Costa Rica
Estrategia Nacional de Ciberseguridad

2022

Gobierno de Costa Rica
OEA / CICTE | PROGRAMA DE CIBERSEGURIDAD

Índice

1. Propósito

El objetivo de esta actualización estrategia nacional de ciberseguridad de Costa Rica, es crear una visión de un ciberespacio abierto, libre y seguro que responda a las ciberamenazas potenciales a las que se enfrenta o puede enfrentar Costa Rica generando un pensamiento estratégico que permite continuar apoyando a las autoridades del país y formuladores de políticas en el desarrollo, establecimiento e implementación de un marco holístico e integral que englobe todas las iniciativas que tienen que ver con la ciberseguridad en el país para evitar la duplicidad de esfuerzos que puede derivarse de intervenciones aisladas y no coordinadas, partiendo de la base que la ciberseguridad es una responsabilidad de todos. El gobierno de Costa Rica ha contado con los líderes de los diferentes sectores críticos desde el punto de vista de la ciberseguridad, academia, sociedad civil, sector público, sector privado, instituciones y empresas de infraestructuras críticas para dar un enfoque multipartes que englobe todos los puntos de vista necesarios para generar un documento lo más completo posible y con una visión común

2. Antecedentes

En las últimas décadas, hemos sido testigos del crecimiento exponencial en el uso de las tecnologías de la información y la comunicación (TIC) y aprovechado las oportunidades socioeconómicas y políticas que se han derivado de ello. La transformación digital que se está viviendo a nivel global es un poderoso facilitador de un desarrollo inclusivo y sostenible, pero también puede presentar una nueva fuente de problemas si la infraestructura subyacente y los servicios que dependen de ella no son seguros ni están protegidos frente a las amenazas cibernéticas.

La naturaleza cambiante del ciberespacio, la mayor dependencia sobre las TIC y la proliferación de riesgos digitales exigen mejoras continuas a las estrategias nacionales de ciberseguridad. La mayoría de los países han acelerado su transformación digital y se preocupan cada vez más por la amenazas inmediatas y futuras a sus servicios críticos, infraestructuras, sectores, instituciones y empresas, así como a la paz y la seguridad internacionales, que podría resultar del mal uso de las tecnologías digitales y la resiliencia inadecuada.

Para aprovechar los beneficios y gestionar los desafíos de la digitalización, el gobierno de Costa Rica confirma su compromiso para mantener un ciberespacio seguro a partir de la puesta al día de su estrategia nacional de ciberseguridad.

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

Políticas y Normas Nacionales

En 2012, Costa Rica aprobó la Ley N° 9048 del 10 de julio de 2012 y la Ley N° 9135 del 24 de abril de 2013 y, mediante el cual se reformó el Código Penal para actualizar las disposiciones para el delito cibernético en Costa Rica. En el año 2012 se promulgaba el Decreto 37.052 que creó el CSIRT Nacional bajo el

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Todo ello antes de desarrollar su primera Estrategia Nacional de Ciberseguridad en 2017.

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

- Ley N°7169 de Promoción del Desarrollo Científico y Tecnológico: El artículo 4º, inciso e), contempla como deber del Estado: "establecer políticas de desarrollo científico y tecnológico, supervisar su ejecución, además de evaluar su impacto y resultados, en el marco de la estrategia de desarrollo nacional" Subsecuentemente, el inciso k) postula como responsabilidad del Estado: "impulsar la incorporación selectiva de la tecnología moderna en la Administración Pública a fin de agilizar y actualizar, permanentemente, los servicios públicos, en el marco de una reforma administrativa, para lograr la modernización del aparato estatal costarricense, en procura de mejores niveles de eficiencia"
- Decreto Ejecutivo N°31659. Establece la creación de existe un Consejo Interinstitucional sobre Terrorismo (CICTE) que: "desarrolle proyectos de seguridad informática e integre el Centro de Respuesta de Incidentes Informáticos (CSIRT por sus siglas en inglés), en apego a la normativa vigente de la Organización de Estados Americanos (OEA)"
- Norma N°37052 para la creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR). Decreta que el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), regido por el Ministerio de Ciencia y Tecnología (MICITT), *con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales*. Ley N°4573 Código Penal: El Código Penal que Costa Rica tipificó varios delitos informáticos entre ellos podemos mencionar el artículo 196 BIS tipificando la violación de comunicaciones electrónicas para descubrir los secretos o vulnerar la intimidad de otros cuando: "sin consentimiento, se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos".

  Por su parte, también el artículo 217 BIS aborda las penas derivadas de la estafa informática cuando: "manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro."

  Además, el artículo 229 BIS y 229 ter considera las penas por daño informático y sabotaje informático cuando: "suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. (…); destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático"

- Ley N°8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales. El artículo 10 relativo a la seguridad de los datos establece que: "El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado". Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada"
- Normas técnicas para la gestión y el control de las Tecnologías de Información: establecen los principios de cumplimiento de las instancias institucionales en materia de Tecnologías de Información y Comunicaciones para asegurar: "el uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo"
  En el apartado décimo primero (11), por su parte, se aborda lo relativo a la ciberseguridad, postulando que: "las instituciones deben tener y aplicar en forma consistente una estructura formal a nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad, debidamente respaldada con la política nacional; (…) haciendo énfasis en la preservación de la confidencialidad, integridad y disponibilidad de la información".
  Además, en el ámbito de los recursos humanos, se postula que: "las prácticas deben apoyar el reclutamiento, selección, contratación, inducción y capacitación continua"
- Norma Nº36274 para crear la Comisión Nacional de Seguridad en Línea. En el artículo 1 se postula como labor de la Comisión: "diseñar las políticas sobre el buen uso de Internet y las Tecnologías Digitales contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que permita beneficiarse de las ventajas de su utilización, y tener una actitud consciente y proactiva frente a los riesgos inherentes a su uso"
- Estrategia para la prevención y respuesta de la explotación y el abuso de niños en línea. Plantea como objetivos específicos en el marco estratégico de ejecución:
  i. construir entornos digitales seguros, en coordinación con la institucionalidad pública, la empresa privada y la sociedad civil.
  ii. implementar medidas integrales para la prevención y respuesta a delitos asociados a EASNNAL, siguiendo el Modelo "WePROTECT"
  iii. reducir los riesgos que puedan derivarse del desconocimiento, incomprensión o uso inadecuado de las tecnologías digitales, por parte de las poblaciones meta.

  El desarrollo de este marco estratégico se realiza, a su vez, por medio de los siguientes ejes: políticas públicas y gobernanza; justicia penal; víctimas; sociedad civil; industria; comunicación y medios.
- Norma N°8934 relativa a la protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. El artículo 2 estipula la obligación de la instalación de filtros en las computadoras de espacios públicos destinadas a personas menores de edad, para bloquear el acceso a sitios y comunicaciones cuyo contenido promueva:
  a) pornografía en general, e infantil en particular.
  b) lenguaje obsceno.
  c) agresión y violencia física, sexual y emocional.
  d) construcción de armas, explosivos
  e) uso de drogas no autorizadas.

f) actividades bélicas.
g) racismo, xenofobia o cualquier forma de discriminación

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

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

Visión general internacional

Las cifras del cibercrimen

El delito cibernético está progresando a un ritmo vertiginoso gracias a la dependencia, cada vez más acentuada, que la sociedad tiene de las tecnologías de la información y la comunicación. La pandemia COVID-19 no ha hecho sino acrecentar esta tendencia ofreciendo nuevos objetivos para estos ataques (agencias de salud pública, instituciones sanitarias, hospitales, entre otros) así como nuevas formas de engaño (compromiso de correos electrónicos corporativos, o BEC por sus siglas en inglés, por parte de entidades involucradas en programas de vacunación).

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

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

El *Ransomware*, los ataques dirigidos y las estafas continúan proliferando y evolucionando, involucrando herramientas cada vez más sofisticadas y dirigiéndose hacia blancos más grandes. Tan solo el primer semestre de 2021 se detectó más de 7,3 millones de ataques de *ransomware*, siendo una de las tendencias más notables el incremento de detecciones de *ransomware* moderno que utiliza herramientas y técnicas similares a aquellas utilizadas por amenazas avanzadas persistentes (APTs por sus siglas en inglés).

[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[2] https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/trend-micro-specialized-cybersecurity-report-for-latin-america-and-the-caribbean

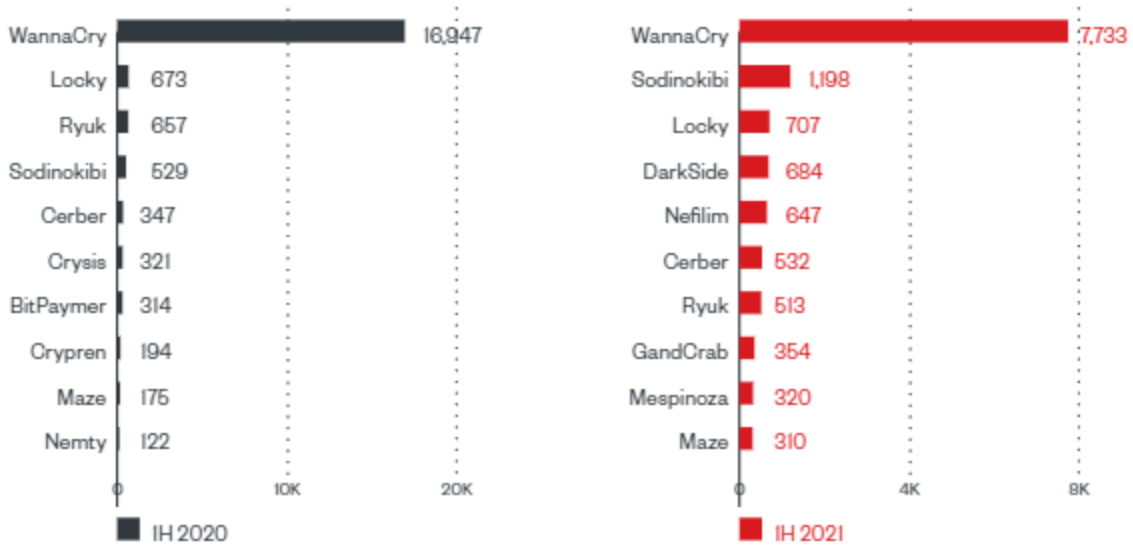


Figura 2. El top 10 de familias de ransomware a lo largo de los estados miembros de la OEA en términos de detecciones de archivos de familias de ransomware en la primera mitad del 2020 y la primera mitad del 2021

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

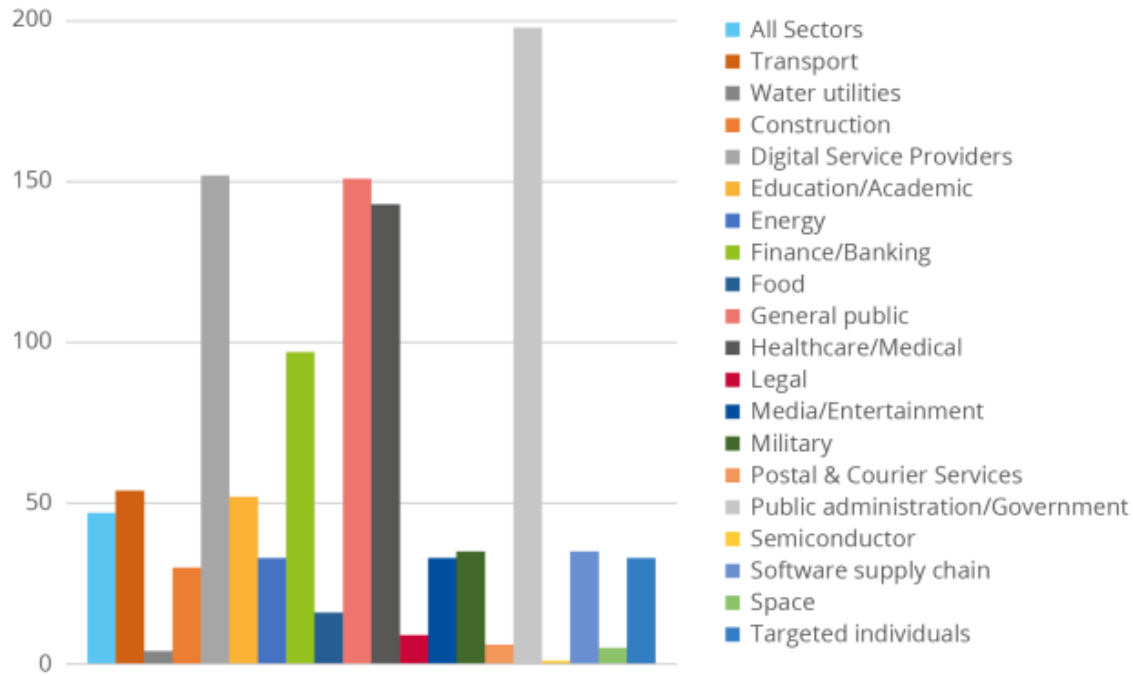
Incluso antes de la pandemia, muchas organizaciones ya estaban adoptando nuevas tecnologías como plataformas en la nube o internet dando por sentado la seguridad de estas herramientas. Las fallas de configuración y la falta de actualizaciones, sin embargo, han estado entre las causas más comunes de infiltraciones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

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

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

estudiados se atribuyeron a grupos APT conocidos. El estudio también determinó que las principales motivaciones de los atacantes eran acceder al código fuente y a los datos de los clientes.

Figure 4: Targeted sectors per number of incidents (April 2020-July 2021)



Costa Rica en el ámbito internacional

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

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

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

Se han establecido alianzas estratégicas de larga duración con organismos multilaterales como el Organismo de Estados Americanos (OEA). Organismo que contribuyó desde 2016 en el proceso de construcción de la Estrategia Nacional de Ciberseguridad y a través del acercamiento con el Comité

Interamericano contra el terrorismo (CICTE) de la OEA hemos generado procesos de formación y capacitación a jóvenes en ciberseguridad y además de formación específica para mujeres en ciberseguridad.

De igual manera a través de esta alianza, se han podido conocer de cerca las experiencias de países exitosos en el tema de ciberseguridad como España y Estonia, y se han logrado hacer los contactos necesarios para intercambio de buenas prácticas y participación en redes de apoyo en ciberseguridad.

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

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

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

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

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

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

A la espera del resultado de las negociaciones sobre Cibercrimen que se mantienen en el seno de la Organización de Naciones Unidas (ONU) mientras esta estrategia está siendo redactada, el Convenio de Budapest sigue siendo el tratado internacional vinculante más relevante sobre delitos cibernéticos y pruebas electrónicas. Con su lenguaje tecnológicamente neutral, la Convención posibilita además el

ejercicio de facultades procesales y herramientas de cooperación internacional en relación con cualquier delito que implique prueba electrónica.

3. Principios generales

Esta estrategia está motivada en los siguientes principios rectores:

1. Las personas son la prioridad
   Las personas son el eje central en la estrategia. El uso de las TIC en los diferentes ámbitos de la vida cotidiana nos obliga a hacer partícipes de esta estrategia a todos los habitantes del país, por lo que la corresponsabilidad en el uso individual de dispositivos y redes será fundamental.
   Por lo anterior, se promoverá el uso de las TIC como un instrumento para el mejoramiento de la calidad de vida de manera segura, procurando generar conciencia por medio de la educación desde edades tempranas sobre los efectos del uso responsable. Se procurará que cualquier acción tenga como prioridad considerar la atención y mitigación de los riesgos que impacten prioritariamente a las poblaciones vulnerables como la niñez, la adolescencia, los adultos mayores, la población indígena y las personas con algún tipo de discapacidad.
2. Respeto a los Derechos Humanos y la Privacidad.
   Garantizar el respeto a los derechos humanos, especialmente los relacionados con el acceso a las TIC, el acceso a la información y el respeto a la privacidad es fundamental. Las medidas y acciones que resulten de esta estrategia deberán en todo momento salvaguardar los derechos humanos y la privacidad de la información de los habitantes del país. Por lo tanto, esta estrategia se ha desarrollado teniendo en cuenta la necesidad de equilibrar la protección de todos los habitantes y el respeto de los derechos humanos básicos y fundamentales, con la necesidad de implementar medidas para mantenerlos seguros en línea. Esto incluye el respeto a la libertad de expresión, la libertad de palabra, el derecho a la privacidad, la libertad de opinión y la libertad de asociación
3. Coordinación y corresponsabilidad de múltiples partes interesadas.
   La ciberseguridad es una responsabilidad compartida de todos los actores que participan en el ecosistema digital, lo cual incluye a los usuarios. Es imperativo que todas las acciones que se deriven de esta estrategia consideren, siempre que sea pertinente, la participación y aporte de todas las partes interesadas, la corresponsabilidad de estos y la necesidad de coordinación entre los distintos actores. Para el proceso de implementación, el apoyo de todos los sectores es fundamental, por esto, se deben considerar y promover los modelos público-público, público-privado y público-sociedad civil; según la idoneidad, requerimientos y alcances de los objetivos a implementar.
4. Cooperación Internacional
   La naturaleza transfronteriza de las tecnologías digitales hace que la temática de la ciberseguridad deba ser atendida desde una perspectiva global. Las amenazas cibernéticas no tienen fronteras, por ello la cooperación internacional se convierte en un eslabón primordial tanto, para la atención de las amenazas como para la transferencia de conocimiento y el desarrollo de acciones locales y globales que ayuden a incrementar la confianza y la seguridad global. Por tanto, la construcción de alianzas, acuerdos y estrechamiento de lazos con otras entidades públicas y privadas que atienden las temáticas relacionadas a la Ciberseguridad tanto a nivel regional e internacional deben ser elementos clave dentro de esta estrategia.

4. Análisis situacional

Costa Rica ha llevado un proceso de acciones para mejorar la ciberseguridad nacional, lo cual llevo al país en el año2017 a generar un norte común desarrollando su primera Estrategia Nacional de Ciberseguridad, que articuló una visión nacional para la coordinación en respuesta a las amenazas cibernéticas. Un documento que se estructuraba a partir de una serie de principios rectores, un marco con un objetivo general y ocho objetivos específicos.

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

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

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

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

Este trabajo, impulsado desde MICITT, también ha contado con socios internacionales como la propia OEA, el Banco Interamericano de Desarrollo y los gobiernos de Israel y Corea del Sur.

Revisión de la Estrategia Nacional de Ciberseguridad de 2017

El Objetivo Específico 8 de la Estrategia Nacional de 2017 (ENC 2017) confirma el propósito de seguir mejorando las capacidades en ciberseguridad del país a partir de la implementación, seguimiento y evaluación de esta que permita evaluar el cumplimiento de las líneas de acción y proponer los ajustes

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

según se requiera. En concreto, la línea estratégica 8.2 establece que se realice una revisión y actualización de la Estrategia Nacional de Ciberseguridad.

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

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

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

i. Consolidación del CSIRT-CR y MITTIC. El análisis de respuestas recopiladas por parte de las partes interesadas sugiere que uno de los elementos más exitosos de la ENC 2017 fue la consolidación del CSIRT-CR como una entidad clave en la coordinación nacional en seguridad cibernética.
ii. Adquisición de una cultura nacional en ciberseguridad. Debido al aumento de iniciativas de concienciación que se están implementando.
iii. Costa Rica país líder regional en materia de ciberseguridad refrendado por el número de iniciativas que se están llevando a cabo en colaboración con socios internacionales en distintas áreas distintivas de seguridad cibernética, demostrando el compromiso de cooperación internacional del país.

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

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

¿Por qué se necesita una estrategia?

El propósito de una estrategia nacional de ciberseguridad es proveer al país de un documento integral que articule y priorice objetivos, señale políticas de apoyo y mecanismos estructurales, establezca roles y responsabilidades, asignación de recursos y rendición de cuentas. Publicar una estrategia siempre es un ejercicio inspirador que educa a las partes interesadas y les explica de qué manera se pueden apalancar los avances tecnológicos para mejorar el bienestar económico, político social y de seguridad del país. A partir de la comunicación de los objetivos y las prioridades, la ENC también ayuda a informar a socios estratégicos y a desalentar potenciales adversarios o criminales.

Las estrategias forman parte de un proceso continuo de evaluación, desarrollo e implementación. Son herramientas vivas que se han de ajustar a las necesidades del país y reajustarse periódicamente para responder a las necesidades políticas, económicas, financieras y tecnológicas del momento. En esta línea, el Modelo de Madurez en Ciber Capacidades de la Universidad de Oxford (CMM por sus siglas en inglés) define al estadio más avanzado de un país en términos de ciberseguridad como Dinámico. Aquí, el país disponible de una estrategia de ciberseguridad flexible que regula, de manera global, los temas de seguridad cibernética con agilidad en la toma de decisiones y la asignación de recursos.

Considerando los avances a nivel nacional de Costa Rica en la madurez cibernética, resultaba necesario revisar y actualizar el marco político, a fin de que refleje las oportunidades y desafíos actuales que permitan una mejora en el ámbito de la ciberseguridad en el futuro. Hacia ese propósito se encamina esta puesta al día de la Estrategia Nacional de Costa Rica, que tiene como objetivo el de reforzar la formulación y continuidad de políticas públicas en materia de ciberseguridad.

Políticas e iniciativas en materia de TIC

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

Actualmente el país cuenta con las siguientes políticas públicas en materia TIC:

A desarrollar por el gobierno de Costa Rica con las iniciativas más recientes en materia de TIC.

1. **Estrategia De Transformación Digital**

La Estrategia de Transformación Digital busca llevar adelante importantes transformaciones digitales en las instituciones del sector público y en la sociedad a fin de potenciar el desarrollo socioeconómico del país y asegurar una mejor calidad de vida para todos los habitantes de manera inclusiva que permita asegurar el desarrollo y el bienestar de los habitantes, a través de las oportunidades brindadas por la cuarta revolución industrial y las sociedades del conocimiento,

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

En el 2020 el país adoptara la Estrategia Nacional de Bioeconomía Costa Rica 2020-2030, como una herramienta alineada a las recomendaciones de acceso de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y las metas plasmadas en el Plan Nacional de Descarbonización. Esta política pretende establecer una economía ecológica, resistente, descarbonizada, competitiva y sustentada en el conocimiento, a través de la incorporación de la bioeconomía circular y la descarbonización de los procesos de producción y consumo. Con ello, se tiene la aspiración de crear un entorno en el que la producción sea sostenible, genere un alto valor agregado en todas las regiones de país, que se base en el aprovechamiento de la biodiversidad, la circularidad en el uso de la biomasa y el progreso tecnológico

3. **Plan Nacional de Desarrollo de Telecomunicaciones (PNDT)**

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

4. **Política Nacional de Sociedad y Economía basada en el Conocimiento (PNSyEC)**

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

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

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

Incidentes cibernéticos

El CSIRT Nacional en su labor de monitoreo de los sitios web públicos del sector público, atención de tiquetes relacionados con incidentes de ciberseguridad, además de los reportes de sitios de phishing y

alertas técnicas, ha visto el crecimiento de los incidentes a nivel nacional presentando los siguientes datos:

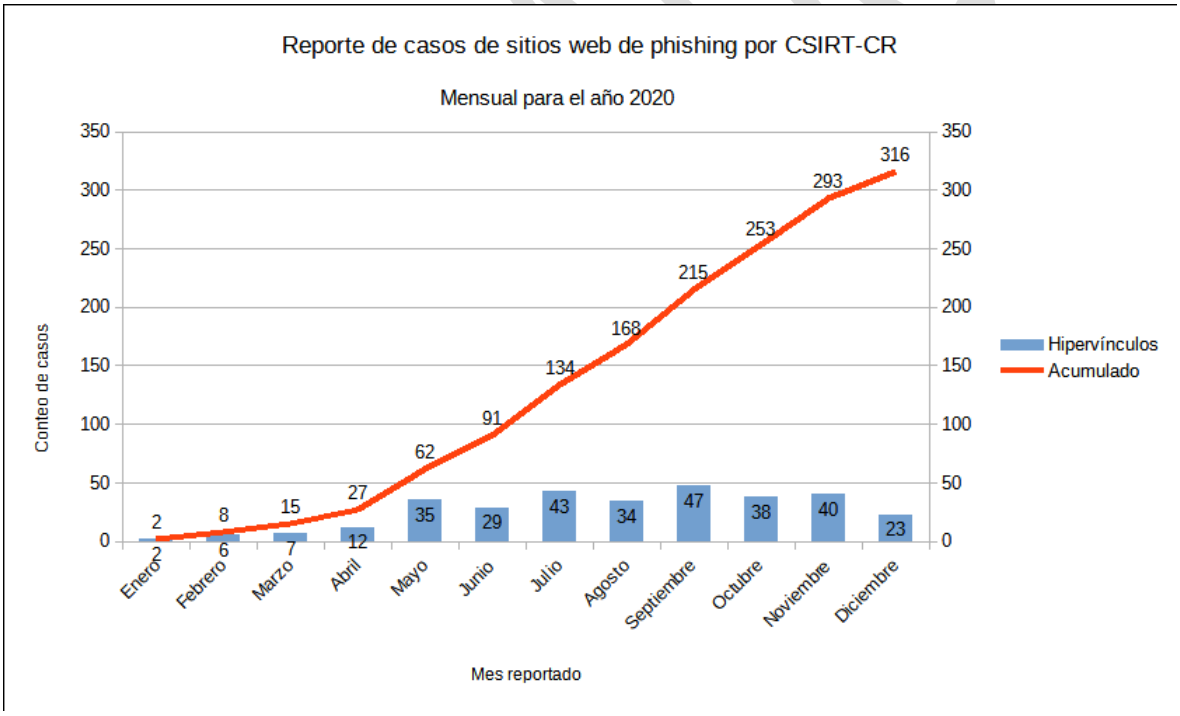
Phishing

2019

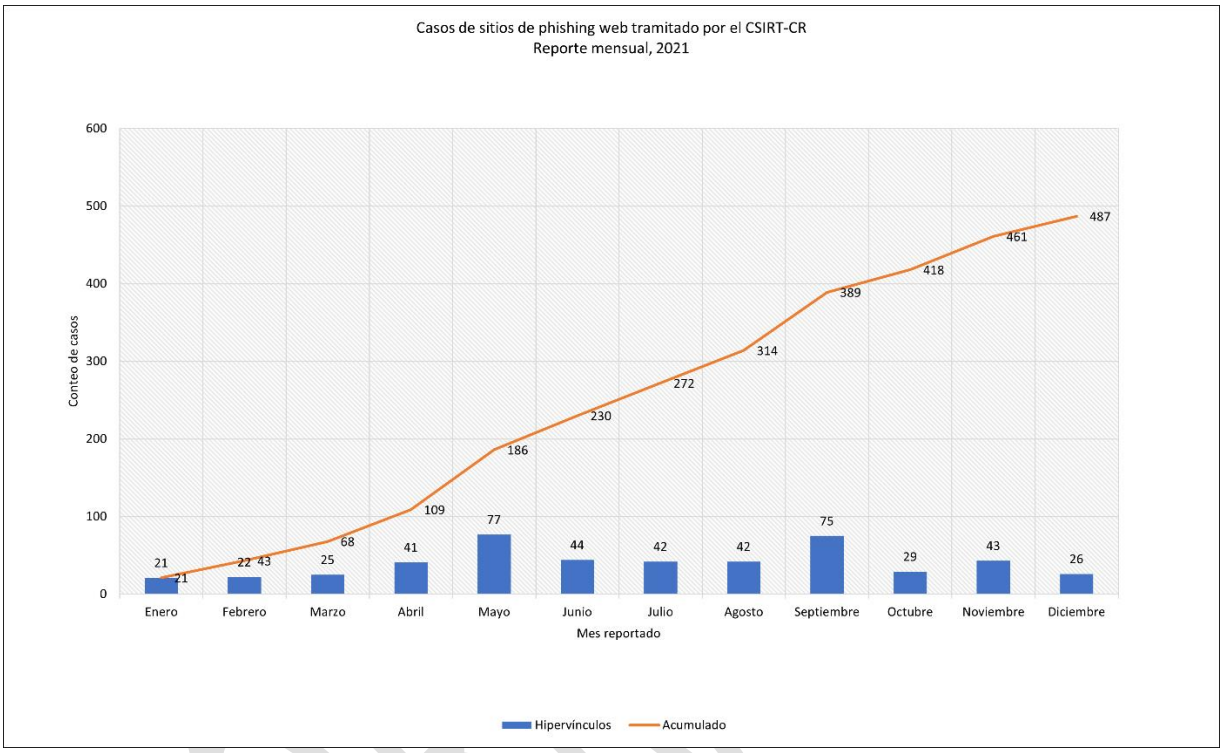
Se reportaron 11 sitios de phishing

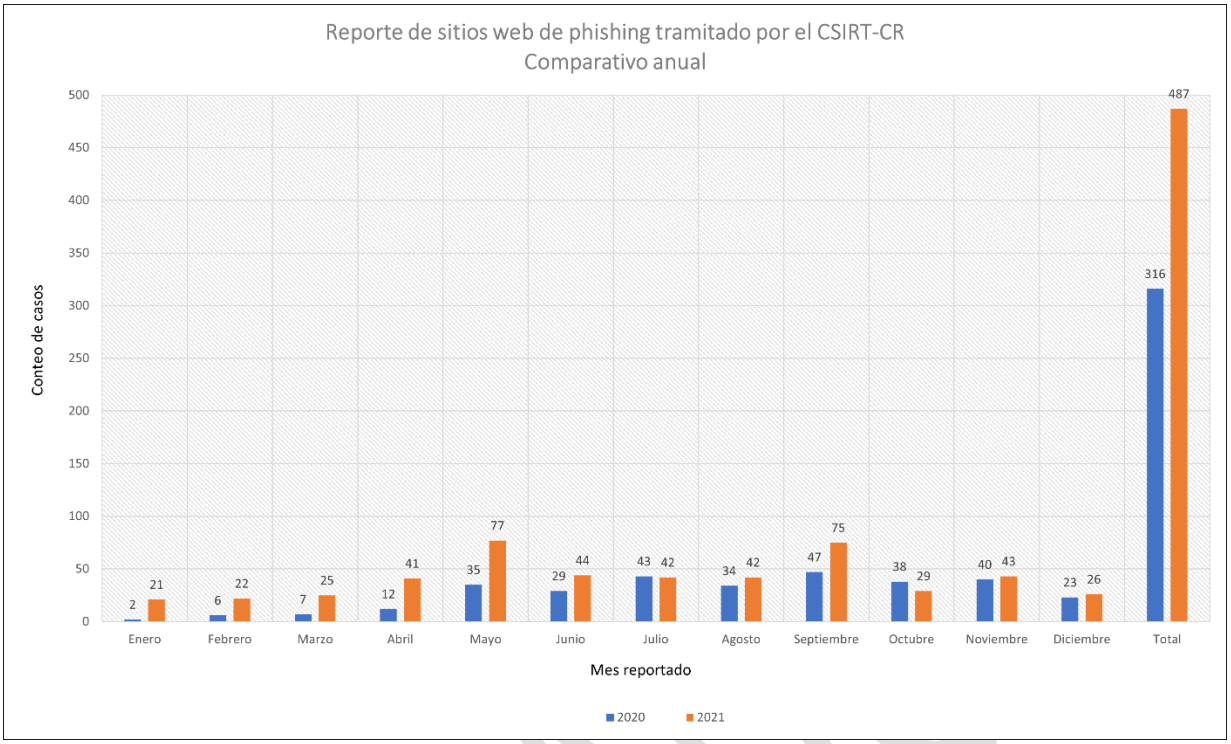
2020

Se reportaron 316 sitios de phishing y se comenzó a llevar un registro detallado de reportes y gráficos



2021


Casos de sitios de phishing web tramitado por el CSIRT-CR
Reporte mensual, 2021
Conteo de casos
600
500
400
300
200
100
0
21
22
25
41
77
44
42
42
75
29
43
26
21
43
68
109
186
230
272
314
389
418
461
487
Enero
Febrero
Marzo
Abril
Mayo
Junio
Julio
Agosto
Septiembre
Octubre
Noviembre
Diciembre
Mes reportado
Hipervínculos
Acumulado



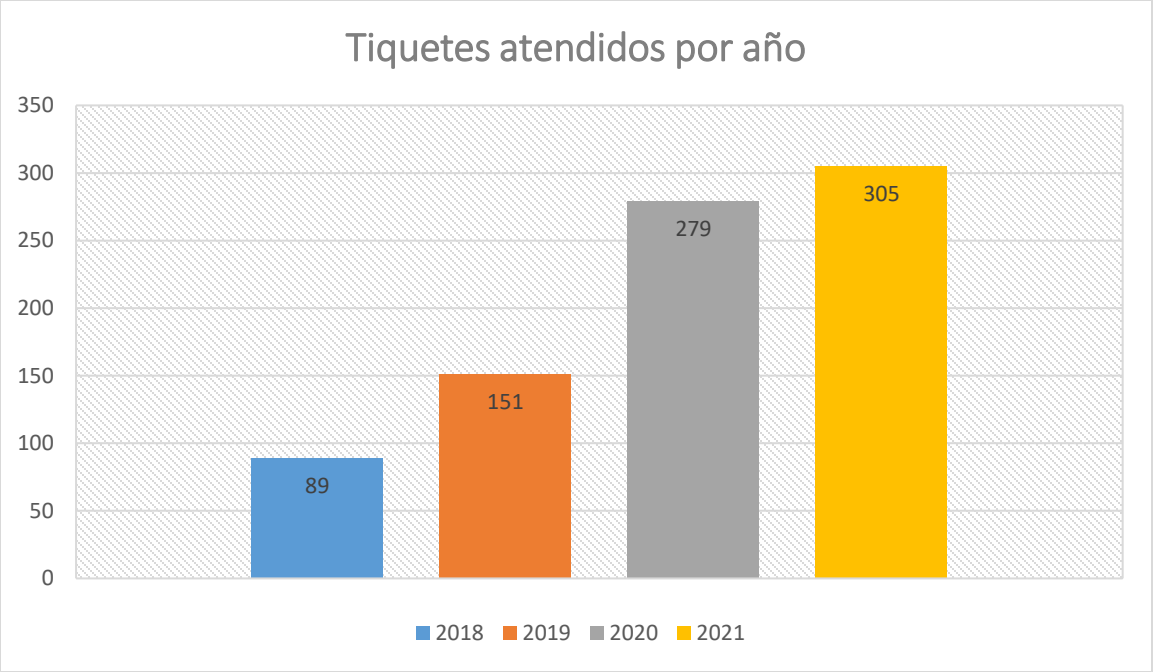
En atención de incidentes por tiquetes se cuentan con los siguientes datos:

2018: 89

2019: 151

2020: 279

2021: 305



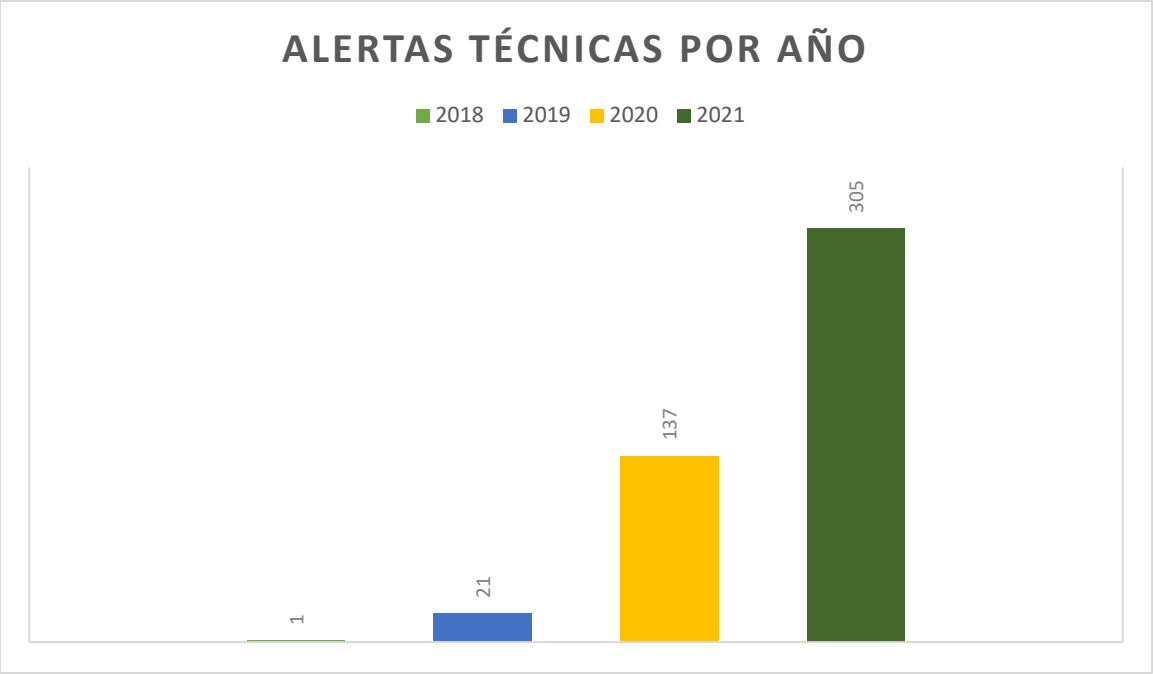
En la generación de alertas técnicas generadas por el CSIRT Nacional se han realizado los siguientes:

2018: 1

2019: 21

2020: 137

2021: 424



5. Enfoque estratégico

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

Ejes transversales

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

1. Coordinación Nacional

Con el propósito de garantizar la coordinación política y técnica que permitan implementar las líneas de acción de este plan es necesaria una estructura que posibilite la acción conjunta entre los distintos

actores. MICITT, será el punto focal a nivel nacional e internacional para cualquier tema relacionado con la seguridad cibernética del país.
Se renovará la composición del Comité Consultivo encargado de velar junto con MICITT por el cumplimiento de la estrategia. Este Comité Consultivo estará formado por:

- Dos representantes del MICITT
- Un representante del Poder Judicial
- Un representante de la SUTEL
- Dos representantes de la sociedad civil
- Dos representantes de la academia
- Dos representantes del Sector Privado
- Un representante de la PRODHAB
- Dos representantes del Sector Financiero

El Comité Consultivo, presidido por el MICITT, reforzará relaciones de coordinación, colaboración y cooperación entre los distintos sectores y partes interesadas en la ciberseguridad, incluyendo al Estado, el sector privado, la academia y la sociedad civil.
Además, tendrá la autoridad para monitorear y evaluar la implementación de los objetivos y de las líneas de acción de este Plan Nacional por parte de los distintos actores gubernamentales.

AGREGAR TEMA CSIRT NACIONAL

- Líneas de acción

1. Coordinación y colaboración:
   i. Diseñar e implementar mecanismos dinámicos de coordinación, articulación y colaboración entre las diferentes agencias de gobierno encargadas de la seguridad digital a nivel nacional.
   ii. Desarrollar planes de acción para garantizar la supervivencia política de la estrategia ante un potencial cambio de gobierno.
2. Búsqueda de recursos:
   i. Creación de comisiones, comités y grupos consultivos para la obtención de recursos que permitan alcanzar los objetivos de esta estrategia.
3. Rendición de cuentas:
   i. Diseñar actividades apropiadas para lograr los objetivos y la operabilidad; además, realizar evaluaciones continuas para conocer si estas actividades están ayudando a obtener los objetivos previstos.
   ii. Adoptar enfoques de trabajo específicos para cada sector, con la finalidad de medir claramente el cumplimiento de los objetivos de la estrategia.

2. Fortalecimiento del Ecosistema de Ciberseguridad

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

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

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

- Líneas de acción

1. Educación académica:
    i. Realizar una Encuesta nacional en de destrezas y brechas de profesionales para medir las necesidades del país en ciberseguridad.
    ii. Incluir los contenidos de ciberseguridad de manera formal y escalonada, iniciando con la inclusión de algunas materias optativas en los cursos de computación, tentativamente sobre los riesgos en el ciber espacio y su ámbito legal.
    iii. Desarrollar junto con la academia mallas curriculares en ciberseguridad.
2. Capacitación de profesionales:
    i. Desarrollar cursos para directores de departamentos tecnológicos en organizaciones y operadores de infraestructura crítica.
    ii. Desarrollar entrenamientos en colaboración con el sector privado para capacitaciones genéricas en ciberseguridad independientemente del puesto de trabajo.
3. Innovación y desarrollo:
    i. Fomentar la innovación en la industria de la ciberseguridad mediante un plan que apoye a la industria en la investigación de productos innovadores.
    ii. Fomentar la creación de nuevas empresas a partir de la creación de incubadoras y desarrollar las existentes a través aceleradoras de emprendimiento para promocionar la colaboración entre la comunidad de expertos en ciberseguridad.
    iii. Desarrollar Sistemas Nacionales de Innovación replicando el modelo de otras naciones para articular la labor entre todos los sectores de la industria y facilitar la exportación de los productos nacionales a otras naciones.

3. Habilitar un ciberespacio más seguro.

Para asegurar el bienestar socio económico y sostenible del país es necesario sensibilizar a los ciudadanos sobre la importancia del uso seguro y responsable de Internet. Para ello es necesario incorporar de manera progresiva buenas prácticas de ciberseguridad hasta que se interiorice en la ciudadanía, el gobierno y las empresas del país.
Tener una cultura en ciberseguridad significa que el conocimiento de técnicas y de conceptos de ciberseguridad sirve de orientación para las prácticas de los usuarios finales de la red.

- Líneas de acción:

1. Concientización de usuarios finales para que todos conozcan los riesgos y tengan el acceso a las herramientas de protección.:
    i. Elaboración de campañas de publicidad que den a conocer mejores prácticas en el uso de nuevas tecnologías.

ii. Desarrollo de campañas para promover entre los usuarios el uso de internet seguro.
iii. Planeación de cursos de alfabetización en ciberseguridad para particulares, en especial en torno a la ingeniería social.
iv. Desarrollar programas conjuntos entre el Ministerio de Educación y las entidades bancarias para realizar un programa interinstitucional del cliente financiero.

2. Concientización de empresas para trabajadores independientemente de su puesto de trabajo:
   i. Desarrollo de campañas para mejorar la cultura empresarial en ciberseguridad.
   ii. Promover reconocimientos nacionales para aquellas empresas e instituciones que incluyan labores de sensibilización en ciberseguridad entre sus empleados.
   iii. Crear campañas de concientización para cambiar la percepción de los costos en las mejoras de ciberseguridad como una inversión y no como un gasto.
3. Concientización de empleados del Sector público:
   i. Elaboración de campañas para concientizar a los funcionarios públicos de la importancia de la ciberseguridad en el ámbito de su trabajo.
   ii. Concientización a los altos jerarcas de los Poderes de la República sobre ciberseguridad
   iii. Fomentar la colaboración horizontal de instituciones expertas con aquellas menos avanzadas para crear espacios donde se compartan buenas prácticas.

4. Fortalecimiento de la cooperación cibernética internacional

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

- Líneas de acción:

1. Estrechar lazos de con países prioritarios con el objetivo de compartir información técnica y operativa sobre amenazas y riesgos cibernéticos, intercambio de buenas prácticas y coordinación del desarrollo de fuerza laboral.
   i. Identificar países prioritarios con los que establecer o mantener una línea de colaboración activa en materia de ciberseguridad.
   ii. Desarrollar programas de cooperación e intercambio de experiencias.
2. Fortalecer la cooperación multilateral para hacer frente a los desafíos transfronterizos y participar en las iniciativas regionales y los foros de discusión internacionales.
   i. Fortalecer la participación del CSIRT-CR en la red de centro de respuestas a incidentes cibernéticos CSIRT Américas.
   ii. Fortalecer la cooperación horizontal a través de la participación en la red hemisférica de gobierno electrónico (Red Gealc)
   iii. Fomentar la participación de funcionarios del país en los procesos de desarrollo de normativa internacional como Naciones Unidas.

5. Gestión del riesgo.

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

- Líneas de acción:

1. Desarrollar un registro nacional de riesgos:
    i. Realizar un estudio de evaluación de riesgos que permita al gobierno supervisar los riesgos y las soluciones adoptadas con el fin de gestionarlos, con énfasis a infraestructuras de servicios esenciales
    ii. Desarrollar un mecanismo para establecer prioridades basado en el cálculo de la probabilidad de que se materialicen los riesgos y sus repercusiones.
    iii. Especificar las responsabilidades de las infraestructuras críticas de cada sector en lo que respecta a la evaluación, aceptación y tratamiento de los riesgos para la ciberseguridad a escala nacional.
    iv. Desarrollar un guía nacional de clasificación de incidentes
2. Identificar una metodología común para gestionar los riesgos para la ciberseguridad que garantice la eficiencia y la coherencia en todas las organizaciones y facilite el intercambio de información sobre riesgos entre sistemas interdependientes.
    i. Desarrollar una metodología que informe sobre la asignación de funciones y responsabilidades para diversos aspectos de la gestión de riesgos, como la evaluación de las amenazas, la valoración de los activos, la ejecución y el mantenimiento de medidas de mitigación y la aceptación de riesgos residuales.
    ii. Desarrollar un programa de certificación para ayudar a evaluar y luego mejorar el cumplimiento.
    iii. Desarrollar recomendaciones sobre cómo minimizar el riesgo mediante una arquitectura y un diseño seguros.
3. Elaborar perfiles de riesgos sectoriales en materia de ciberseguridad para comprender los riesgos de una manera menos subjetiva mediante la asignación de valores numéricos a variables relacionadas con diferentes tipos de amenazas y el peligro que representan.
    i. Elaborar de perfiles de riesgos para los sectores que el país considera fundamentales para su sociedad y su economía.
    ii. Actualizar periódicamente estos perfiles para garantizar que se mantengan al día y contengan datos veraces.

6. Protección de Servicios Esenciales.

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

- Líneas de acción.

1. Establecer una definición e inventario de las infraestructuras críticas del país.

i. Identificar las infraestructuras críticas del país de acuerdo con los criterios de esencialidad internacionalmente aceptados.
ii. Definir los niveles de incidentes que pueden presentarse en las infraestructuras críticas para determinar si se catalogan como amenaza nacional o institucional

2. Establecer protocolos y marcos regulatorios para la implementación de buenas prácticas y estándares internacionales de protección de infraestructura crítica.
   i. Crear un mecanismo de supervisión para la implementación de buenas prácticas y estándares internacionales.
   ii. Evaluar la gestión de riesgos de cada institución para detectar similitudes que puedan ser consideras en la propuesta del protocolo.
   iii. Establecer protocolos de comunicación de incidentes en infraestructuras críticas.
   iv. Definir claramente entre las labores de comunicación de incidentes y las propias de gestión técnica para y establecer grupos de trabajo para cada una de ellas.
   v. Homogeneizar los marcos normativos de ciberseguridad para infraestructuras críticas.
3. Realizar procesos de seguimiento con las organizaciones para que desarrollen y cumplan la normativa referente a ciberseguridad.
   i. Establecer un calendario de apoyo y seguimiento con las empresas e instituciones de servicios esenciales

7. Fortalecimiento del marco legal en Ciberseguridad y TIC.

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

- Líneas de acción:

1. Proponer legislación sobre ciberdelincuencia que tenga por objeto reducir la delincuencia en línea.
2. Fomentar la creación de un proceso para supervisar la aplicación y revisión de la legislación y los mecanismos de gobernanza

8. Gestión de la comunicación en crisis de ciberseguridad.

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

- Líneas de acción:

1. Crear un comité de comunicación de crisis cibernéticas con responsabilidades específicas de sus representantes, quienes deben representar de las partes responsables del manejo de un incidente cibernético nacional (Ejemplos: CERT nacional, MITICC, etc.)
2. Producir de una matriz de riesgos cibernéticos y de reputación que puedan escalar a posibles crisis de comunicación, con ponderaciones según factibilidad y plan de acción para cada caso.
3. Desarrollar acciones de alerta temprana para la identificación de posibles crisis cibernéticas
4. Construir un mapa de audiencias clave y partes interesadas en obtener información en cuanto al desarrollo de un ataque o incidente cibernético.

5. Elaborar un plan de acción general para el manejo de incidentes o crisis cibernéticas con responsabilidades específicas según los involucrados, designación de voceros principales o secundarios, acciones de mitigación de crisis comunicacional y plan de recuperación.

6. Objetivo general

Áreas de enfoque

Teniendo en cuenta la experiencia en la implementación de la ENC 2017 así como la revisión que de la misma se realizó en 2021, se han considerado los siguientes objetivos auxiliares:

1. Desarrollo de capacidades en ciberseguridad empresarial

Las consecuencias de un ataque aumentan a medida que las interdependencias de los sistemas de estas organizaciones se vuelven más complejas. Tener un teléfono inteligente nos permite llevar una variedad de "dispositivos" (teléfono, cámara, calendario, TV, rastreador de salud, una biblioteca completa de libros y mucho más) en nuestro bolsillo, simplificando nuestras vidas. El Internet de las cosas nos permite realizar innumerables tareas al pronunciar un comando simple. Pero los procesos necesarios para administrar y mantener todas estas conexiones, incluida la ciberseguridad, también se están volviendo más complejos. La ciberseguridad debe ser entendida como una responsabilidad compartida entre las autoridades y los líderes del sector privado que haga posible mitigar riesgos y reducir los costes de ataques cibernéticos.

- Líneas de acción:

1. Fomentar la creación de asociaciones entre el sector público y el privado para promover la seguridad digital en tecnologías emergentes.
2. Crear incentivos para dinamizar los mercados a nivel nacional relacionados con la seguridad digital.
3. Establecer medidas para mejorar la seguridad digital a través de la cadena de suministro de bienes y servicios tecnologías de la información.
4. Realizar campañas de divulgación para presentar entre el sector empresarial el valor agregado de invertir en ciberseguridad.
5. Realizar campañas de comunicación para aumentar la difusión y visibilidad de las actividades de ciberseguridad que se desarrollan en cada sector.

2. Desarrollo de capacidades de ciberseguridad del turismo.

El aumento del número de transacciones comerciales en línea potenciado, sin duda, durante la pandemia COVID-19, la demanda de experiencias 'inteligentes' de viajeros, y el desarrollo de las también llamadas ciudades inteligentes (*Smart cities*) está provocando una aceleración de la digitalización de los viajes y el turismo. Según GlobalData[5], se espera que el valor de mercado de viajes en línea siga aumentando en el futuro y alcance los $ 765.3 mil millones en 2025.

[5] https://store.globaldata.com/report/online-travel-theme-analysis/

Grupos de hostelería, empresas de turismo, aerolíneas y agencias de servicios de alquiler de coches que utilizan plataformas en línea y portales de reserva son potenciales objetivos del cibercrimen. En general, todo el ecosistema de dependencia de terceros hace que sea más fácil para los cibercriminales obtener datos confidenciales.
Por esta razón es prioritario que todo el sector establezca protocolos de ciberseguridad y forme a su propio personal para mantener sus sistemas seguros y protegerse de ataques como el robo de datos, secuestro de sus servicios en línea o ataques a sus sistemas de software y hardware.

El Turismo aporta el 6.3% del Producto Interior Bruto (PIB) a la economía del país, según el Instituto Costarricense de Turismo[6]. Se trata de un sector conformado en gran mayoría por medianas y pequeñas empresas (MIPyMES) que suelen no tener presupuesto asignado específicamente para TIC ni para ciberseguridad. Las grandes cadenas hoteleras con más presupuesto suelen contar software más avanzados que sí cuentan con herramientas de protección más solventes, pero la mayoría de la industria no tiene departamentos internos de TIC y subcontratan los servicios.
El MICITT pretende potenciar el sello turístico y la ciberseguridad para presentar Costa Rica como un destino seguro desde un punto de vista también cibernético. El reciente proyecto de ley "Nómadas Digitales" busca garantizar la seguridad en la conexión a internet en lugares turísticos, además de promover la especialización en ciberseguridad de las empresas proveedoras de software para fomentar buenas prácticas tales como no guardar la información de tarjetas de crédito.

- Líneas de acción:

1. Capacitar a MIPyMES en ley de protección de datos, mercadeo, creación de marca país digital, prácticas de turismo ciberseguro, etc.
2. Crear de lineamientos básicos para el desarrollo o contratación de sistemas para el sector turismo.
3. Desarrollar capacitaciones a los profesionales del sector, así como sus proveedores de infraestructuras.
4. Desarrollar un software con los requerimientos mínimos de seguridad para las MIPyMES.
5. Promover la especialización en ciberseguridad de las empresas proveedoras de software para fomentar buenas prácticas en el sector turismo.
6. Registrar ante el ICT también a los usuarios que ofertan sus viviendas en plataformas de servicios de alojamiento por parte de no profesionales.
7. Colaborar con el sector privado para impulsar pagos en línea y la aplicación de soluciones innovadoras que mejoren los servicios de las empresas turísticas de manera segura.
8. Trabajar con el tejido turístico empresarial existente e incorporar nuevas formas de servicios turísticos por parte de no profesionales para desarrollar una campaña de concientización alrededor del concepto, para usuarios y proveedores de servicios.

[6] 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

3. Alfabetización digital

En América Latina y el Caribe (como en el resto del mundo) la brecha en la demanda de mano de obra en ciberseguridad sigue siendo importante. Aunque esta brecha ha disminuido durante los últimos dos años, un estudio de la ONG (ISC)2[7] estima que todavía hay una necesidad de 2.72 millones de profesionales de ciberseguridad en todo el mundo.

Para abordar esta problemática se recomienda la elaboración de un Plan Nacional de Alfabetización digital de sectores vulnerables con el objetivo de hacer frente a la a la necesidad de formación en cultura digital para mejorar el conocimiento en ciberseguridad, delitos informáticos y su prevención Este plan ha de contar con todas las partes interesadas para su redacción, y ha de definir metas a largo plazo, objetivos medibles y acciones que se puedan incorporar en cada etapa de la educación y el ciclo de desarrollo de la fuerza laboral.

- Líneas de acción:

1. Ciclos de charlas y conferencias en las aulas para las etapas de educación primaria y secundaria.
2. Campañas de información sobra el desarrollo de una carrera en ciberseguridad.
3. Desarrollo de entrenamientos en línea y laboratorios.
4. Fomento de concursos y competiciones que alienten la participación en ejercicios cibernéticos.

Todas estas iniciativas han de tener en cuenta dos elementos transversales fundamentales, como son el enfoque de género y la necesidad de llegar a la población más vulnerable como minorías, personas con habilidades especiales o aquellos en riesgo de exclusión por pobreza.

4. Desarrollo de Planes de Acción

La nueva estrategia contendrá planeas de acción específicos, adoptando enfoques de trabajo específicos para cada sector, con la finalidad de medir claramente el cumplimiento de los objetivos.

Para ello, se desarrollará una matriz que correlacione:

- Objetivos específicos o áreas de enfoque que se desarrollan en esta estrategia.
- Plan de acción para cada uno de los objetivos específicos con el objetivo de implementar las metas descritas por cada uno de ellos.
- Actividades que se llevarán a cabo dentro de este plan de acción.
- Responsables de implementar el plan de acción, ya sea el MICITT u otros ministerios o agencias encargados.
- Plazos para la ejecución de cada una de las actividades que formen parte del plan de acción.
-

5. Desarrollo de ciberseguridad con l el sector financiero

El sector financiero, y en particular la banca, es uno de los sectores con mayor índice de digitalización en todo el mundo. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica, realizan transacciones por internet o pagos a través de

[7] https://www.isc2.org/Research/Workforce-Study

dispositivos móviles. Esta adaptación de los modelos de negocio y la explotación de canales virtuales tiene como contrapartida la aparición de nuevos riesgos que se deben prevenir con el fin de mitigar las situaciones de fraude a los que está expuesto actualmente el sector y, por supuesto sus usuarios.

Para neutralizar lo anterior, los Bancos han de concentrar sus esfuerzos en lograr fundamentos técnicos, de fuerza laboral y de gobernanza en ciberseguridad. Esto a requiere sacar la seguridad cibernética de su nicho aislado en el negocio y extender la responsabilidad de esta a nivel de junta directiva, que pueda garantizar que la seguridad cibernética sea una problemática central en el momento de definir los productos de la empresa, sus servicios y cómo planea crecer.

- Líneas de acción:
    1. Desarrollar legislación específica sobre ciberseguridad en el sector bancario que complemente el Reglamento General del Desarrollo de la Tecnología de la Información del Consejo Nacional de Supervisión del Sistema Financiero.
    2. Fomentar espacios de colaboración entre el sector financiero y las agencias gubernamentales como el Foro Interbancario de Seguridad de la Información de la Cámara de Banca y la Asociación Bancaria Costarricense.
    3. Fortalecer la disponibilidad de capital humano, que esté desarrollado y cuente con la experiencia teórica y práctica pertinente.
    4. Desarrollar labores de concientización que cambien el enfoque de abordaje de reactivo a preventivo para desarrollar la resiliencia organizacional.
    5. Desarrollar metodología para la gestión de riesgos de proveedores.
    6. Creación de un CSIRT sectorial orientado a apoyar y gestionar las capacidades del sector financiero para mejorar la comunicación y hacer frente a amenazas.
    7. Realización de campañas de concientización para usuarios.
    8. Fortalecer las auditorías se las entidades financieras.

    Potenciar el uso del Modelo de Madurez de Gestión de la Seguridad de la Información

6. Infraestructura resiliente

El aumento de la interconectividad en la práctica totalidad de nuestras acciones está aumentando el número de infraestructuras críticas que se han de proteger. Garantizar que no se producirán incursiones maliciosas en nuestros sistemas es una quimera imposible de alcanzar. Por el contrario, las organizaciones y los países han de centrarse en sufrir los menos daños posibles cuando un ataque cibernético se produzca.

Para ello, es necesario establecer modelos de actuación que afronten de manera coordinada una respuesta eficaz que garantice la confianza en los servicios que ofrecen las organizaciones a la sociedad, especialmente cuando los servicios que ofrecen son de carácter esencial.

Los modelos estándares de ciberseguridad y ciberresiliencia son instrumentos vitales para ayudar a las organizaciones a evaluar, desarrollar y mejorar sus estrategias, metodologías y procedimientos de protección frente a las ciber amenazas. Para garantizar la ciberresiliencia se ha de establecer un mecanismo de diagnóstico y medición de la capacidad de las organizaciones para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital.

Este modelo identifica la capacidad de las organizaciones para anticiparse, resistir, recuperarse y evolucionar ante incidentes que puedan afectar a la prestación de sus servicios. Además, define

algunos dominios funcionales: política de ciberseguridad, gestión de riesgos y formación; gestión de vulnerabilidades y supervisión continua; gestión de incidentes y de la continuidad; gestión de la configuración y cambios, y comunicación.

Para desarrollar este modelo[8], será necesario establecer:

- Una metodología que contiene el marco conceptual. Su objetivo es ayudar a todas las partes interesadas en medir sus capacidades de ciberresiliencia y disponer de un procedimiento que permita conocer el grado de madurez de sus controles de ciberresiliencia. El modelo está destinado a un uso bajo la forma de consulta que puede lanzarse entre las organizaciones de cualquier sector esencial, o como herramienta de autoevaluación de las capacidades de ciberresiliencia para dichas organizaciones.
- Un diccionario de indicadores que describe los indicadores para la mejora de la ciberresiliencia en organizaciones y empresas de sectores industriales e infraestructuras críticas industriales con respecto a ámbitos de IT (Information Technology) y OT (*Operation Technology*).
- Un formulario que consiste en una plantilla con la cual las organizaciones pueden analizar su ciberresiliencia según se describe en la metodología.

7. Ciberseguridad Industrial.

La digitalización y la hiperconectividad llevada al ámbito industrial han conducido la revolución conocida como industria 4.0, amplificando la innovación y el desarrollo económico de las industrias del país.

Para asegurar que este desarrollo se hace de forma segura se han de tomar medidas para proteger los sistemas de control industrial (SCI), incluidos los sistemas de control de supervisión y adquisición de datos (SCADA por sus siglas en inglés), los sistemas de control de distribución y otros sistemas que realizan funciones de control.

Los ICS se encuentran en muchas industrias, como la eléctrica, agua y aguas residuales, petróleo y gas natural, química, farmacéutica, alimentos y bebidas, y manufacturera como, por ejemplo, la industria del motor, aeroespacial y bienes duraderos.

- Líneas de acción:

1. Promover un marco que facilite la identificación de vulnerabilidades actuales y futuras en entornos de sistemas de control y automatización industrial.
2. Promover entre las organizaciones industriales el enfoque *Security by Design* para que tengan en cuenta la ciberseguridad desde las etapas incipientes del diseño se sus productos.
3. Fomentar la adhesión de las organizaciones del sector privado a estándares industriales como la ANSI/ISA-62443[9].

[8] Basado en el modelo de Indicadores para la Mejora de la Ciberresiliencia (IMC) del INCIBE-CERT.

[9] https://www.isa.org/intech-home/2018/march-april/departments/new-isa99-standard-on-developing-products-that-are

7. Implementación y Evaluación

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

Área de enfoque / Objetivo Auxiliar	Plan de acción	Actividades	Responsables	Financiación	Plazos

Para asegurar que esta estrategia se aplica con arreglo a su plan de acción, se establece un proceso oficial de supervisión y evaluación de esta para determinar si sigue siendo pertinente en vista de la evolución de los riesgos, si sigue respondiendo a los objetivos del gobierno y qué ajustes son necesarios.

Para garantizar una supervisión y una evaluación eficaces durante la ejecución de la estrategia, el Comité Consultivo apoyara tanto el proceso de ejecución como de seguimiento de los planes de implementación que permitan supervisar y evaluar el progreso y la eficiencia de la ejecución.

La supervisión y medición del rendimiento y de la aplicación satisfactoria del plan de ejecución de la estrategia deben formar parte de los mecanismos de gobernanza establecidos. La evaluación continua del plan de ejecución (es decir, lo que marcha bien y lo que no) aporta información sobre la estrategia.

El establecimiento de métricas o indicadores fundamentales de rendimiento (IFR) para objetivos a corto, medio y largo plazo ayuda a reforzar los mecanismos de gobernanza y gestión. Los indicadores o métricas fundamentales de rendimiento deben ser: específicos, cuantificables, viables, con responsables encargados y estar dentro de un plazo determinado.