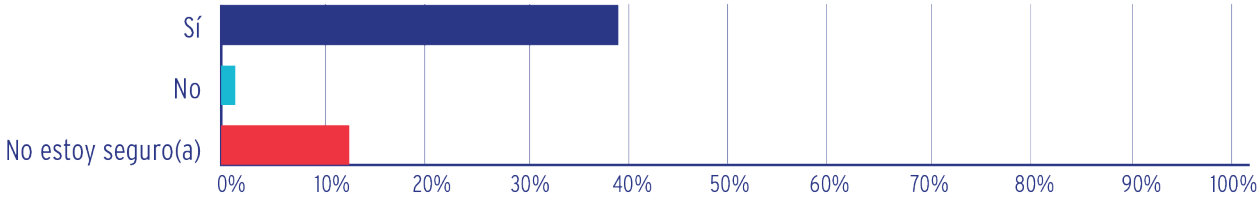
Línea Estratégica 2.2 Sector Público

Dentro de la segunda línea estratégica, la ENC 2017 incorpora el desarrollo de campañas de concienciación y educación dirigidas a los funcionarios públicos, focalizados al tipo de institución en el que se desempeñan y enfatizando mejores prácticas de protección y aseguramiento de datos sensibles contenidos en sistemas de información. Basado en la información recopilada, es evidente que, sí se han llevado a cabo esfuerzos para realizar campañas de concienciación para funcionarios públicos, no obstante, el alcance y visibilidad de estas varía entre las instituciones gubernamentales. Considerando que casi el **56%** de los encuestados indicaron no estar seguros sobre la existencia de campañas de concienciación y educación dirigidos a funcionarios públicos, se destaca la necesidad de adoptar un plan de comunicación extenso y de manera uniforme para todas las entidades gubernamentales.

1 https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/ENISA_Measuring_Awareness_Final.pdf
2 https://discovery.ucl.ac.uk/id/eprint/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Q11 2.2.1 ¿Se han desarrollado campañas de concienciación y educación dirigidas a los funcionarios públicos?

Respuestas: 23



Opciones respondidas	Respuestas	
Sí	39.13%	9
No	4.35%	1
No estoy seguro(a)	56.52%	13
Total		**23**

Al elaborar su respuesta, un encuestado indico que *"en el caso del INA (Institución Nacional de Aprendizaje) se desarrollan campañas internas a partir de las buenas prácticas en protección de datos y atención a ataquen que se deben llevar a cabo, así como capacitaciones sobre el tema"*, otras organizaciones que realizaran esfuerzos similares son el Ministerio de Hacienda y Ministerio de Educación Pública, así como de manera destacable, distintos encuestados corroboran las iniciativas que se emplean desde el Poder Judicial.

RECOMENDACIÓN

Considerando las respuestas mixtas en relación con el conocimiento sobre si existen campañas para funcionarios públicos, se recomienda que en la próxima ENC se contemple el desarrollar una campaña de mensajería centralizada que pueda incorporar distintas campañas para funcionarios públicos focalizadas al tipo de institución en el que se desempeñan. Asimismo, se podría considerar asignar a una institución como responsable de implementar estos esfuerzos y de generar una base de datos acerca de las campañas internas que se realizan en las distintas entidades de gobierno, a fin de coordinar los distintos esfuerzos procedidos dentro de los Ministerios.

Línea Estratégica 2.3 Micro, Pequeña y Mediana Empresa

Dentro de las tres líneas estratégicas definidas en este objetivo, en esta línea de trabajo se observó un menor nivel de implementación, considerando que más del **85%** de los encuestados indicaron no estar seguros del **desarrollo de conversatorios y foros de intercambio de información sobre temas de seguridad cibernética, específicamente para las Micro, Pequeña y Mediana Empresa** (PYMES).

Nivel de implementación

En general, en lo que se refiere al establecimiento de campañas de concienciación sobre ciberseguridad, se puede observar el gran avance en esta área. Sin embargo, de la misma manera se puede constatar la necesidad de una mayor coordinación para unificar esfuerzos y visibilidad entre todos los sectores y grupos poblacionales focalizados. Los encuestadores proveyeron comentarios y sugerencias sobre esta área, algunas de las respuestas fueron las siguientes:

1. **Las campañas de ciberseguridad deben ser masivas y constantes a través de medios de comunicación como TV, radio y redes sociales. Es necesario invertir suficiente dinero en publicitar la ciberseguridad, en especial para prevenir fraudes bancarios (llamadas de la reforma) y robo de información personal.**
2. **Implementando programas de capacitación/charlas conjuntas atendiendo de manera integral cada contexto/población. Desarrollando y trasladando documentos de buenas prácticas a las partes interesadas. Que se desarrollen programas de cursos, capacitaciones, y especializaciones en donde participen personal de las instituciones, y que estos programas sean amparados y apoyados por actores como el servicio civil, la academia, y entes especializados externos.**
3. **Primero definir las metas y verificar que el propósito sea el mismo para alinear las estrategias institucionales y definir puntos de articulación para proponer diferentes iniciativas de trabajo conjunto [sectores público y privado], empezando por la promoción de una cultura de cibersegura.**

Las respuestas por parte de los encuestados sugieren que a partir de la aprobación de la ENC 2017, hubo gran progreso en el fomento de concienciación y educación en ciberseguridad. No obstante, la falta de **conversatorios y foros de intercambio de información sobre temas de ciberseguridad para las PYMES** es evidente, considerando que el **95%** respondió de manera indecisa. Aun así, los resultados sugieren que hubo un nivel significativo de implementación con el nivel promedio de 3 correspondiente para el segundo objetivo específico de la estrategia nacional.

Desarrollo de la Capacidad Nacional de Seguridad Cibernética

El desarrollo de capacidades se ha convertido en un término frecuente en los debates de seguridad cibernética en el mundo.[3] Desarrollar un programa de desarrollo de capacidad eficaz y eficiente es complejo, dado que requiere financiación sostenible, habilidades, continuidad y una metodología integral. Al desarrollar nuevos programas o emprender programas existentes, es importante involucrar elementos específicos que permitan materializar el impacto deseado. Si bien a nivel mundial, varias entidades como la Unión Europea, ASEAN y la OEA han adoptado un enfoque regional para el desarrollo de capacidades, es necesario que los países cuenten con programas de desarrollo de capacidades contextualizados a la realidad nacional, a fin de adoptar propuestas que abordan los desafíos y oportunidades que contribuyan al incremento del talento cibernético local.

3 https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Summary-Capacity-Building.pdf

Como lo demuestra la organización *Carnegie Endowment for International Peace*, en el diagrama a continuación, el desarrollo de capacidades se puede definir como "una forma de empoderar a las personas, las comunidades y los gobiernos para lograr sus objetivos de desarrollo mediante la reducción de los riesgos de seguridad digital derivados del acceso y el uso de la información y la comunicación tecnologías" y puede ser abordado desde la prevención hasta la respuesta a incidentes cibernéticos.[4]

Figura 2 Conceptualización del Desarrollo de Capacidades en Ciberseguridad[5]

4 Priority #5: Capacity-Building - International Strategy to Better Protect the Financial System Against Cyber Threats - Carnegie Endowment for International Peace

5 Instituto de Estudios de Seguridad de la Unión Europea, "Riding the Digital Wave – The Impact of Cyber Capacity Building on Human Development", diciembre de 2014, https://www.iss.europa.eu/content/riding-digital-wave-%E2%80%93-impact-cyber-capacity-buildinghuman-development

Línea Estratégica 3.1 Formación de recurso humano especializado

La ENC 2017 identifica la protección de sistemas informáticos y la adopción de buenas prácticas cibernéticas como el propósito principal para impulsar una cultura en seguridad cibernética, es por ello por lo que una parte integral de la estrategia consiste en la implementación de medidas destinadas a la alfabetización, concienciación y formación del recurso humano en materia de ciberseguridad. Considerando que frecuentemente se realizan ataques dirigidos a funcionarios públicos para tener acceso a sistemas de información gubernamental, la estrategia destaca la importancia de contar con un nivel de competencia dentro del personal público, particularmente entre los administradores y responsables de la toma de decisiones.

En este sentido, la estrategia identifica como una de sus actividades **fomentar la divulgación y promoción de oportunidades de especialización o capacitación en seguridad cibernética disponibles local o internacionalmente para funcionarios del sector público**, algo que se ha conseguido de acuerdo con **45%** de los encuestados. Algunos indicaron distintas iniciativas de capacidad y formación que se llevan a cabo mediante acuerdos bilaterales y asistencia por parte de organismos internacionales como la OEA. Sin embargo, la brecha, representada por el **55%** de las personas que indicaron no tener conocimiento de estas iniciativas, sugiere que existe la oportunidad de promover la divulgación y visibilidad de programas de desarrollo disponibles, en función de un diagnóstico previo o de una necesidad manifestada en el sector público.

RECOMENDACIÓN

Habida cuenta de que existen algunos programas de educación secundaria y oportunidades de formación profesional en materia de ciberseguridad, se debe considerar un mapeo de estos cursos y centralizar el acceso de la información respecto a ofertas académicas de profesionalización, así como promover este recurso a nivel nacional.

La institucionalización de planes de estudio nacionales en materia de seguridad cibernética puede contribuir a que una sociedad cuente con los recursos humanos necesarios para atender la demanda de habilidades de ciberseguridad que induce la conectividad digital. Al respecto, la ENC 2017 incluyó el desarrollo de planes de estudio para impulsar la oferta académica que incorpore módulos de ciberseguridad a programas de pregrado, posgrado y doctorado. Al evaluar el nivel de implementación de esta línea estratégica, 35% de los encuestados indicaron que sí se han **propuesto adecuaciones en la oferta académica que permitan desarrollar planes de estudio o incorporar módulos de ciberseguridad en educación secundaria**, mientras que el **40%** señaló no estar seguro sobre esto.

En las respuestas complementarias de las partes interesadas se evidencia que se ha incorporado programas especializados en ciberseguridad en educación secundaria, así como el establecimiento de estándares de cualificación en el campo de ciberseguridad dentro del Marco Nacional de Cualificaciones de la Educación y Formación Técnica Profesional de Costa Rica. Sin embargo, los resultados de las encuestan sugieren que existe un limitado conocimiento sobre las ofertas académicas actuales.

RECOMENDACIÓN

Con el objetivo de incrementar y fortalecer la fuerza laboral del sector de seguridad cibernética, se podría incorporar planes educativos no solo en educación secundaria, sino también en educación primaria y secundaria, oportunidades de formación laboral (por ejemplo, pasantías y practicas), y grupos de investigación de posgrado, de modo que se fomente una trayectoria profesional en ciberseguridad y el desarrollo de un ecosistema de educación cibernética (Figura 3).

Figura 3 Posibles áreas para el desarrollo del ecosistema de ciber educación

Respecto a la **promoción de la inclusión del tema de ciberseguridad en al menos un curso de carreras no tecnologías**, el **57%** indico que no tener conocimiento sobre esto, mientras que el **42%** contesto de manera afirmativa. No obstante, al elaborar su respuesta, en general, no se observó gran indicación de que se haya incorporado cursos en carreras no técnicas, en cambio los encuestados señalaron distintos cursos de especialización en ciberseguridad.

Línea Estratégica 3.2 Investigación y Desarrollo

En marcado en esta línea estratégica, la última actividad propuesta en el tercer objetivo específico es la **gestión de alianzas entre universidades públicas y privadas con motivo de desarrollar proyectos de investigación sobre amenazas cibernéticas** y soluciones innovadoras para enfrentar incidentes cibernéticos, a lo que se observó una abrumadora respuesta del **85%** respondiendo no estar seguro sobre el tema y ninguno de los encuestados que respondieron a esta pregunta indicaron tener conocimiento sobre la implementación de esta línea estratégica.

RECOMENDACIÓN

Para proteger a una nación contra futuros ataques cibernéticos, es necesario ser proactivo al pensar en su fuerza laboral. Por consiguiente, se recomienda incluir en la próxima ENC medidas para promover temas de ciberseguridad en educación primaria, a fin de generar interés en la materia dese una edad temprana. El marco ciberseguridad de NICE formulado por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en ingles) de Estados Unidos es un mecanismo de buena práctica a nivel global. Este mecanismo consiste en un marco de políticas sobre cómo los sectores privados, público y académico pueden establecer una taxonomía y un léxico común a través del cual se pueda elaborar un plan común estratégico de reclutamiento y gestión de talento.[6]

Adicionalmente, en términos de educación, la Organización de los Estados Americanos y Amazon Web Services publicaron en el 2020 un informe técnico titulado *"Educación en seguridad cibernética: Planificación para el futuro a través del desarrollo de la fuerza laboral"*, el cual describe los pasos para desarrollar un plan de acción de educación en ciberseguridad, incluyendo mecanismos para integrar la educación en ciberseguridad en el desarrollo de políticas y planes de estudio escolares para abordar la escasez de habilidades en seguridad cibernética en América Latina y el Caribe. También ofrece un conjunto de herramientas, iniciativas y mecanismos a nivel nacional para generar interés en carreras de seguridad cibernética.[7]

Nivel de implementación

Considerando todas las líneas estratégicas, se les pidió a los encuestados, en una escala de 1 a 5 (1-estar muy de acuerdo en que se implementó el objetivo y 5-estar muy en desacuerdo con que se implementó el objetivo), que indicaran su opinión sobre el nivel de implementación de estas. Las respuestas por parte de los encuestados sugieren que existe la oportunidad de incrementar la visibilidad sobre las distintas iniciativas de desarrollo de capacidades en ciberseguridad. No obstante, se observa un nivel significativo de implementación con un nivel promedio de 3.

	1. Totalmente en desacuerdo	2. En desacuerdo	3. Indeciso	4. De acuerdo	5. Totalmente de acuerdo	Total	Promedio
1. Se ha fomentado la divulgación y promoción de oportunidades de especialización o capacitación en seguridad cibernética disponibles local o internacionalmente para funcionarios del sector público	10.35% 2	15.79% 3	21.05% 4	47.37% 9	5.26% 1	19	3.21

6 https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
7 http://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

1. Totalmente en desacuerdo | 2. En desacuerdo | 3. Indeciso | 4. De acuerdo | 5. Totalmente de acuerdo

	1. Totalmente en desacuerdo	2. En desacuerdo	3. Indeciso	4. De acuerdo	5. Totalmente de acuerdo	Total	Promedio
2. Se han propuesto e impulsado adecuaciones en la oferta académica que permitan desarrollar planes de estudio de seguridad cibernética o añadir módulos de ciberseguridad a los programas pertinentes de pregrado, posgrado y doctorado	10.35% 2	15.79% 3	47.37% 9	21.05% 4	5.26% 1	19	2.95
3. Se ha promovido la inclusión del tema de ciberseguridad en algún curso de carreras no tecnológicas	5.26% 1	10.53% 2	57.89% 11	21.05% 4	5.26% 1	19	3.11
4. Se han gestionado alianzas con universidades públicas y privadas para desarrollar proyectos de investigación sobre las amenazas emergentes y el desarrollo de soluciones innovadoras a los incidentes cibernéticos	0.00% 0	10.53% 2	78.95%	10.53% 2	0.00% 0	19	3.00

Fortalecimiento del marco jurídico en Ciberseguridad y TIC

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) afirma que el panorama cambiante del delito cibernético y las brechas de habilidades resultantes son desafíos decisivos para los organismos encargados de hacer cumplir la ley y los fiscales, especialmente la aplicación de leyes transfronteriza. Por esta razón, es necesario contar con una legislación actualizada y ágil. Según UNCTAD, mientras que 154 países (79%) han promulgado leyes sobre delitos cibernéticos, el patrón varía según la región: Europa tiene la tasa de adopción más alta (93%) y Asia y el Pacífico tienen la más baja (55%). Esta legislación nacional busca tipificar como delito los delitos y el uso de computadoras de manera amplia. Además, el Consejo de Europa ha señalado que, si bien se han logrado avances en el marco jurídico del delito cibernético, se requiere una mayor creación de capacidades para garantizar que la aplicación de la legislación por parte de los profesionales de la justicia penal se lleve a cabo de manera adecuada.

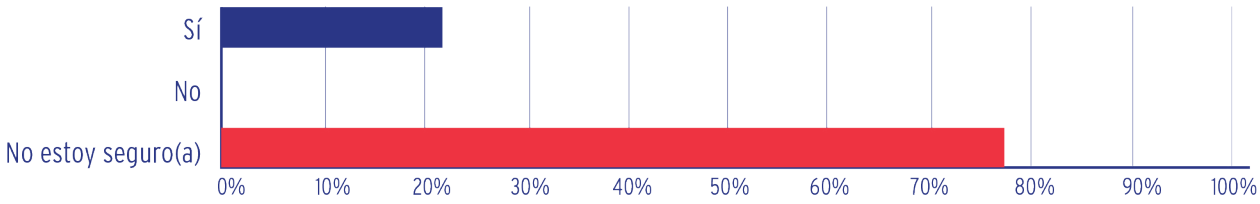
El Consejo de Europa reitera que "la legislación que define claramente la conducta que constituye un delito y establece poderes para asegurar pruebas electrónicas limitadas por condiciones y salvaguardas es la base para una respuesta de justicia penal efectiva frente al ciberdelito y que cumpla con los requisitos de derechos humanos y el estado de derecho."[8] Por lo tanto, intrínsecamente, un marco legislativo sólido solo puede fortalecer los poderes de investigación que permiten abordar el delito cibernético.

Línea Estratégica 4.1 Fortalecer el marco normativo y procesal en ciberdelincuencia

Como primer paso para combatir el ciberdelito, la ENC 2017 estipula la necesidad de revisar el marco legal, regulatorio y procesal existente relacionado con el ciberdelito. Consecuentemente, la estrategia indica que se debe **constituir un comité especializado que revise la normativa vigente para garantizar la existencia de herramientas procesales adecuadas en el ámbito del ciberdelito**, a lo que solo el **21%** de los encuestados indicaron que se empleó dicha acción. Las respuestas escritas destacaron que existe una *Comisión de Ciberseguridad y Ciberdelincuencia el Poder Judicial*, pero no es claro si dicho comité tiene el mandato de revisar la legislación existente para garantizar que las herramientas procesales sean las adecuadas para abordar el ciberdelito.

Q27 4.1.1 ¿Se ha creado una comisión especializada con el objetivo de revisar la normativa vigente, para garantizar que existan herramientas procesales adecuadas en materia de delincuencia cibernética?

Respuestas: 19



Opciones respondidas	Respuestas	
Sí	21.05%	4
No	0.00%	0
No estoy seguro(a)	78.95%	16
Total		**19**

8 https://www.coe.int/en/web/cybercrime/-/global-state-of-cybercrime-legislation-update-

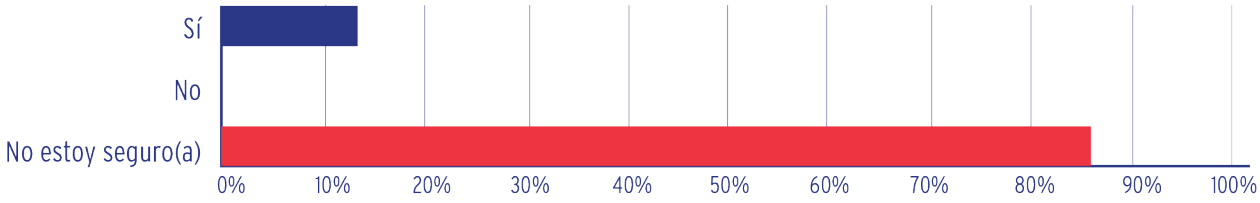
Línea Estratégica 4.2 Crear capacidades en Ciberseguridad para la aplicación de la ley en el sistema penal de justicia

La ENC 2017 indica que el marco legal de Costa Rica debe tomar en cuenta la necesidad de que los responsables de la aplicación de la ley investiguen los delitos cibernéticos de manera efectiva y que los equipos de respuesta a incidentes detecten un incidente con prontitud. Es por ello por lo que las entidades correspondientes deben contar con la autoridad necesaria para disuadir las amenazas identificadas. En este sentido, la ENC 2017 incluye el desarrollo de capacidades en ciberseguridad para la aplicación de la ley dentro del sistema de justicia como una línea estratégica. Como curso de acción inicial para lograr esta línea estratégica, se enfatiza **la identificación de áreas clave del sistema de justicia penal que requieren fortalecer sus capacidades y conocimientos en ciberseguridad.** Cuando se preguntó si se implementó esta última actividad, solo el **13%** de los encuestados respondieron afirmativamente.

Un encuestado identificó lo siguiente como un área que requiere fortalecimiento de capacidades: *"la Fiscalía adjunta de Fraudes y Cibercrimen ocupa dotar de más personal que investigue esta materia, ya que la cantidad de fiscales es insuficiente y su conocimiento principalmente se concentra en la estafa informática. Por lo anterior, también el mismo debe capacitarse más. De similar manera, la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial (OIJ), requiere capacitación y recursos."*

Q29 4.2.1 ¿Se han identificado las áreas claves del sistema penal de justicia, que requieren fortalecer sus capacidades y conocimientos en materia de Ciberseguridad?

Respuestas: 15



Opciones respondidas	Respuestas	
Sí	13.33%	2
No	0.00%	0
No estoy seguro(a)	86.67%	13
Total		**15**

Además, aunque el **93%** de los encuestados no estaba seguro de si se había **colaborado en la generación de capacidades para áreas clave identificadas**, varias respuestas escritas aludieron al hecho de que el poder judicial, a través de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial, tiene como objetivo fortalecer la ciberseguridad del Poder Judicial y la capacidad de respuesta de la policía judicial, fiscalía y poder judicial en materia de ciberdelito. Asimismo, las respuestas indican que el Poder Judicial, con el apoyo técnico de organismos internacionales, realiza iniciativas de capacitación, tal y como lo hace en conjunto con el Consejo de Europa a través del programa GLACY que busca brindar capacitación basada en la Convención de Budapest.

RECOMENDACIÓN

Se recomienda que para el desarrollo de la nueva ENC se establezca un grupo de trabajo específicamente para analizar el marco legal y las brechas que deben abordarse a nivel nacional. Este grupo también debe 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.

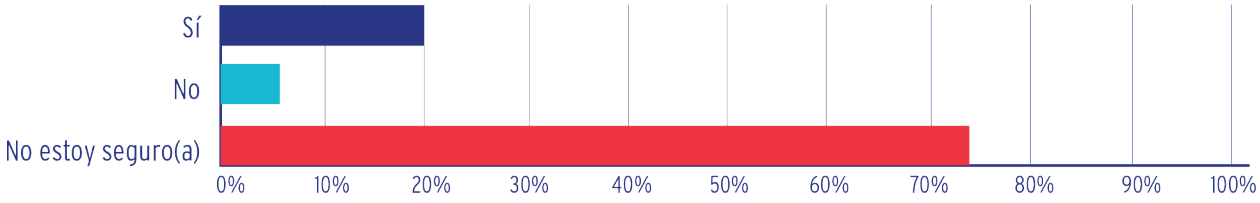
Línea Estratégica 4.3 Fomentar redes de confianza para el intercambio de información entre los socios interesados en el sistema penal de justicia

No está claro si existen **redes de confianza respaldadas por un instrumento jurídico de confidencialidad para el intercambio seguro de información relevante relacionada con los delitos cibernéticos**, como lo demuestra el **73%** de los encuestados que no estaban seguros de esta actividad. No obstante, un encuestado indicó que *"a través del MICITT, se cuenta con una Red de colaboración y enlaces de ciberseguridad de entidades bancarias y financieras, la cual por su naturaleza se utiliza para delitos relacionados con el sistema financiero nacional."*

Asimismo, las respuestas escritas indican que OIJ y CSIRT-CR tienen un canal abierto para el intercambio de información. Por lo tanto, con base en las respuestas, se puede suponer que existe cierto nivel de comunicación y colaboración entre las fuerzas del orden y el CSIRT nacional. Este tipo de cooperación es una oportunidad para mejorar el intercambio de información y la designación de una clara división de tareas y mandatos una vez que se comparte la información. De igual manera, el intercambio de información entre el CSIRT y las fuerzas del orden es vital para crear un perfil de amenaza para el país y resolver incidentes cibernéticos.

Q33 4.3.1 ¿Se han generado redes de confianza apoyadas mediante un instrumento jurídico de confidencialidad para el intercambio seguro de información relevante vinculada con delitos cibernéticos?

Respuestas: 15



Opciones respondidas	Respuestas	
Sí	20.00%	3
No	6.67%	1
No estoy seguro(a)	73.33%	11
Total		**15**

Se debe alentar tanto a las empresas privadas como al Gobierno a establecer políticas sólidas de divulgación de vulnerabilidades como elementos esenciales de un programa de gestión de vulnerabilidades eficaz y fundamentales para la seguridad de los sistemas de información gubernamentales accesibles a través de Internet. Cuando las agencias integran los informes de vulnerabilidades en sus actividades de gestión de riesgos de ciberseguridad existentes, pueden evaluar y abordar una gama más amplia de inquietudes. Además, las políticas de divulgación de vulnerabilidades mejoran la resistencia de los servicios en línea al fomentar una colaboración significativa entre los sectores y el público en general. En este sentido, uno de los tres cuestionarios distribuidos para actores específicos se centró en "Investigación del Ciberdelito". En este sentido, ante la pregunta sobre si **se han diseñado trámites expeditos para el intercambio de información confidencial**, persiste la falta de información sobre este tipo de trámites, ya que el **86%** indicó que no estaba seguro de esto.

RECOMENDACIÓN

Se recomienda que la próxima ENC incluya líneas estratégicas y actividades concretas relacionadas con los mecanismos de notificación de incidentes y los procedimientos de investigación. Para ello, las iniciativas existentes que se llevan a cabo en esta área deben primero ser analizadas y las brechas de implementación identificadas deben ser incluidas y fortalecidas en la siguiente estrategia. También se debe considerar la integración de la agenda digital nacional y el aumento de los servicios digitales que ofrecerá el gobierno, así como los mecanismos para que el usuario final reporte los incidentes.

Entre las preguntas incluidas en el cuestionario, se preguntó a los actores relevantes si existían **iniciativas público-privadas para compartir información y colaborar en el estado de incidentes o actividades ciberdelincuentes**, a lo que las respuestas abrumadoras indicaron que el CSIRT-CR es una entidad clave que opera a nivel informativo y preventivo, generando alertas de ciberseguridad. Un encuestado indicó que se estableció *"un organismo especializado en la fiscalía para la atención e investigación de casos asociados con el ciberdelito"* para manejar las investigaciones del ciberdelito. Además, con respecto a la pregunta, **¿qué limitaciones considera que existen para compartir información sobre estafas cibernéticas avanzadas y vulnerabilidades asociadas?**, destacan las siguientes respuestas:

1. **El miedo a violar los términos de confidencialidad, tener la capacidad crítica de saber qué se puede y qué no se puede compartir y asegurar que el medio sea correcto y seguro, para no hacer más vulnerable la situación.**
2. **Por mencionar algunos: conocimiento en detección y atención de ciberamenazas, personal dedicado a estas tareas en las instituciones, recursos asignados para tal fin en las instituciones, el valor/ importancia que el país (el gobierno) le da a la atención de estas actividades (recursos y capacidades que destina para capacitación, fortalecimiento, herramientas, etc.).**
3. **La definición de protocolos y datos mínimos a compartir; así como generar la confianza para crear la cultura requerida.**
4. **El TI-CSIRT-CR está compartiendo información sobre amenazas y vulnerabilidades de muy buena manera, funciona bien para aquellos de nosotros que estamos atentos a estas comunicaciones. La mayor limitación es la exposición a la opinión pública de cualquier institución o banco, dado que en el caso de que haya una vulnerabilidad que los afecte, la situación se oculta.**

La ciberseguridad es un bien público que es más fuerte cuando todas las partes interesadas tienen la capacidad de contribuir. Un componente clave para recibir apoyo de ciberseguridad del público en general al establecer políticas formales que describan las actividades que se pueden realizar para encontrar e informar vulnerabilidades de una manera legalmente autorizada. Dichas políticas podrían ayudar a la entidad gubernamental responsable de investigar el delito cibernético a remediar las vulnerabilidades antes de que puedan ser explotadas. Es en este sentido que un encuestado señala que existen mecanismos de notificación de incidentes sobre la actividad del ciberdelito *"a través de los teléfonos que especifique la Sección de Delitos Informáticos del Poder Judicial y, eventualmente, la Fiscalía Adjunta de Fraude y Ciberdelincuencia".* Sin embargo, información detallada relacionada con los mecanismos de notificación de incidentes y los procedimientos de investigación sobre el delito cibernético es muy limitada de acuerdo con las respuestas recibidas por los encuestados.

Nivel de implementación

Considerando todas las líneas estratégicas, se les pidió a los encuestados, en una escala de 1 a 5 (1-estar muy de acuerdo en que se implementó el objetivo y 5-estar muy en desacuerdo con que se implementó el objetivo), que indicaran su opinión sobre el nivel de implementación de estas. Las respuestas por parte de los encuestados sugieren que existe la oportunidad de incrementar la visibilidad acerca de la manera en la cual las autoridades gubernamentales están abordando el cibercrimen desde el marco jurídico. No obstante, se observa un nivel significativo de implementación con un nivel promedio de 3.

Protección de Infraestructuras Críticas

Esta sección tiene como propósito evaluar los avances en la protección de infraestructuras críticas. Dentro de este objetivo, la ENC 2017 define un conjunto de actividades para asegurar la continuidad y funcionalidad de las infraestructuras criticas ante un eventual ataque cibernético.

Línea Estratégica 5.1 Identificación y Clasificación de las Infraestructuras Críticas

La ENC 2017 determina la **identificación de la Infraestructura Crítica (CI) nacional es un paso crucial para aplicar medidas de seguridad.** Sin embargo, aunque el **40%** de los encuestados indicó que se había realizado la identificación de CI, hay una indicación limitada de que dicha acción se llevó a cabo de manera integral, ya que el **40%** de los encuestados mencionaron que no estaban seguros. Esto es importante de resaltar, ya que incluso si se ha realizado la identificación de CI, el nivel de conocimiento de su existencia habría resultado en que no fuera tan efectivo.

RECOMENDACIÓN

Con respecto al desarrollo de la nueva ENC, se recomienda realizar un mapeo (en la medida de lo posible) de forma horizontal y vertical basado en la independencia intersectorial de la Infraestructura de Información Crítica (CII) de Costa Rica. Esto puede facilitar significativamente el acceso a la información necesaria durante un significativo incidente cibernético.

Asimismo, ante la pregunta de si **se estableció una comisión de generación de política pública conformada por un representante y un suplente de cada una de las instituciones públicas y entidades privadas identificadas, con el fin de garantizar la operatividad y estabilidad continua de estos servicios**, ninguno de los encuestados indicó afirmativamente y el **71%** dijo que no estaba seguro. Un encuestado indicó que *"se encuentra en marcha una propuesta de Ley de Protección de Infraestructura Crítica, liderada por el Ministerio de Seguridad Pública, que aún no ha sido presentada a la Asamblea Legislativa".* Dado que esta propuesta de ley busca mejorar la prevención, la preparación y respuesta del país ante ataques deliberados que afecten infraestructuras críticas, se recomienda que la misma debe ser alineada e incluida en las siguientes ENC.

RECOMENDACIÓN

El análisis de amenazas facilita las alertas tempranas a los grupos objetivo que potencialmente se verían afectados si se concretara la amenaza percibida. Es necesario que exista una mayor coordinación con las autoridades de TIC para garantizar pruebas y evaluaciones periódicas de las infraestructuras crítica, los servicios esenciales y la red gubernamental, lo cual ayudaría al cumplimiento de estándares de seguridad y la presentación de informes. Se recomienda establecer una línea de informes con subcomités de industria para garantizar que se mantenga y actualice un registro nacional de incidentes con el fin de informar los niveles de riesgo nacionales y el modelado de amenazas futuras.

Línea Estratégica 5.2 Implementación de medidas de seguridad de los Sistemas de Información y Telecomunicaciones de la Administración Pública

Si bien la mayoría de los actores indicaron que no estaban seguros de si se realizó el **diseño de protocolos de ciberseguridad para los Ministerios del Poder Ejecutivo, acorde al estado de madurez de cada una de las instituciones y según las necesidades del sector público**, un encuestado resaltó que *"a través del CSIRT se han realizado evaluaciones del estado de los sistemas de los ministerios".* La ENC 2017 determina que el CSIRT-CR del MICITT funcionará como colaborador y asesor en el diseño de dichas herramientas. Aunque no está claro si esto se ha implementado, cuando se preguntó a qué entidad se informa en caso de un incidente de infraestructura crítica, la gran mayoría identificó al CSIRT-CR del MICTT como la entidad identificada para responder a las amenazas cibernéticas en la infraestructura crítica.

RECOMENDACIÓN

Se recomienda que los informes de nivel ejecutivo con un análisis de la información sobre amenazas se proporcionen a los tomadores de decisiones para guiar la asignación de activos clave, considerando que las alertas se envían comúnmente al personal técnico y de TIC y no necesariamente a aquellos con autoridad para asignar recursos según sea necesario. Generar concientización entre los jefes de entidades gubernamentales sobre el posible impacto que los incidentes cibernéticos pueden tener en sus operaciones debe elevarse, lo cual podría afectaría la forma en que asignan los recursos adecuados para abordar las vulnerabilidades de respuesta a incidentes.

Los actores claves identificaron las siguientes barreras para el intercambio de información y cooperación relacionadas con la protección de los sistemas cibernéticos de la infraestructura crítica de Costa Rica:

1. **La falta de estándares de comunicación y la definición de tipos de información, lo que fomenta la colaboración en el entendimiento conjunto del entorno de amenazas y la coordinación de acciones conjuntas para la detección y respuesta a eventos e incidentes.**
2. **Existe una cultura de secretismo en cuanto a vulnerabilidades y ataques, lo que impide que instituciones y empresas sean más proactivas en la colaboración conjunta en la lucha contra grupos organizados que operan de forma similar con diferentes objetivos.**
3. **Desconocer los mecanismos, dinámicas y objetivos del intercambio de información y cooperación. Posible falta de protocolos, reglas y regulaciones para sustentar los procedimientos.**

Nivel de implementación

Considerando todas las líneas estratégicas, se les pidió a los encuestados, en una escala de 1 a 5 (1-estar muy de acuerdo en que se implementó el objetivo y 5-estar muy en desacuerdo con que se implementó el objetivo), que indicaran su opinión sobre el nivel de implementación. La implementación de este objetivo tuvo un promedio de 2.95, dado a que mayoritariamente no hubo conocimiento de la creación de una comisión para generar políticas públicas con el fin de garantizar la operatividad y estabilidad de continua de servicios de infraestructura critica. No obstante, la identificación de infraestructuras críticas del país ha sido señalado como una acción que fue impleméntenla de manera significativa, iniciativa que, de acuerdo con la ENC 2017, era crucial para la aplicación de medidas de seguridad. Esto constituye un gran avance en la capacidad nacional de protección de infraestructura critica.

	1. Totalmente en desacuerdo	2. En desacuerdo	3. Indeciso	4. De acuerdo	5. Totalmente de acuerdo	Total	Promedio
1. Se han identificado las infraestructuras críticas del país como paso crucial para la aplicación de medidas de seguridad	7.14% 1	7.14% 1	50.00% 7	35.71% 5	0.00% 0	14	3.14
2. Se ha creado una comisión para la generación de la política pública conformada por un representante y un suplente de cada una de las instituciones públicas y entidades privadas identificadas, con el fin de garantizar la operatividad y estabilidad continua de estos servicios	7.14% 1	14.29% 2	78.57% 11	0.00% 0	0.00% 0	14	2.71
3. Se han diseñado protocolos de ciberseguridad para los Ministerios del Poder Ejecutivo, acorde al estado de madurez de cada una de las instituciones y según las necesidades existentes en el sector público	7.14% 1	0.00% 0	78.57% 11	14.29% 2	0.00% 0	14	3.00

Gestión de Riesgo

La adopción de un proceso de gestión de riesgo es esencial para garantizar la continuidad y operacionalización de una entidad ante un incidente cibernético. La planificación de la gestión de riesgo permite tomar medidas proactivas y disminuir la incertidumbre que comúnmente conllevan las amenazas cibernéticas. La siguiente sección evalúa el nivel de coordinación y comunicación entre distintos sectores, como el sector financiero, gubernamental y privado, en la implementación de un modelo de gestión de riesgo para cada institución.

Línea Estratégica 6.1 Mejorar la seguridad de los productos y servicios vinculados con la seguridad de la información

La ENC 2017 destaca las normas como NIST, INTE/ISO/IEC, COBIT, recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT), que deben tenerse en cuenta al **promover el desarrollo e implementación de estándares de ciberseguridad para el funcionamiento de organizaciones públicas y privadas.** A lo cual el **57%** de los encuestados indicó que no estaba seguro, mientras que el **28%** indicó que tener conocimiento sobre normas de ciberseguridad que se promueven en organizaciones públicas y privadas. Los encuestados que se manifestaron afirmativamente en la implementación de esta acción indicaron que conocen que esta se está implementando en el sector público y que el MICITT hace recomendaciones importantes.

En este sentido, dentro del marco de funciones del CSIRT Nacional se realizan análisis de los portales web de los Ministerios, y Municipalidades, además de instituciones que solicitan realizar los análisis, lo cual permite generar un informe detallado del estado actual de los sitios web. El resultado de dichos análisis se entrega a cada institución de forma oficial y confidencial, brindando datos valiosos para que el departamento de tecnologías de cada institución corrija las deficiencias encontradas a fin de evitar y prevenir incidentes informáticos.

RECOMENDACIÓN

Se debe considerar un programa de concientización y posiblemente grupos de trabajo entre las partes interesadas para desarrollar estándares específicos a cada industria a nivel nacional. Es evidente que, si bien el gobierno ha implementado varios estándares, existe la oportunidad de construir mayores líneas de comunicación con las partes interesadas para aumentar su conocimiento de estos esfuerzos.

Línea Estratégica 6.2 Implementación de mejores prácticas y definición de requisitos mínimos de seguridad de la información en el Sector Financiero

Dentro de esta línea estratégica, se prioriza la creación de un mecanismo de coordinación y comunicación con el sector financiero. Algunos actores señalan que se han establecido comunicación recurrente con el sistema financiero a través del CSIRT nacional. Al respecto, la herramienta de monitoreo del CSIRT-CR, está en constante revisión del estado de los portales de los sitios web del sector financiero, así como de los Ministerios, Municipalidades, Instituciones adscritas y autónomas, que permitan brindar en tiempo real cuando algún portal sufre algún incidente. Igualmente, el CSIRT Nacional recibe información internacional de colaboración sobre Ataques de Denegación de Servicio, Defacement, vulnerabilidades, etc., que permite reportar a distintas instituciones con el objetivo de que estas tomen las acciones adecuadas para corregir la situación.

Línea Estratégica 6.3 Adopción de medidas de seguridad de referencia

Ante la pregunta acerca de que si se **ha promovido la incorporación de medidas adecuadas de seguridad, privacidad y propiedad de los datos, para aquellos servicios que se prestan a la ciudadanía, favoreciendo el uso de certificados digitales de autenticación y enfatizando la implementación de normas estrictas para la protección de datos en los servicios de almacenamiento, como los de computación en la nube**, el **64%** de los encuestados que respondieron indicaron que no estaban seguros, mientras que el **14%** respondió afirmativamente.

Línea Estratégica 6.4 Establecimiento de una red de intercambio de información para las entidades gubernamentales

Una comunicación y coordinación adecuada tienen el potencial de reducir los riesgos y minimizar los posibles impactos de ciberamenazas e incidentes cibernéticos. Cuando se preguntó a los encuestados sobre si se ha **facilitado y promovido el intercambio de información entre los responsables de seguridad de la información del gobierno a través de una red confiable,** las partes interesadas que respondieron indicaron que no estaban seguras acerca de esta iniciativa.

RECOMENDACIÓN

Para el nueva ENC se recomienda que se consideren canales de comunicación claros entre las entidades gubernamentales sobre las pautas y estándares de seguridad de referencia. Se podría asignar a una entidad centralizada la responsabilidad de desarrollar estándares de referencia, considerando las diversas infraestructuras de TIC utilizadas, y establecer campañas de sensibilización, así como talleres para su implementación. Esta iniciativa podría incluir trabajar con propietarios y operadores de Infraestructuras Críticas Nacionales.

Una entidad centralizada que pudiera cumplir con esta función deberá poseer el mandato y la capacidad técnica para desarrollar y monitorear la implementación de estas normas. Esta entidad también debe poseer la capacidad de llevar a cabo acuerdos de cooperación con otras agencias, como la academia y la comunidad técnica, con la finalidad de disponer de mejores condiciones para mantenerse al tanto de las tendencias emergentes.

Figura 4 Posibles funciones para la entidad centralizada

Línea Estratégica 6.5 Fortalecimiento del Centro de Respuesta a Incidentes de Seguridad Informática CSIRT-CR

Un análisis alentador fue que la mitad de los actores que respondieron, indicaron que se **ha fortalecido la resiliencia frente a disturbios e incidentes cibernéticos**, destacando que esto comúnmente se ha hecho internamente a nivel institucional. La asignación de recursos exclusivos para atender a todos los componentes del CSIRT-CR y la promoción y apoyo para establecer CSIRT sectoriales se incluyó en la ENC 2017. Las partes interesadas aluden al hecho que depositan una gran confianza en CSIRT-CR y, por lo tanto, deben percibirlo como una entidad competente para abordar la respuesta a incidentes a nivel nacional. Una de las acciones destables que se ha realizado desde el CSIRT Nacional son las alertas técnicas. En los casos de recibir información internacional, o nacional, de posibles afectaciones o vulnerabilidades a la ciberseguridad, el CSIRT-CR emite alertas técnicas y actualmente se han realizado 323 alertas técnicas. Además, actualmente en colaboración la OEA/CICTE se está trabajando en el desarrollo del Malware Information Sharing Platform (MISP), para el intercambio de información en ciberseguridad en conjunto con el CSIRT-CR y las instituciones de las redes de enlaces de ciberseguridad, iniciando con las instituciones del sector financiero.

Nivel de implementación

El nivel de implementación de un medio de 3 sugiere que este objetivo se implementó parcialmente. Consecuentemente, se recomienda tomar medidas adecuadas que permitan generar la visibilidad del mandato legal del CSIRT-CR como coordinador nacional en gestión y respuesta a incidentes cibernéticos.

Cooperación y Compromiso Internacional

La naturaleza interconectada de la ciberseguridad hace que la cooperación internacional tenga un enfoque primordial para implementar con éxito todos los objetivos adscritos a la ENC 2017, así como la próxima estrategia a desarrollar. Las ciberamenazas tienen la capacidad de impactar significativamente la seguridad internacional y la economía global. Asimismo, dado que el ciberespacio tiene un carácter evolutivo rápido y constante, la necesidad del intercambio de conocimiento y mejores prácticas es indispensable para asegurar un ciberespacio nacional próspero que permita conducir un país hacia un panorama más próspero y seguro.

Línea Estratégica 7.1 Involucrar a la comunidad internacional en el apoyo de los objetivos de la Estrategia Nacional

La ENC 2017 considera la cooperación internacional como clave para avanzar en los ámbitos de la ciberseguridad, tales como las medidas penales, técnicas, educativas, desarrollo de capacidades y seguridad. Una de las líneas estratégicas de este objetivo se basa en fomentar la participación en foros especializados a nivel nacional e internacional con el fin de fortalecer la cooperación en ciberseguridad con otros aliados. Solo en el año 2021, Costa Rica ha participado en distintas estancias regionales e internacionales, incluyendo la conferencia "Iniciativa Regional de Educación y Capacitación en Seguridad Cibernética (RICET)", en el Sistema de la Integración Centroamericana (SICA) sobre la Estrategia Regional Digital para Centroamérica, en el foro regional para la Cooperación Digital con Corea, así como en el Simposio de Ciberseguridad de la OEA, convocado Comité Interamericano Contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE).

En virtud de la activa participación de Costa Rica en foros nacionales e internacionales relacionados en materia de ciberseguridad, se evidencia la gestión que se ha realizado para fortalecer los recursos y la infraestructura esencial de ciberseguridad del país a través de pasantías, capacitaciones, talleres, entre otros.

El fortalecimiento de capacidades se ha realizado mediante la cooperación con distintos gobiernos, incluyendo Israel, España, Estados Unidos, entre otros. Así como con organismos expertos en la materia como el Programa de Ciberseguridad de CICTE/OEA mediante el programa "Creando una Trayectoria Profesional en Ciberseguridad, Pathways2Progress" que fomenta la capacitación de estudiantes en seguridad digital, así como el "CyberWomen Challenge". Adicionalmente, Costa Rica ha gestionado cooperación con Cyber Resilience for Development (Cyber4Dev) de la Unión Europea diseñado para promover la ciberresistencia y la ciberseguridad.

Las siguientes son sugerencias para considerar en este objetivo específico para la siguiente estrategia por desarrollar:

1. **Además de valorar la participación en foros internacionales, se pueda profundizar en las membresías del país en instancias internacionales que tratan el tema de ciberseguridad como el CICTE, ONU u otras, que va más allá de solo participación o cooperación internacional, ya que en ellas se toman decisiones de política exterior que para el caso de Costa Rica tenemos que coordinar con cancillería y con otras instancias nacionales, ya que muchas veces en estos espacios se ven los temas de manera más integral por ejemplo la parte de justicia y ciberdelincuencia (que si bien son cosas distintas, pueden ser complementarias), y en el tema internacional algunas veces lo trabajan de manera integral.**
2. **La estrategia sugiera una hoja de ruta, por ejemplo, en la solicitud de capacitaciones, ya que muchas instancias internacionales brindan estas capacitaciones, pero no hay una definición adecuada, para pedirle a quién y hasta donde llegar para que toda la cooperación brindada sea atinente no haya traslapes y repeticiones, si no más bien complementariedades que aprovechen mejor el tiempo y los recursos.**
3. **Desde la Unidad de Cooperación Internacional, hemos tratado de hacer un ejercicio de identificación de países que trabajan el tema de ciberseguridad, como un tipo de mapeo, con los cuales no con todos tenemos relación aún debido a la falta de recurso humano para poder explotar más este punto, pero podría ser interesante considerar algo así para la estrategia.**

Nivel de implementación

El nivel de implementación de promedio 3 sugiere que este objetivo fue implementado. Sin embargo, este objetivo requiere de mayor visibilidad y revisión para optimizar las oportunidades que permite la cooperación internacional.

Implementación, Seguimiento y Evaluación

La adopción de una metodología de implementación y seguimiento es parte esencial para asegurar que una ENC pueda traspasar de la elaboración a la implementación. Adicionalmente, factores como la designación de entes responsables de la implementación, seguimiento y actualización, así como la asignación adecuada de recursos financieros y humanos son elementos claves para la operacionalización y continuidad de la estrategia. La siguiente sección evalúa el seguimiento y evaluación dedicada a la implementación de la ENC 2017.

Línea Estratégica 8.1 Realizar el seguimiento de la aplicación de la Estrategia Nacional de Ciberseguridad, y evaluar el grado de éxito de cumplimiento de sus objetivos

Para implementar adecuadamente una estrategia de ciberseguridad, deben de existir mecanismos de monitoreo y evaluación. En este sentido, la ENC 2017 determina que se debe **diseñar y aplicar una metodología de implementación y seguimiento que permita evaluar el cumplimiento de las líneas de acción planteadas en la estrategia.** Para ejecutar esto, la ENC 2017 asigna al MICITT como entidad responsable de solicitar información sobre el avance de las iniciativas. Además, como Coordinador Nacional se le otorga la facultad de evaluar las actividades, proponer recomendaciones e informar anualmente al Presidente de la República y al Consejo de Gobierno sobre los avances de implementación de la estrategia. Dentro del alcance del CSIRT-CR, una de sus principales funciones es el desarrollo, revisión y seguimiento de la Estrategia Nacional de Ciberseguridad. Dicha función actualmente se está llevando a cabo al ser la entidad que lidera la revisión de la ENC 2017.

Línea Estratégica 8.2 Realizar una revisión y actualización de la Estrategia Nacional de Ciberseguridad cada dos años o según sea necesario

La ENC 2017 asigna la responsabilidad al **Comité Consultivo de analizar la estrategia y emitir informes que contengan recomendaciones para efectuar las modificaciones que considere oportunas.** Los actores que respondieron sobre si se implementó este último indicaron que no estaban seguros y se necesita mayor información para obtener un panorama acertado. No obstante, el hecho de que este informe tenga como objetivo principal analizar el nivel de implementación de la ENC 2017 y a brindar recomendaciones que permitan servir como punto de partida para la próxima ENC de Costa Rica indica que esta línea estratégica se ha accionado.

Nivel de implementación

El nivel de implementación obtuvo un promedio de 3, sugiriendo que este objetivo fue implementado a cierta extensión. Sin embargo, se requiere más información para analizar adecuadamente el alcance de que obtuvo este objetivo.

SEIS

Contribución de Expertos

CYBER4Dev

Introducción

Costa Rica publicó su primera estrategia nacional de ciberseguridad en 2017 para apoyar el proceso de digitalización en curso del país. Costa Rica ha identificado el uso de las TIC como uno de los factores clave que permiten mejorar el desarrollo nacional. De 2016 a 2020, el país ha demostrado avances en áreas de política y estrategia de ciberseguridad, cibercultura y sociedad, educación en ciberseguridad, estándares y marcos legales[9]. Costa Rica ocupa el lugar 55º en el Índice Nacional de Seguridad Cibernética[10] y el puesto 76º en el Índice Mundial de Ciberseguridad[11]. En el hemisferio occidental, Costa Rica está entre los mejores, ocupando el 8º puesto, entre Chile y Colombia. En la región de América Latina y el Caribe, Costa Rica es uno de los países más digitalizados y se ha desarrollado significativamente durante la última década. Los usuarios de internet representaron más del 74% de la población en 2018, con mayores aumentos en el año anterior. También mejoró el desempeño en el Índice de Gobierno Electrónico, que mide la disposición y capacidad de las administraciones nacionales para utilizar la tecnología de la información y las comunicaciones (TIC). El país aún sigue rezagado en cuanto a las políticas de datos de gobiernos abierto, pues se sitúa por debajo de la región y los promedios de la OCDE en los índices respectivos de la OCDE.[12]

Este proceso de digitalización en Costa Rica exige también medidas adecuadas para gestionar y mitigar los riesgos relacionados con la digitalización. La seguridad cibernética es uno de los desafíos clave de la digitalización y, por lo tanto, la planificación nacional de las actividades respectivas mediante el establecimiento y actualización periódica de la Estrategia Nacional de Ciberseguridad es esencial para todo el país y la sociedad.

Este capítulo tiene como objetivo revisar la actual Estrategia Nacional de Ciberseguridad - Costa Rica 2017 (ENC 2017) a partir de documentos de disponibilidad pública, centrándose en los objetivos de esta estrategia y sin pretender proporcionar ninguna evaluación independiente al actual nivel de madurez de ciberseguridad de Costa Rica ni la implementación de la estrategia.

9 Informe de seguridad cibernética de 2020: Riesgos de ciberseguridad, progreso y camino a seguir en América Latina y el Caribe https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
10 https://ncsi.ega.ee/
11 https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/
12 OCDE y otros (2020), Latin American Economic Outlook 2020: Digital Transformation for Building Back Better, OCDE Publishing, París, https://doi.org/10.1787/e6e864fb-en.

Principios, estructura y objetivos de la estrategia de 2017

La estrategia de Costa Rica se basa en los siguientes cuatro principios:

- ☑ **Las personas son prioritarias**
- ☑ **Respeto por los derechos humanos y la privacidad**
- ☑ **Coordinación y corresponsabilidad de múltiples partes interesadas**
- ☑ **Cooperación internacional**

La ENC de Costa Rica 2017 es un buen ejemplo del enfoque de "Toda la Nación"[13], en el que además de la estrategia del Gobierno se establecen metas y objetivos para varias partes interesadas a fin de garantizar un enfoque integral, en el que el modelo de gestión de la ciberseguridad se basa más en la cooperación que en la coordinación pura.

El objetivo general de la estrategia establece una clara declaración de misión y visión- el objetivo es desarrollar un marco rector para las acciones del país en materia de seguridad en el uso de las TIC, promoviendo la coordinación y cooperación de los múltiples actores y fomentando la educación, medidas de prevención y mitigación que hagan frente a los riesgos relacionados con el uso de las TIC para lograr un entorno más seguro y confiable para todos los residentes[14] del país.

También se establecieron en la estrategia un número de objetivos y metas específicos (5 líneas estratégicas) para respaldar el objetivo general de aumentar la ciberseguridad y la resiliencia del país.

Áreas de enfoque generalmente reconocidas de la Estrategia Nacional de Ciberseguridad[15]:	Comentarios a la ENC-2017
Gestión: creación de una estructura, modelos de coordinación y cooperación, asignación de recursos y planes de aplicación.	Sin comentarios. *La estrategia aborda la necesidad de una coordinación nacional con las partes interesadas para definir su papel y línea de acción en el proceso de mitigación, gestión, recuperación y continuidad en caso de un incidente de ciberseguridad. La estrategia define como partes interesadas el sector público, la academia, las organizaciones no gubernamentales, el sector privado, la sociedad civil y la comunidad técnica. Designa la función de Coordinador Nacional, la necesidad de colaboración entre el sector público y el privado. (Objetivo específico 1)*

13 Hathaway M.E,Klimburg (2012) Consideraciones Preliminares: Sobre Ciberseguridad Nacional, Manual de marco de seguridad cibernética nacional. Publicación del COE de la CCD de la OTAN, Tallin 2012

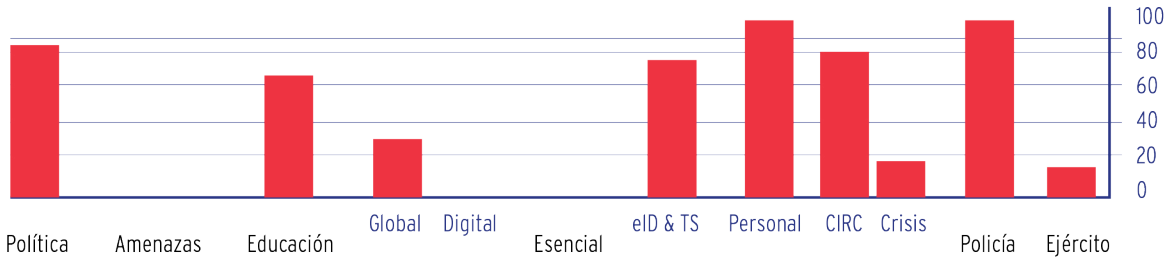
14 https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

15 Por ejemplo: la Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (ComSec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia para la Defensa Cibernética Cooperativa de la OTAN (CCD COE de la OTAN). 2018. Guía para el Desarrollo de una Estrategia Nacional de Ciberseguridad - Compromiso estratégico en ciberseguridad. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Áreas de enfoque generalmente reconocidas de la Estrategia Nacional de Ciberseguridad:	Comentarios a la ENC-2017
Gestión de riesgos: definir un enfoque de gestión de riesgos, una metodología común de gestión de riesgos y desarrollo de perfiles de riesgo sectoriales.	Se necesitan algunas mejoras. *La estrategia también podría hacer hincapié en el papel de la recopilación, el análisis y la distribución de datos sobre amenazas. Además, la red de intercambio de información, una herramienta que podría servir como plataforma de inteligencia de amenazas (línea estratégica 6.4), se centra únicamente en entidades gubernamentales.*
Preparación y resiliencia: establecimiento de capacidad de respuesta ante incidentes, planificación de contingencias, uso compartido de información y ejercicios cibernéticos.	Se necesitan algunas mejoras. *La estrategia también podría abordar la administración de crisis cibernéticas, la planificación de contingencias y recuperación ante desastres, y los ejercicios de ciberseguridad.*
Infraestructura crítica y servicios esenciales: establecimiento de un enfoque de administración de riesgos para proteger la infraestructura crítica, definir líneas de base de ciberseguridad, etc.	Se necesitan algunas mejoras. *El Objetivo específico 5 se refiere a la protección de la infraestructura crítica, sin embargo, no incluye mecanismos para el seguimiento y actualizaciones regulares de la lista de elementos y proveedores de la infraestructura crítica.*
Creación de capacidades y concientización: educación sobre seguridad cibernética, papel de la academia, capacitación y campañas de concienciación.	Se necesitan algunas mejoras. *La estrategia no cubre aspectos de concientización pública y la destreza cibernética/TIC que generalmente se abordan a través de la educación básica, campañas de sensibilización pública, etc.*
Legislación: establecer un marco legal adecuado para combatir el delito cibernético, proteger la infraestructura crítica, la privacidad, etc.	Sin comentarios.
Cooperación internacional.	Sin comentarios.

A partir del 25 de noviembre de 2019, Costa Rica se ubica en el puesto 55º del Índice de ciberseguridad de la CSI[16]. La evaluación se basa en los datos proporcionados por los funcionarios de Costa Rica. En general (véase la ilustración a continuación) estos datos se muestran en consonancia con las observaciones sobre el contenido de la estrategia.

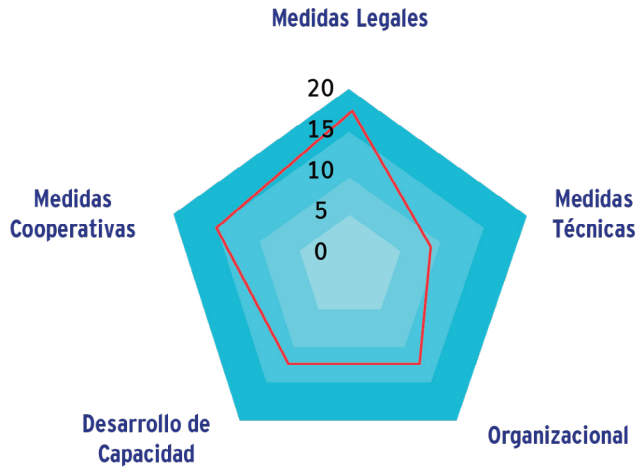
Porcentaje de cumplimiento del NCSI



Origen: Informe EGA, NCSI sobre Costa Rica

Las observaciones también están respaldadas por la evaluación realizada por la UIT durante el proceso de la SIG[17], como se muestra en el siguiente gráfico.

Costa Rica



Nivel de desarrollo:
País en desarrollo

Área(s) de fuerza relativa
Medidas Legales

Área(s) de crecimiento potencial
Medidas Técnicas

Puntaje General	Medidas Legales	Medidas Técnicas	Medidas Organizacionales	Desarrollo de Capacidad	Medidas Cooperativas
67.45	17.62	9.14	12.66	12.11	15.93

Fuente: ITE Global Cybersecurity Index v4, 2021

Sin embargo, es importante entender que la clasificación en los índices mencionados no se basa plenamente en el contenido y la forma de las Estrategias Nacionales de Ciberseguridad, sino más bien en las medidas y marcos ya existentes. Por lo tanto, la evolución, planeada en la estrategia, puede no estar reflejada en las clasificaciones. No se tuvo acceso al plan de implementación de la ENC 2017 para este capítulo, por lo que las observaciones a continuación se basan únicamente en el texto de la estrategia.

16 https://ncsi.ega.ee/country/cr/
17 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

RECOMENDACIÓN

La planificación estratégica nacional suele definirse como un enfoque estructurado y consultivo para la adopción de decisiones importantes y la aplicación de medidas importantes. Este enfoque forma y subyace a los acuerdos nacionales, las actividades y sus propósitos. También es importante considerar el desarrollo de estrategias como un proceso continuo y con visión de futuro. Una estrategia no es estática, pero debe preverse un proceso integrado para actualizarla y adaptarla a las necesidades futuras durante la etapa de redacción. La estrategia final debe incluir opciones informadas y el patrón de acción resultante para las decisiones futuras. La estrategia también debe incluir un plan de acción de alto nivel sobre cómo alcanzar los objetivos deseados, así como indicadores con los que medir los logros.

Los pasos clave para el desarrollo de una estrategia nacional de ciberseguridad pueden describirse como:

1. Iniciar el proceso de estrategia y acordar los pasos del proceso
2. Identificar a las personas e instituciones involucradas en el desarrollo de la estrategia, determinando los poderes de las partes de acuerdo con actos legales y reglamentarios
3. Acordar misión y valores
4. Acordar el entorno externo e interno e identificar fortalezas, debilidades, oportunidades y amenazas
5. Identificar tareas estratégicas
6. Desarrollar una estrategia para realizar las tareas: un proceso a la deriva
7. Revisión y adopción de la estrategia
8. Crear una visión organizacional eficaz y un proceso para implementar la estrategia
9. Evaluar la estrategia aplicada, el proceso de planificación estratégica y su implementación

Origen: Planificación estratégica nacional para la seguridad cibernética[18]

En general, la estrategia nacional debe velar por que se aborden los siguientes factores clave de éxito[19]:

- ☑ **Legislación efectiva**
- ☑ **Competencias suficientes**
- ☑ **Enlaces a la toma de decisiones políticas**
- ☑ **Capacidades y experiencia**
- ☑ **Recursos financieros**

Además, es importante tener en cuenta que los incidentes de ciberseguridad nunca se pueden prevenir por completo, ni siquiera con las medidas de seguridad más estrictas. La rápida digitalización del desarrollo y la economía digital, por ejemplo, las industrias inteligentes como Smart Agricultura, el transporte autónomo, etc., también incrementan el potencial de graves incidentes de seguridad. Por lo tanto, además de prevenir incidentes, la estrategia debe centrarse en la capacidad de resistencia cibernética; es decir, el control y la reducción de los daños causados por los incidentes.

Esto requiere dos tipos de acción: en primer lugar, medidas proactivas destinadas a prevenir incidentes, y, en segundo lugar, medidas reactivas para controlar y reducir los daños.

18 Vaks, T.(2020) National Strategic Planning for Cyber Security. Ciberseguridad nacional en la práctica. Disponible: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf
19 Martti Lehto & Jarno Limnéll (2021) Liderazgo estratégico en seguridad cibernética, caso Finlandia, Information Security Journal: Una perspectiva global, 30:3, 139-148, DOI: 10.1080/1939355.2020.1813851

Origen: Seguridad cibernética resistente[20]

La estrategia debe abordar la necesidad de identificar y comprender las amenazas potenciales (inteligencia de amenazas) y los riesgos asociados con estas amenazas (conciencia de riesgos). También es necesario contar con recursos para detectar incidentes (administración de incidentes) y hacer frente a ellos, y para planificar actividades y recursos a fin de hacer frente a los daños causados por los incidentes (recuperación). La existencia de tales medidas, por un lado, incrementará la capacidad de prevenir incidentes al aumentar la seguridad total y, por otro lado, reducirá significativamente el impacto adverso de los incidentes en la sociedad costarricense.

Se recomendaría que la nueva estrategia de seguridad cibernética preste atención a los siguientes aspectos:

Visión clara y declaración de objetivos. Por ejemplo: Fomentar un ciberentorno de confianza que optimice la preparación de Costa Rica en materia de ciberseguridad y las capacidades de coordinación para abordar la exposición de las naciones al riesgo cibernético. Visión – Costa Rica Ciber segura y protegida.

Considerar la creación del Consejo Nacional de Ciberseguridad - Asegurar un alto nivel de control político y alineación con los intereses de la Seguridad Nacional. Organismos de coordinación de alto nivel a nivel gubernamental. Reuniones regulares, organismo de supervisión para la implementación de CSS. Inicio y supervisión de los respectivos actos legales, regulaciones, etc.

Fortalecer la gestión de riesgos, considerar la posibilidad de establecer una metodología común de evaluación de los riesgos cibernéticos, evaluaciones periódicas de los riesgos en los sectores, un repositorio de riesgos, un registro de incidentes cibernéticos y un informe obligatorio.

Establecimiento de un organismo central de coordinación para la gestión de incidentes a gran escala y el intercambio de información.

Informes periódicos de Análisis de Riesgos y Panorama de Amenazas tanto para el sector público como para el privado (incluye la versión confidencial y pública).

Desarrollo de planes de gestión de incidentes cibernéticos a gran escala como parte de la planificación nacional de emergencia.

Definición clara de IIC (infraestructura de información crítica).

20 Vaks, T.(2020) National Strategic Planning for Cyber Security. Ciberseguridad nacional en la práctica. Disponible: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

Ciberseguridad de Infrastructures Críticas.

Desarrollar un estándar básico de ciberseguridad nacional para infraestructuras críticas que incluya requisitos de alto nivel para software y hardware que se puedan utilizar en servicios vitales.

Desarrollar un programa integral para aumentar la conciencia sobre el delito cibernético en las poblaciones. Se puede implementar como parte de las campañas de concienciación digital (IT), en cooperación con las telecomunicaciones, los proveedores de servicios de pago, etc.

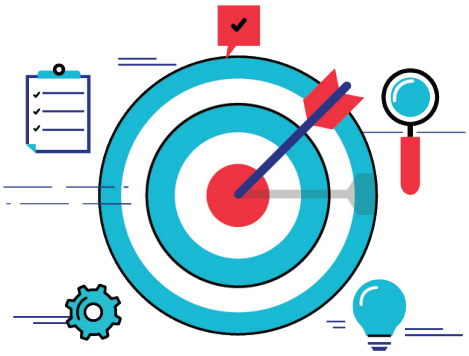
Desarrollar e incluir programas básicos de educación en ciberseguridad para cada nivel educativo.

SIETE

Reflexiones Finales

Implementación General de la ENC

Basado en los resultados del cuestionario, existe cierta dificultad para determinar cuáles de estas iniciativas se implementaron y en qué medida lograron con éxito su propósito previsto, ya que no todas las preguntas planteadas a los encuestados fueron respondidas de manera uniforme y/o con la misma cantidad de información. Además, se pidió a las partes interesadas que completaran cuestionarios que a menudo incluían preguntas fuera de su ámbito de trabajo de experiencia. Como tal, muchas de las respuestas podrían haber obtenido un resultado más alto si las preguntas se respondieran exclusivamente en función del alcance del trabajo del encuestado. Por tanto, las conclusiones extraídas de estos resultados se limitan a cuestiones de conocimiento y visibilidad de la ENC 2017.



La gran cantidad de respuestas negativas o "no estoy seguro(a)" indica que es posible que la ENC no haya sido comunicada y sensibilizada de manera estratégica y suficiente entre los actores clave dentro de Costa Rica. Esto incluye las entidades y agencias gubernamentales que pueden haber tenido alguna utilidad en la etapa de implementación. Por lo tanto, se recomienda que la próxima iteración incluya **una estrategia de comunicación integral y un plan de acción/implementación**, con el fin de comprender cuáles de las iniciativas propuestas en la estrategia disponían de un implementador líder, cuáles fueron efectivamente implementadas y en qué medida tuvieron éxito en lograr su propósito previsto.

Éxitos

I. El análisis de respuestas recopiladas por parte de las partes interesadas sugiere que uno de los elementos más exitosos de la ENC 2017 fue la consolidación del CSIRT-CR como una entidad clave en la coordinación nacional en materia de seguridad informática y cibernética. Según las respuestas escritas, las partes interesadas parecen depositar una gran confianza en el CSIRT-CR y, por lo tanto, es evidente que el CSIRT-CR es una institución que ejerce sus funciones de acuerdo con el Decreto: Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR Nº 37052-MICIT.

II. El MICITT se ha consolidado como la entidad líder en ciberseguridad a nivel nacional, esto es evidente por las frecuentes citaciones de la institución por parte de las partes interesadas como entidad encargada de llevar a cabo esfuerzos nacionales en materia de ciberseguridad.

III. Otro éxito a destacar es el aumento de iniciativas de concienciación que se están implementando y que demuestran el avance de Costa Rica en la adquisición de una cultura de ciberseguridad.

IV. Con respecto al objetivo 7, cooperación y compromiso internacional, a lo largo de las respuestas de los cuestionarios, los encuestados destacaron diversas iniciativas que se están llevando a cabo en colaboración con socios internacionales en distintas áreas distintivas de seguridad cibernética, demostrando el compromiso de cooperación internacional del país. Asimismo, en los últimos años, Costa Rica destaca como un país líder en materia de ciberseguridad a nivel regional.

Oportunidades

Una de las oportunidades más destacables es la necesidad de realizar un mapeo de las instituciones que desempañan un papel clave en la implementación en conjunto con MICITT y CSIRT-CR. Los grupos de interés sugirieron varias entidades que están involucradas en distintos ámbitos de ciberseguridad. Sin embargo, la ENC 2017 no define claramente un rol para cada entidad. No está claro el alcance que tiene el Comité Consultivo en la implementación y operacionalizad de las funcionen adscritas a la ENC 2017. Por lo tanto, se recomienda desarrollar un mecanismo y una metodología que permita establecer un nivel de rendición de cuentas a los objetivos que se proponen y comprometen a efectuar en la próxima ENC. Esto podría contribuir a asegurar que las iniciativas se monitoreen adecuadamente y se actúe con prontitud, a fin de generar confianza en el cumplimiento de los objetivos estratégicos propuestos en la próxima estrategia. Esta responsabilidad se puede lograr optimizar desarrollando un plan de acción que se publique simultáneamente con la nueva estrategia, o poco después, para permitir que se comprometan acciones concretas a desarrollen posteriormente.

Además, se puede concluir que Costa Rica puede beneficiarse del establecimiento de una comunicación coordinada con las partes interesadas y los profesionales que residen y operan dentro del país. El número limitado de respuestas puede ser indicativo de una brecha en la coordinación efectiva con estas partes interesadas. Puede sugerir que se necesita enfocar esfuerzos para optimizar la colaboración con socios al completar recursos, tanto financieros como humanos, para llevar a cabo iniciativas de mutuo interés, al igual que establecer canales de comunicación más coordinados y cohesivos con las partes interesadas que afecten directamente la implementación de la nueva estrategia. Una mayor concienciación de estas partes interesadas puede mejorar las iniciativas existentes y garantizar que se tengan debidamente en cuenta las necesidades y realidades de ciberseguridad que existen en la sociedad de Costa Rica.

Igualmente, se observó que había cierto margen de mejora para facilitar los flujos de información del CSIRT-CR al sector privado, en particular a los propietarios de infraestructura crítica, en el aspecto técnico y en el establecimiento de estándares de ciberseguridad de referencia. También se recomienda aumentar la concienciación sobre las iniciativas de creación de capacidad, ya que muchos de los encuestados indicaron un conocimiento desproporcionado, dado que el nivel de conocimiento sobre estas dependía de la organización en la que se desempeñaba la persona. En consecuencia, una de las necesidades más urgentes podría considerarse que es la creación de una estructura de gobernanza y poner en prueba su funcionamiento durante los ejercicios de respuesta cibernética, ya que estos son pasos vitales para mejorar estructura institucional para efectuar respuesta en caso de incidentes cibernéticos nacionales. Además, proporcionará una mayor claridad sobre las estructuras de gestión y los mandatos del marco de gobernanza.

Prioridades para la próxima ENC

Se recomienda que se considere una entidad gubernamental designada, así como cualquier otra entidad que este involucrada en el proceso de implementación, como responsable de evaluar la implementación efectiva de cada iniciativa determinada en la estrategia a desarrollar. La atención también debe centrarse en el desarrollo de un plan de acción complementario para implementar cualquier iniciativa previamente publicitada y recientemente desarrollada que aún no se haya llevado a cabo en función de cumplir con los objetivos de la ENC 2017. Presentar un plan de implementación con mecanismos mensurables demostraría un compromiso con el cumplimiento de los objetivos de la estrategia y contribuiría a generar confianza y conocimiento de la estrategia entre las partes interesadas, al igual que mejorar los desafíos identificados a lo largo de ENC 2017. Al mismo tiempo, es muy recomendable 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 dentro del marco de la siguiente ENC. Para efectuar esta última recomendación, se debe de tomar en cuenta la realización de un mapeo de las interdependencias transfronterizas e intersectoriales de las infraestructuras de información críticas y las partes interesadas relacionadas.

En materia de desarrollo de capacidades, dado que existen algunos programas de educación secundaria, en el campo de la ciberseguridad, se debe considerar un mapeo de estos cursos y centralizar el acceso a la información sobre ellos. Este recurso centralizado también debe promoverse a nivel nacional y se recomienda ser incluido en la nueva ENC. Asimismo, se considera importante que esfuerzos en materia de educación y ciberseguridad sean llevados a cabo de manera conjunta con el ministerio responsable de la educación desde el inicio de la elaboración de la siguiente estrategia y que se acuerden acciones.

Dado que el sector turístico en Costa Rica representa el 8.2% de su PIB, la ciberseguridad debe ser un elemento por considerar, a fin de contribuir a la sostenibilidad económica del sector.[21] Es por esto por lo que se recomienda que se tenga en cuanta en la siguiente estrategia actividades que promuevan la interdependencia de la ciberseguridad como elemento fundamental en la escalabilidad y sostenibilidad de los sectores económicos más importantes del país. Además, en el curso de la recuperación económica de la industria hospitalaria y de viajes debido a la pandemia de COVID-19, se deben tener en cuenta consideraciones de inversión en ciberseguridad, con la finalidad de proteger ataques y vulnerabilidades del sector y aumentar la confianza internacional en el sector turístico de Costa Rica. Por ello, se recomienda que, durante la etapa de elaboración de la nueva estrategia, se consideren líneas estratégicas con base en los sectores económicos más importantes para brindar estabilidad y crecimiento de manera uniforme y no únicamente en el sector financiero.

Es evidente a partir de la publicación de la ENC 2017, Costa Rica ha progresado de manera exponencial en materia de ciberseguridad, tal y como lo muestran indicadores internacionales como el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones.

21 https://www.ict.go.cr/es/noticias-destacadas-2/1358-industria-tur%C3%ADstica-aporta-6,3-del-pib-a-la-econom%C3%ADa-de-costa-rica.html

ANEXO I
Resumen Ejecutivo del Estado de Madurez Cibernética de Costa Rica
(2016-2020)

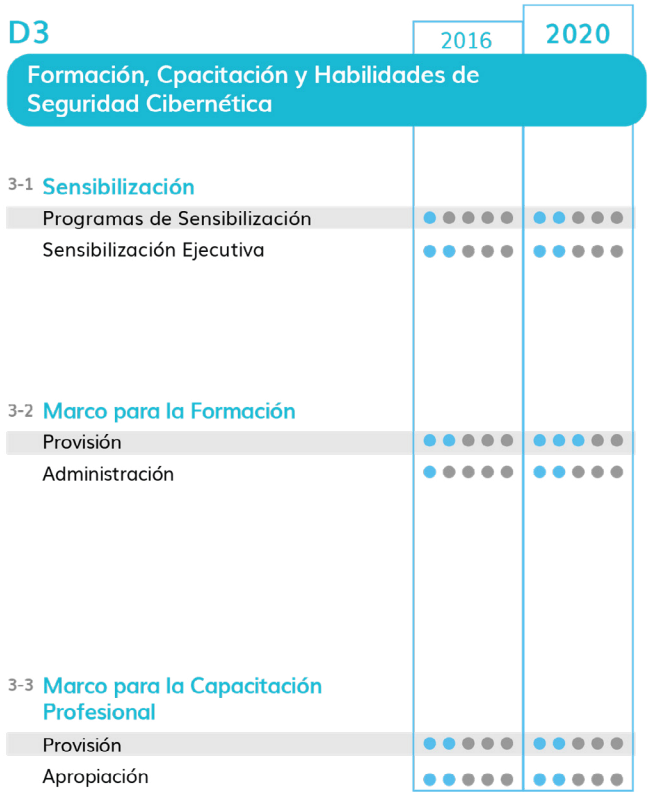
En 2017 el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica presentó la Estrategia Nacional de Ciberseguridad con el objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de las TIC, desarrollar la coordinación y cooperación entre las partes interesadas, y promover medidas de educación, prevención y mitigación del riesgo de utilizar las TIC. Sin embargo, si bien las normas de seguridad cibernética a nivel nacional se publicaron hace poco, Costa Rica ya había dado pasos significativos para asegurar su ciberespacio. En 2012 se creó un CSIRT nacional bajo el MICITT por medio del Decreto Nº 37.052 para coordinar entre los diferentes interesados todo lo relacionado con información y seguridad cibernética, y para formar un equipo de expertos en seguridad TIC destinado a prevenir y responder a los incidentes cibernéticos contra las instituciones gubernamentales. Además, CSIRT-CR es miembro de la red CSIRT Américas.

La Estrategia Nacional define la infraestructura crítica en términos de "sistemas de información y redes, que en caso de falla podrían tener un impacto serio en la salud, la seguridad física y operativa, la economía y el bienestar de los ciudadanos, o el funcionamiento efectivo del gobierno y economía del país". La Estrategia también describe la necesidad de determinar la infraestructura crítica del país y crear un comité para generar políticas conformadas por miembros de entidades públicas y privadas clasificadas como infraestructura crítica. El conocimiento sobre cuestiones de seguridad cibernética por parte del sector privado es limitado, pero desde 2017 proliferan las empresas enfocadas en brindar soluciones y servicios de ciberseguridad. Los costarricenses tienen muchas oportunidades de seguir estudiando sobre seguridad cibernética, y algunas universidades ofrecen programas más cortos de capacitación y diplomados.147 También se han realizado varios eventos de creación de capacidad en colaboración con instituciones internacionales, como la capacitación brindada por el Centro Criptológico Nacional de España para funcionarios públicos y la capacitación profesional en colaboración con la OEA y la Fundación Citi.

En 2012, Costa Rica aprobó el Decreto Legislativo Nº9.048, mediante el cual se reformó el Código Penal para introducir formalmente disposiciones para el delito cibernético. Algunos argumentan que esto no es suficiente, ya que hay problemas con la aplicación del marco y el decreto no es exhaustivo, lo que deja sin regulación los delitos como skimming (robo de información de la tarjeta de crédito), grooming (generar la confianza de alguien para aprovecharse de este), o el ciberacecho. Costa Rica ha adherido al Convenio de Budapest en 2017, así como también a otros convenios, y está desarrollando una estrategia nacional contra el ciberdelito. Para la privacidad y protección de datos, Costa Rica cuenta con la Ley Nº 8.968 de Protección de la Persona frente al tratamiento de sus datos personales. Esta ley se aplica a las bases de datos de los sectores público y privado. Desde 2010 Costa Rica tiene un borrador de estrategia para el gobierno electrónico con la visión de ser un país de referencia en América Latina en lo que concierne al gobierno digital mediante servicios centrados en el ciudadano, transparencia en los servicios e interconexión de instituciones gubernamentales basadas en un entorno favorable para las TIC y el establecimiento de una sociedad igualitaria y segura.


D1
2016
2020
Política y Estrategia de Seguridad Cibernética
1-1 Estrategia de Seguridad Cibernética
Desarrollo de la Estrategia
Organización
Contenido
1-2 Respuesta a Incidentes
Identificación de Incidentes
Organización
Coordinación
Modo de Operación
1-3 Protección de la Infraestructura Crítica (IC)
Identificación
Organización
Gestión de Riesgos y Respuesta
1-4 Manejo de Crisis
Manejo de Crisis
1-5 Defensa Cibernética
Estrategia
Organización
Coordinación
1-6 Redundancia de Comunicaciones
Redundancia de Comunicaciones


D2
2016
2020
Cultura Cibernética y Sociedad
2-1 Mentalidad de Seguridad Cibernética
Gobierno
Sector Privado
Usuarios
2-2 Confianza y Seguridad en Internet
Confianza y Seguridad en el Internet del usuario
Confianza del Usuario en los Servicios de Gobierno Electrónico
Confianza del Usuario en los Servicios de Comercio Electrónico
2-3 Comprensión del Usuario de la Protección de la Información en Línea
Comprensión del Usuario de la Protección de Información Personal en Línea
2-4 Mecanismos de Denuncia
Mecanismos de Denuncia
2-5 Medios y Redes Sociales
Medios y Redes Sociales


D3
2016
2020
Formación, Cpacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación


D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Lesgislación sobre Protección de Datos
Protección Infantil en Línea
Lesgislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva contra el Delito Cibernético
Legislación Procesal contra el Delito Cibernético
4-1 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal


D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares de Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la Infraestructura del Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

ANEXO II
Lista de los Actores Principales

- Abriendo Datos Costa Rica
- Agencia de Protección de datos de los Habitantes
- Banco Promerica de Costa Rica S.A.
- Cámara de Bancos e Instituciones Financieras de Costa Rica
- CINDE
- Contraloría General de la República
- Cooperativa Sulá Batsú
- Defensoría de los Habitantes
- Instituto Nacional de Aprendizaje
- Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
- Ministerio de Educación Pública – Direccion de Educación Técnica y Capacidades Emprendedoras
- Ministerio de Hacienda
- Ministerio de la Presidencia
- Ministerio de Relaciones Exteriores y Culto de Costa Rica
- Ministerio Público
- Organismo de investigación Judicial
- Promotora del Comercio Exterior de Costa Rica
- Sistemas de Emergencia 9-1-1
- Superintendencia de Telecomunicaciones
- Universidad Escuela Libre de Derecho
- Universidad Latina de Costa Rica

Informe 2021

REVISIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE COSTA RICA (2017)

Con el apoyo técnico de:

OEA Más derechos para más gente