Costa Rica

Estrategia Nacional de

CIBERSEGURIDAD

2023 - 2027

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Contenido

Siglas y Acrónimos *3*

Resumen ejecutivo *4*

Antecedentes *5*

CAPÍTULO 1. Introducción *7*

CAPÍTULO 2. Construcción de la estrategia *7*

CAPÍTULO 3. Contexto actual *11*

CAPÍTULO 4. Principios rectores *15*

Respeto a los Derechos Humanos y la Privacidad **15**

Enfoque basado en riesgos y resiliencia cibernética **15**

Coordinación y corresponsabilidad de múltiples partes interesadas **16**

Fomento de Cooperación Internacional **16**

CAPÍTULO 5. Marco Estratégico para la seguridad cibernética *17*

OBJETIVO ESTRATÉGICO 1: Gobernanza **18**

OBJETIVO ESPECÍFICO 1.1 18

OBJETIVO ESPECÍFICO 1.2 19

OBJETIVO ESPECÍFICO 1.3 19

OBJETIVO ESPECÍFICO 1.4 20

OBJETIVO ESPECÍFICO 1.5 20

OBJETIVO ESTRATÉGICO 2: Gestión de Riesgos de Ciberseguridad **21**

OBJETIVO ESPECÍFICO 2.1 21

OBJETIVO ESTRATÉGICO 3: Protección y resiliencia de infraestructuras críticas frente amenazas en ciberseguridad. **22**

OBJETIVO ESPECÍFICO 3.1 22

OBJETIVO ESPECÍFICO 3.2 22

OBJETIVO ESPECÍFICO 3.3 23

OBJETIVO ESPECÍFICO 3.4 24

OBJETIVO ESPECÍFICO 3.5 25

OBJETIVO ESPECÍFICO 3.6 25
OBJETIVO ESPECÍFICO 3.7 25
OBJETIVO ESPECÍFICO 3.8 26

OBJETIVO ESTRATÉGICO 4: Cultura cibernética y sociedad. 27
OBJETIVO ESPECÍFICO 4.1 27
OBJETIVO ESPECÍFICO 4.2 27
OBJETIVO ESPECÍFICO 4.3 27
OBJETIVO ESPECÍFICO 4.4 28
OBJETIVO ESPECÍFICO 4.5 28
OBJETIVO ESPECÍFICO 4.6 28

OBJETIVO ESTRATÉGICO 5: Formación, capacitación, y habilidades de seguridad cibernética. 29
OBJETIVO ESPECÍFICO 5.1 29
OBJETIVO ESPECÍFICO 5.2 29
OBJETIVO ESPECÍFICO 5.3 30
OBJETIVO ESPECÍFICO 5.4 30

OBJETIVO ESTRATÉGICO 6: Marcos Legales y Regulatorios. 30
OBJETIVO ESPECÍFICO 6.1 31

OBJETIVO ESTRATÉGICO 7: Fomento de Cooperación Internacional 31
OBJETIVO ESPECÍFICO 7.1 31
OBJETIVO ESPECÍFICO 7.2 32
OBJETIVO ESPECÍFICO 7.3 32
OBJETIVO ESPECÍFICO 7.4 32
OBJETIVO ESPECÍFICO 7.5 33

EJES TRANSVERSALES 34
1. Alianza público-privada 34
2. Fortalecimiento del marco legal en ciberseguridad y TIC 35
3. Convenios internacionales 35
4. Colaboración y coordinación interinstitucional 35

Capítulo 8 – Reflexiones finales 36

Glosario 37

Referencias 39

Siglas y Acrónimos

CCSS	Caja Costarricense del Seguro Social
CEPAL	Comisión Económica para América Latina y el Caribe
CICTE/OEA	Comité Interamericano contra el terrorismo del Organismo de Estados Americanos
CISTE	Consejo Interinstitucional sobre Terrorismo
CNSL	Comisión Nacional de Seguridad en Línea
CSIRT	Centro de Respuesta de Incidentes de Seguridad Informática
DISNA	Dirección de Inteligencia y Seguridad Nacional
ENISA	Agencia de la Unión Europea para la Ciberseguridad
ENC	Estrategia Nacional de Ciberseguridad
ETD	Estrategia de Transformación Digital
FODESAF	Fondo de Desarrollo Social y Asignaciones Familiares
GCCD	Global Cybersecurity Center for Development
ICE	Instituto Costarricense de Electricidad
IMN	Instituto Meteorológico Nacional
IFAM	Instituto de Fomento y Asesoría Municipal
JASEC	Junta Administrativa del Servicio Eléctrico Municipal de Cartago
KISA COREA	*Korea* Internet & Security Agency
MH	Ministerio de Hacienda
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
MTSS	Ministerio de Trabajo y Seguridad Social
OEA	Organismo de Estados Americanos
OCDE	Organización para la Cooperación y el Desarrollo Económico
OIJ	Organismo de Investigación Judicial
PIB	Producto Interno Bruto
PNCTI	Plan Nacional de Ciencia, Innovación y Tecnología
PNDT	Plan Nacional de Desarrollo de Telecomunicaciones
PNSEBC	Política Nacional de Sociedad y Economía basada en el Conocimiento
PRODHAB	Agencia de Protección de datos de los Habitantes
PYMES	Pequeña y mediana empresa
RACSA	Radiográfica Costarricense Sociedad Anónima
SOC	Centro de operaciones de seguridad
SUTEL	Superintendencia de Telecomunicaciones
TI	Tecnología de la Información
TIC	Tecnologías de la Información y la Comunicación
ODS	Objetivos de Desarrollo Sostenible

Resumen ejecutivo

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

La naturaleza cambiante del ciberespacio, la mayor dependencia a las TIC y la proliferación de riesgos digitales, exigen mejoras continuas a las estrategias nacionales de ciberseguridad. La mayoría de los países han acelerado su transformación digital abordando las amenazas inmediatas y futuras a sus servicios críticos, infraestructuras, sectores, instituciones y empresas, así como a la paz y la seguridad internacionales, que podrían alterarse por el mal uso de las tecnologías digitales y la falta de resiliencia.
Para aprovechar los actuales beneficios que brinda la tecnología y gestionar los desafíos a los que conlleva la digitalización, el gobierno de Costa Rica confirma su compromiso para mantener un ciberespacio seguro a partir de la puesta al día de su Estrategia Nacional de Ciberseguridad.

Las estrategias forman parte de un proceso continuo de evaluación, desarrollo e implementación. Son herramientas vivas que se han de ajustar a las necesidades del país y reajustarse periódicamente para responder a las necesidades políticas, económicas, financieras y tecnológicas del momento. Considerando los avances a nivel nacional de Costa Rica en la madurez cibernética, resultaba necesario revisar y actualizar el marco de política pública, a fin de que refleje las oportunidades y desafíos actuales que permitan una mejora en el ámbito de la ciberseguridad en el futuro.
El propósito de esta estrategia es proveer al país de un documento integral que articule y priorice objetivos, señale políticas de apoyo y mecanismos estructurales, establezca roles y responsabilidades, asignación de recursos y rendición de cuentas.

La Estrategia Nacional de Ciberseguridad de Costa Rica 2017 (ENC 2017) proporcionó un marco estratégico para lograr los objetivos socioeconómicos que dependían de la seguridad del ciberespacio. A medida que ha aumentado la necesidad de proteger el espacio digital

para contribuir a la prosperidad del país, se ha vuelto necesaria la puesta al día de dicha estrategia para que se convierta en el pilar esencial para el diseño e implementación de instrumentos de política pública frente a los riesgos emergentes que amenazan el funcionamiento básico de la sociedad.

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

Antecedentes

Costa Rica cuenta con la Estrategia de Transformación Digital 2018-2022, que establece la hoja de ruta para la transformación digital del país y cuyo objetivo es acelerar la productividad, la competitividad y el desarrollo socioeconómico, tomando ventaja de la cuarta revolución industrial y las sociedades del conocimiento y para procurar el bienestar de todos sus habitantes de manera inclusiva y potenciar el desarrollo sostenible del país. Dicha estrategia aborda el tema de la ciberseguridad, pero no de forma robusta. Cuando se realice su revisión, ya que las actividades de esta estrategia finalizaron el 2021, se recomienda el fortalecimiento de la ciberseguridad, como un eje transversal, en los objetivos estratégicos y específicos de la nueva ruta de transformación digital del país.

Ante los ataques cibernéticos del presente año (2022), el Gobierno (2018-2022) emitió la Directriz No. 133-MP-MICITT, en la que se giraron varias instrucciones a las entidades de la Administración Pública Central, entre ellas, la de reportar los incidentes cibernéticos al CSIRT-CR y de implementar medidas y mecanismos de seguridad.

El nuevo Gobierno (2022-2026) emitió el Decreto Ejecutivo No. 43542-MP-MICITT de 2022, donde se declaró estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas

de información de distintas instituciones del país. La intención de ese decreto es facilitar la disponibilidad de recursos y los actos administrativos necesarios para atender la emergencia.

Costa Rica ha llevado un proceso de acciones para mejorar la ciberseguridad nacional, lo cual llevó al país en el año 2017 a generar un norte común desarrollando su primera Estrategia Nacional de Ciberseguridad, que articuló una visión nacional para la coordinación en respuesta a las amenazas cibernéticas. Un documento que se estructuró a partir de una serie de principios rectores, un marco con un objetivo general y ocho objetivos específicos. Es importante recordar que mediante, el Decreto N° 37.052 se creó 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 personas expertas destinado a prevenir y responder tanto amenazas como ataques cibernéticos contra las instituciones gubernamentales. El trabajo del CSIRT Nacional empezó a ser efectivo hasta el año 2018, cuando se convierte en la instancia líder 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 es el de posicionar a Costa Rica entre los países con mayor madurez en ciberseguridad de la región, al tiempo que se mejoren las capacidades de todos sus sectores, tanto desde el punto de vista de la inversión en tecnología como el aprovechamiento de las oportunidades que de este desarrollo pudieran surgir.

El MICITT ha liderado los trabajos para mejorar los estándares técnicos que tienen que cumplir las instituciones que evalúa la Contraloría General de la República 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 2020, situó a Costa Rica en el número 76 a nivel global y la posición 8 de América, mejorando 39 lugares respecto de la anterior medición. El reporte del Estado de la Ciberseguridad de la OEA/BID también refleja las mejoras del país en las cinco dimensiones en las que este informe basa

el nivel de madurez en ciberseguridad de los países. Este informe destaca especialmente la madurez del país respecto a los marcos legales y regulatorios y a los marcos de capacitación profesional. En general, Costa Rica ha demostrado que está dispuesto a invertir el capital político, el tiempo, el dinero y los recursos para contar con un ciberespacio más seguro para sus ciudadanos. Sin embargo, cabe mencionar el National Cyber Security Index, en el cual para el año 2020 Costa Rica se encontró en la posición 53, siendo el número 5 en América, pero para el año 2022, se descienden 22 puestos, siendo ahora la posición #75.

CAPÍTULO 1. Introducción

En la era de la transformación digital, la ciberseguridad se ha convertido en una preocupación crítica para los gobiernos de todo el mundo. La creciente dependencia de la tecnología y el aumento de las amenazas cibernéticas hacen que la protección de los sistemas informáticos y de tecnología de la información de un país sea esencial para garantizar la seguridad nacional y la estabilidad económica.

La creación de una estrategia nacional de ciberseguridad se ha convertido en un requisito fundamental para proteger la infraestructura crítica de un país, incluyendo sus redes de comunicaciones, sistemas de energía y transporte, instituciones financieras, así como los datos personales y la información confidencial de los ciudadanos.

La estrategia nacional de ciberseguridad aborda las amenazas cibernéticas desde una perspectiva holística y considera factores como la gestión de riesgos, la protección de la información, la gestión de incidentes y la continuidad del negocio. Además, involucra a todas las partes interesadas, desde los gobiernos y las empresas hasta la sociedad civil y el público en general.

CAPÍTULO 2. Construcción de la estrategia

La creación de una estrategia nacional de ciberseguridad requiere un enfoque riguroso y una evaluación exhaustiva de la situación actual de la seguridad cibernética del país, así como la incorporación de métricas y estadísticas para evaluar el proceso de implementación

de esta. Solo entonces se pueden identificar las debilidades y desarrollar una estrategia coherente y efectiva para fortalecer las capacidades de ciberseguridad del país.
Aunado a lo anterior, para la elaboración de la estrategia se consideraron los resultados del análisis de las evaluaciones del reporte de riesgos, avances y el camino a seguir en América Latina y el Caribe del 2016 y 2020 (OEA y BID), el cual ofrece una perspectiva longitudinal sobre el desarrollo detallado de la capacidad de seguridad cibernética y una oportunidad para Costa Rica de evaluar el progreso y avances en ciberseguridad para alinear las estrategias nacionales de seguridad y los planes de acción, con el fin de para fortalecer las capacidades cibernéticas. Estos datos proporcionan una visión sobre el impacto de las inversiones realizadas en este campo, así como identificar los logros obtenidos en la implementación de las estrategias y la orientación de las políticas y prioridades de inversión.

La base de los estudios regionales de la OEA y el BID en 2016 y 2020 utilizada fue mediante el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés), el cual sigue un enfoque integral que entiende la capacidad dentro de cinco dimensiones:

Ilustración 1 - Dimensiones del CMM

Fuente: Elaboración propia, 2023.

Este modelo tiene como objetivo medir el nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica el reflejo de su grado de avance en la materia. Se utilizan cinco etapas de madurez, que se determinan mediante

una evaluación, que van desde la etapa inicial, que es la más básica, hasta la etapa dinámica, la más avanzada.

Tabla 1 - Cinco etapas de madurez de la capacidad de ciberseguridad

Dinámica: En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). Las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias con calma. Sin embargo, la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.	
Estratégica: En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones.	
Consolidada: Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida.	
Formativa: Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto.	
Inicial: En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estado muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética.	

Fuente: El Modelo de Madurez de la Capacidad de Ciberseguridad, Revista Seguridad 360, 2022.

Bajo este enfoque el país ocupa el puesto número 84 en la región. De los análisis y mediciones del informe de la OEA y el BID en 2016 y 2020 se aprecian los indicadores generados para Costa Rica basados en las dimensiones del CMM.

Tabla 2 - Dimensiones del CMM

Indicadores 2016 y 2020 de Costa Rica

Fuente: Informe de Revisión de la estrategia nacional de ciberseguridad de Costa Rica (2017) elaborado por (CICTE/OEA)

Fuente: Informe de Revisión de la estrategia nacional de ciberseguridad de Costa Rica (2017) elaborado por (CICTE/OEA)

CAPÍTULO 3. Contexto actual

Según la "Guía Estratégica para Mejorar la Postura de Ciberseguridad", un instrumento de evaluación desarrollado por Amazon Web Services (AWS) en colaboración con el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) y la Organización de los Estados Americanos (OEA), se examina el estado actual y panorama de la ciberseguridad en Costa Rica. Esta guía proporciona información sobre el contexto actual del país en relación con la ciberseguridad, destacando:

Desde el año 1997, el Organismo de Investigación Judicial cuenta con una sección de análisis informática, pero no es hasta el 2004, que se constituye como una sección de delitos informáticos para combatir el cibercrimen.

En el año 2001, se promulga la Ley No. 8148, mediante la cual se adicionan varios delitos informáticos al Código Penal (Ley No. 4573). En el año 2012, mediante la Ley No. 9048 se aprobó la reforma y adición de varios artículos y la modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal. En el año 2013, mediante la Ley. No. 9135, se adicionan y reforman varios delitos informáticos a la legislación penal costarricense.

Costa Rica fue uno de los primeros países en LATAM en adoptar las medidas del Convenio de Budapest, el cual firmó el 10 de abril de 2019. Con esta firma, Costa Rica se comprometió a adaptar la legislación nacional para cumplir con los estándares establecidos en el convenio y cooperar con otros países en la lucha contra el cibercrimen. La ratificación de este tratado refleja el compromiso de Costa Rica para fortalecer su capacidad en la prevención y combate de delitos informáticos, mejorar la cooperación internacional en este ámbito y proteger a sus ciudadanos en el entorno digital.

Al adoptar estas medidas, los países que se adhieren al Convenio de Budapest contribuyen a un enfoque global más efectivo y coordinado en la lucha contra el cibercrimen y a la protección de sus ciudadanos en el entorno digital.

En el año 2011, mediante Ley No. 8968, se promulgó la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, y en el año 2012, mediante Decreto Ejecutivo No. 37,554-JP se aprobó su reglamento.

El país cuenta con un centro de respuesta a incidentes cibernéticos denominado CSIRT-CR, con sede en el MICITT, y que fue legamente establecido en el año 2012 (Decreto No. 37052-MICIT de 2012), pero que inició operaciones formalmente hasta el año 2018. Según ese decreto, el CSIRT-CR tendrá facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la seguridad de la información y cibernética. De lo anterior, se desprende que el mandato legal y naturaleza del CSIRT-CR es de un CSIRT de Gobierno, y no de un CSIRT nacional.

El país cuenta con una Estrategia Nacional de Ciberseguridad (ENC) aprobada en el año 2017, que define la hoja de ruta y los objetivos estratégicos para mejorar las capacidades de ciberseguridad del país. Sin embargo, el periodo de vigencia de la ENC terminó en el año 2021. Esta ENC está basada en 8 objetivos específicos: (i) coordinación, (ii) conciencia pública, (iii) desarrollo de la capacidad nacional de la seguridad cibernética, (iv) fortalecimiento del marco jurídico en ciberseguridad y TIC, (v) protección de infraestructuras críticas, (vi) gestión de riesgos, (vii) cooperación y compromiso internacional, y (viii) implementación, seguimiento y evaluación.
De conformidad con la ENC, específicamente en su línea estratégica 1.1., se designa al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) como ente

coordinador de la ciberseguridad nacional y será el punto focal a nivel nacional e internacional sobre temas relacionados con la seguridad cibernética. Lo anterior en concordancia con el Decreto Ejecutivo No. 41187-MP-MIDEPLAN, donde al MICITT se le otorga la rectoría en temas de ciencia, tecnología, telecomunicaciones y gobernanza digital.

El país participa activamente en el frente de cooperación internacional en ciberseguridad. Costa Rica fue uno de los primeros países de LATAM en adherirse al Convenio de Budapest sobre Ciberdelincuencia, específicamente en el año 2017 mediante Ley No. 9452.

En el año 2020, el MICITT adopta el Código Nacional de Tecnología Digital - recientemente actualizado a su versión 3.0 - como un compendio de criterios técnicos básicos -que incluye aspectos de seguridad tecnológica e infraestructura y tecnología en la nube- que todo proyecto digital debe contemplar para su desarrollo dentro de las instituciones de la administración pública. Además, es la guía básica para que la Dirección de Gobernanza Digital del MICITT pueda valorar objetivamente los proyectos tecnológicos de importancia nacional y en caso de que estos reúnan los criterios técnicos mínimos deseables, se pueda otorgar el Sello de Gobierno Digital -según los lineamientos para su otorgamiento.

A finales del año 2021, el MICITT adoptó las normas técnicas para la gestión y el control de las tecnologías de información, las cuales sustituyeron las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CODFOE), derogadas por la Contraloría General de la República (CGR), mediante Resolución No. R-DC-17- 2020, a partir del 1ero de enero del 2022. En esa misma resolución de la CGR se modifica parcialmente las Normas de Control Interno para el Sector Público (N-2-2009CO-DFOE).

Asimismo, en el año 2021, el MICITT publicó, en colaboración con la OEA y Cyber4Dev, un reporte de revisión de la estrategia nacional de ciberseguridad 2017, en donde se analizaron y evaluaron, en conjunto con varios actores del ecosistema, los objetivos de esta y su proceso de implementación. De este reporte se desprende que no se recolectaron métricas y estadísticas para determinar el nivel de cumplimiento y éxito de los 8 objetivos específicos arriba indicados. También se señaló que, dicha estrategia no fue ampliamente comunicada y visibilizada al público en general. Este reporte también generó una serie de recomendaciones.

Ante los ataques cibernéticos del año 2022, el Gobierno (2018-2022) emitió la Directriz No. 133-MP-MICITT, en la que se giraron varias instrucciones a las entidades de la Administración Pública Central, entre ellas, la de reportar los incidentes cibernéticos al CSIRT-CR y de implementar medidas y mecanismos de seguridad.

El nuevo Gobierno (2022-2026) emitió el Decreto Ejecutivo No. 43542-MP-MICITT de 2022, donde se declaró estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información de distintas instituciones del país. La intención de ese decreto es facilitar la disponibilidad de recursos y los actos administrativos necesarios para atender la emergencia.

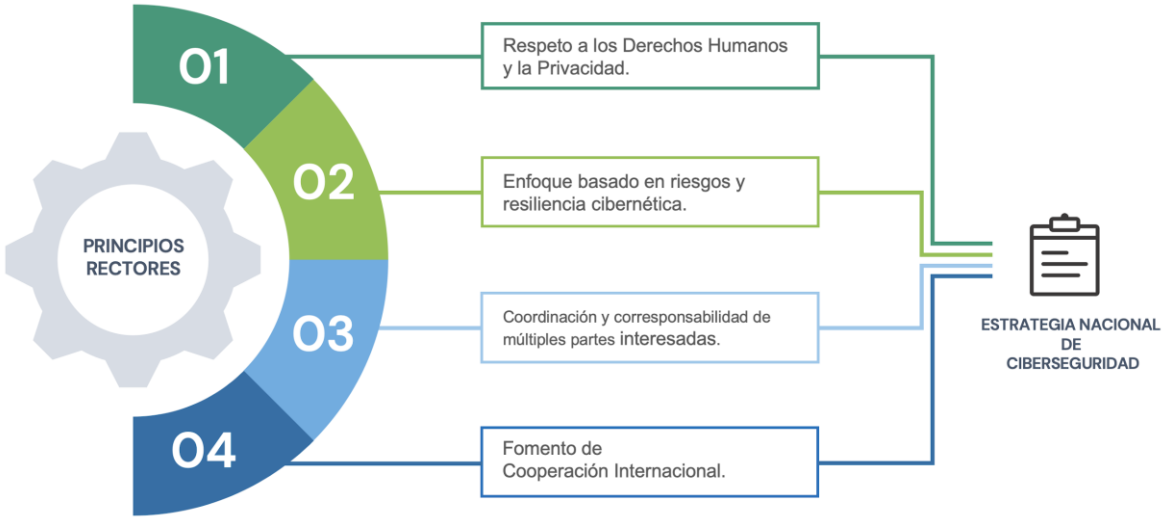
Con fundamento en el anterior decreto y la Ley No. 8488, en junio del año en curso, se emitió un Plan General de la Emergencia (PGE), donde se da una explicación causal del evento generador de la emergencia, la estimación de los daños y pérdidas, la definición de las acciones, las obras necesarias para su atención, así como la estimación de los recursos. Además, en el PGE se cita el Informe de Diagnóstico del Sector Público MICITT- DGD-INF-099-2022, en el cual se evidencian hallazgos y oportunidades de mejoras en materia de ciberseguridad y gobernanza de la tecnología, los cuales son insumos para la estrategia para determinar la situación actual, brechas y oportunidades para mejorar la postura de ciberseguridad a nivel país.

Entre las iniciativas propuestas en el PGE figura la creación de un “Protocolo para el desarrollo de acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional”, el cual fue desarrollado y está en proceso de revisión por parte de un equipo interinstitucional compuesto por la Comisión Nacional de Emergencias, el CSIRT-CR del MICITT, Instituto Costarricense de Electricidad y el Viceministerio de Telecomunicaciones del MICITT.

CAPÍTULO 4. Principios rectores

Esta estrategia está motivada en los siguientes principios rectores:

Ilustración 2 - Principios Rectores



Respeto a los Derechos Humanos y la Privacidad

El respeto a los Derechos Humanos y la privacidad es fundamental en cualquier sociedad que busque garantizar la dignidad y el bienestar de sus ciudadanos. La protección de la privacidad individual y la observancia de los Derechos Humanos son valores esenciales que deben ser priorizados en todas las políticas y acciones, especialmente en el ámbito de la tecnología y la seguridad digital. Al considerar la creciente interconexión de nuestras vidas a través de la tecnología, es imprescindible que se establezcan salvaguardias adecuadas para garantizar que los avances tecnológicos no menoscaben estos principios fundamentales. Esto implica un enfoque equilibrado en la promoción de la innovación, la seguridad y el respeto a la privacidad, para lograr un entorno digital en el que los Derechos Humanos sean respetados y protegidos.

Enfoque basado en riesgos y resiliencia cibernética

El enfoque basado en riesgos y la resiliencia cibernética son componentes clave para abordar eficazmente las amenazas en el ámbito digital. Este enfoque permite la identificación y evaluación de riesgos, lo que facilita la implementación de medidas de

protección y la preparación adecuada ante posibles incidentes. La resiliencia cibernética implica la capacidad de anticiparse, resistir y recuperarse de ataques informáticos, garantizando la continuidad y estabilidad de los sistemas y la información.

Coordinación y corresponsabilidad de múltiples partes interesadas

La coordinación y corresponsabilidad entre múltiples partes interesadas son fundamentales para abordar con éxito los desafíos en materia de ciberseguridad. La colaboración entre gobiernos, empresas, organizaciones no gubernamentales y ciudadanos permite la creación de un enfoque unificado y eficaz en la protección del entorno digital. Este trabajo conjunto fomenta la adopción de medidas preventivas y correctivas, así como el intercambio de información y conocimientos, para garantizar una respuesta integral y efectiva frente a las amenazas cibernéticas.

Fomento de Cooperación Internacional

La cooperación internacional es crucial para enfrentar de manera efectiva los desafíos globales en materia de ciberseguridad. Al trabajar conjuntamente, los países pueden compartir conocimientos, recursos y mejores prácticas para desarrollar estrategias y soluciones más sólidas, así como la cooperación en implementar programas de desarrollo de conocimiento y capacidades de ciberseguridad. Esta colaboración transfronteriza permite la creación de una red de apoyo mutuo que fomenta un enfoque unificado en la lucha contra las amenazas cibernéticas, promoviendo un entorno digital más seguro y protegido a nivel mundial.

CAPÍTULO 5. Marco Estratégico para la seguridad cibernética

La Estrategia Nacional de Ciberseguridad es una herramienta esencial para garantizar la seguridad y protección de la información y sistemas críticos del Estado y de los ciudadanos. El objetivo principal es establecer un marco de acción integral que permita prevenir y mitigar los riesgos y amenazas en el entorno digital, fomentar la innovación y el desarrollo de soluciones en ciberseguridad, fortalecer la capacidad de respuesta ante incidentes de ciberseguridad, promover una cultura de seguridad sólida; así como la concientización de los ciudadanos con el fin ayudar a garantizar la estabilidad del país y su economía, proteger la información personal y crítica del Estado y de los ciudadanos, y mantener la confianza en el uso de los sistemas digitales.

Para que estos objetivos sean realizables se debe llevar a cabo un programa que contenga todas acciones necesarias con el objetivo de implementar y aumentar las capacidades de ciberseguridad como Identificación, detección, protección, respuesta y recuperación, a un nivel holístico contemplando todas las áreas para establecer un nivel de madurez deseado en las instituciones de gobierno.

La estrategia de ciberseguridad se basa en siete objetivos fundamentales y cada uno desarrollado de acuerdo con los marcos y buenas prácticas de ciberseguridad. Asimismo, se integra la ciberseguridad con la gestión de riesgos y la continuidad para abarcar de forma integral una estrategia robusta de ciberseguridad.

Ilustración 3 - Objetivos estratégicos

Fuente: Elaboración propia, 2023.

OBJETIVO ESTRATÉGICO 1: Gobernanza

La gobernanza efectiva en ciberseguridad es un componente crucial para garantizar la protección y resiliencia de la infraestructura digital de una nación, así como para promover un entorno en línea seguro y confiable para sus ciudadanos. El objetivo de la estrategia es establecer objetivos claros y ambiciosos que plasmen la visión del gobierno en este ámbito. Para asegurar una efectiva implementación, es necesario delinear las funciones y responsabilidades de las entidades involucradas, identificando y otorgando poder a la autoridad competente encargada de la ejecución. Además, se debe implementar un mecanismo que permita identificar e involucrar a las entidades gubernamentales que serán responsables de llevar a cabo la estrategia, asegurando una cooperación efectiva y eficiente entre los diferentes actores.

OBJETIVO ESPECÍFICO 1.1
1.1. **Fortalecer la gobernanza** en el ámbito de la ciberseguridad.
Líneas de acción

1.1.1. Desarrollar un marco regulatorio sólido y actualizado en materia de ciberseguridad, que permita una mejor coordinación entre los distintos actores involucrados, tanto del sector público como privado.

1.1.2. Establecer mecanismos de colaboración y comunicación eficientes entre las instituciones gubernamentales, empresas del sector, organismos internacionales y expertos en la industria para el intercambio de información y buenas prácticas.

1.1.3. Impulsar la creación de una Agencia Nacional de Ciberseguridad con las competencias suficientes para emitir lineamientos de carácter vinculante a las instituciones del sector público, así como recomendaciones al sector privado.

OBJETIVO ESPECÍFICO 1.2
1.2. **Asegurar el presupuesto** adecuado para la implementación de planes de acción en materia de ciberseguridad.
Líneas de acción
1.2.1. Identificar las necesidades financieras a corto, mediano y largo plazo para la ejecución de proyectos, medidas y acciones estratégicas en el ámbito de la ciberseguridad. 1.2.2. Desarrollar un plan de inversión y asignación de recursos que garantice la disponibilidad de fondos suficientes para llevar a cabo iniciativas propuestas, incluyendo la posibilidad de buscar financiamiento externo, cuando sea necesario para la implementación de las políticas y acciones en materia de ciberseguridad, priorizando las áreas de mayor impacto y urgencia. 1.2.3. Asegurar la asignación de presupuesto específico para ciberseguridad en los organismos gubernamentales. Garantizar la inclusión de partidas presupuestarias específicas destinadas a ciberseguridad en los diferentes organismos gubernamentales responsables de la implementación de acciones y políticas en este ámbito. 1.2.4. Fomentar la colaboración público-privada en la financiación de proyectos de ciberseguridad. Estimular la inversión y la participación del sector privado en la financiación de proyectos de ciberseguridad, mediante incentivos fiscales, subvenciones u otros mecanismos de apoyo financiero.

OBJETIVO ESPECÍFICO 1.3
1.3. Garantizar la **cooperación interinstitucional** en la implementación de políticas, estrategias y acciones en materia de ciberseguridad a nivel nacional e internacional.
Líneas de acción
1.3.1. Desarrollar protocolos y mecanismos de comunicación eficientes. Establecer protocolos y sistemas de comunicación que permitan un intercambio de información ágil y seguro entre las diferentes instituciones gubernamentales involucradas en ciberseguridad. 1.3.2. Elaborar planes de acción en conjunto en materia de ciberseguridad.

Definir objetivos, metas y acciones específicas para abordar los desafíos y prioridades comunes en ciberseguridad, en colaboración con todos los organismos gubernamentales pertinentes.

1.3.3. Fomentar la capacitación y formación conjunta.
Organizar y diseñar programas de formación y capacitación en ciberseguridad para el personal de las instituciones gubernamentales, promoviendo la colaboración y el aprendizaje conjunto.

1.3.4. Realizar ejercicios y simulacros interinstitucionales.
Implementar ejercicios y simulacros que involucren a diferentes instituciones gubernamentales, con el fin de evaluar y mejorar la coordinación y respuesta ante incidentes de ciberseguridad.

OBJETIVO ESPECÍFICO 1.4
1.4. Garantizar la **cooperación intersectorial** en la implementación de políticas, estrategias y acciones en materia de ciberseguridad, involucrando a los distintos sectores relevantes de la sociedad.
Líneas de acción

1.4.1. Establecer una plataforma de colaboración intersectorial en ciberseguridad.
Crear un espacio de diálogo y coordinación que involucre a representantes de diferentes sectores, como gobierno, academia, industria y sociedad civil, para abordar de manera conjunta los desafíos y oportunidades en ciberseguridad.

1.4.2. Fomentar la participación activa de los distintos sectores en la toma de decisiones.
Establecer mecanismos de consulta y participación para que los diferentes sectores puedan contribuir con sus conocimientos y perspectivas en la formulación de políticas y acciones en materia de ciberseguridad.

1.4.3. Crear alianzas y acuerdos de colaboración intersectoriales.
Estimular la firma de acuerdos de cooperación entre los distintos sectores para compartir recursos, conocimientos y buenas prácticas en ciberseguridad, impulsando proyectos y acciones conjuntas.

1.4.4. Establecer un sistema de alerta y respuesta intersectorial ante incidentes de ciberseguridad
Implementar mecanismos de comunicación y coordinación que permitan una rápida y eficiente respuesta a incidentes de ciberseguridad, involucrando a los distintos sectores afectados y movilizando los recursos necesarios.

1.4.5. Fomentar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad.
Incentivar la colaboración entre los distintos sectores en proyectos de investigación y desarrollo tecnológico en el ámbito de la ciberseguridad, promoviendo la transferencia de conocimientos y la adopción de soluciones innovadoras.

OBJETIVO ESPECÍFICO 1.5
1.5. Desarrollar **un marco legal y regulatorio integral** que permita la gobernanza nacional de la ciberseguridad.
Líneas de acción

1.5.1. Consultar y colaborar con actores clave en la elaboración de un marco legal y regulatorio. Involucrar a representantes de diferentes sectores, como gobierno, academia, industria y sociedad civil, en un proceso de consulta y colaboración para identificar las necesidades, desafíos y oportunidades en la gobernanza nacional de la ciberseguridad. Esto asegurará que el marco legal y regulatorio sea integral y refleje las diversas perspectivas y realidades. 1.5.2. Análisis y adaptación de las mejores prácticas internacionales. Investigar y analizar las mejores prácticas y experiencias internacionales en materia de marcos legales y regulatorios en ciberseguridad. Adaptar estos enfoques al contexto nacional, considerando las características y desafíos específicos del país, para desarrollar un marco legal y regulatorio sólido, actualizado y acorde con las tendencias globales en la materia.

OBJETIVO ESTRATÉGICO 2: Gestión de Riesgos de Ciberseguridad

El Objetivo Estratégico 2, centrado en la Gestión de Riesgos de Ciberseguridad, busca establecer un enfoque proactivo y sistemático para identificar, evaluar y abordar las amenazas y vulnerabilidades en el entorno digital. Esta gestión de riesgos es fundamental para fortalecer la resiliencia de las infraestructuras críticas, proteger los activos de información y garantizar la continuidad de las operaciones en caso de incidentes cibernéticos. Al adoptar una estrategia basada en la gestión de riesgos, se promueve la colaboración entre el sector público y privado, permitiendo una toma de decisiones más informada y la asignación adecuada de recursos para minimizar los riesgos y mejorar la seguridad en el ciberespacio.

OBJETIVO ESPECÍFICO 2.1
2.1. Definir un **mecanismo de gestión de riesgos** en ciberseguridad que permita la identificación, evaluación y mitigación de amenazas y vulnerabilidades.
Líneas de acción
2.1.1. Establecer un marco de gestión de riesgos en ciberseguridad. Desarrollar un marco metodológico y normativo que oriente la gestión de riesgos en ciberseguridad, incluyendo la identificación, evaluación, priorización y tratamiento de los riesgos. 2.1.2. Capacitar al personal en la aplicación del mecanismo de gestión de riesgos.

	Implementar programas de capacitación y formación para el personal encargado de la gestión de riesgos en ciberseguridad, asegurando que cuenten con las habilidades y conocimientos necesarios para aplicar el mecanismo de manera efectiva.
2.1.3.	Monitorear y actualizar periódicamente el mecanismo de gestión de riesgos. Establecer procesos de seguimiento y revisión periódica del mecanismo de gestión de riesgos en ciberseguridad, adaptándolo a las nuevas amenazas, vulnerabilidades y tendencias en el ámbito de la ciberseguridad.

OBJETIVO ESTRATÉGICO 3: Protección y resiliencia de infraestructuras críticas frente amenazas en ciberseguridad.

El Objetivo Estratégico 3 aborda la Protección y Resiliencia de Infraestructuras Críticas frente a amenazas en ciberseguridad, enfocándose en salvaguardar los sistemas esenciales para el funcionamiento y bienestar de la sociedad. Esta meta busca garantizar la disponibilidad, integridad y confidencialidad de dichas infraestructuras, implementando medidas preventivas y de respuesta ante incidentes cibernéticos, fortaleciendo así la capacidad de recuperación y adaptación ante posibles ataques.

OBJETIVO ESPECÍFICO 3.1	
3.1.	Establecer un **inventario actualizado y priorizado de las infraestructuras críticas** en función de su importancia, vulnerabilidad y potencial impacto en caso de un incidente de ciberseguridad.
Líneas de acción	
3.1.1.	Identificar y categorizar las infraestructuras críticas. Realizar un diagnóstico para identificar y clasificar las infraestructuras críticas en función de su importancia, vulnerabilidad y potencial impacto en caso de un incidente de ciberseguridad.

OBJETIVO ESPECÍFICO 3.2	
3.2.	Crear y mantener un **conjunto de normativas, estándares y directrices** específicos para garantizar la protección y resiliencia de las infraestructuras críticas en materia de ciberseguridad alineados a estándares internacionales en la industria.
Líneas de acción	

3.2.1. Desarrollar un marco normativo y de buenas prácticas para la protección de infraestructuras críticas.
Establecer normas, estándares y directrices para la protección y resiliencia de las infraestructuras críticas en materia de ciberseguridad, basadas en las mejores prácticas internacionales.

OBJETIVO ESPECÍFICO 3.3

3.3. Desarrollar y mantener una infraestructura de monitoreo y alerta temprana que permita la detección, prevención y respuesta rápida a incidentes de ciberseguridad que afecten a infraestructuras críticas.

Líneas de acción

3.3.1. Fomentar la creación de SOC sectoriales.

3.3.2. Implementar un SOC nacional y mecanismos de coordinación y articulación con los SOC sectoriales, utilizando sistemas de monitoreo y alerta temprana.
Instalar y mantener sistemas de monitoreo y alerta temprana que permitan detectar, prevenir y responder de manera eficiente a incidentes de ciberseguridad que afecten a las infraestructuras críticas. Para ello se plantea la creación de un SOC Nacional y SOC sectoriales los cuales estarían operando 24/7:

- **SOC Nacional**: Ente supervisor de los sectores, que estaría a cargo del monitoreo, prevención; además de iniciar actividades de respuesta en coordinación con los SOC Sectoriales y equipos de expertos de las organizaciones. Proveerá insumos para elaboración y diseño de protocolos de ciberseguridad y verificar el cumplimiento de normativas.
- **SOC Sectoriales** se incluye:
    1. SOC de Gobierno e instituciones definidas como servicios esenciales: Ministerio de Presidencia, Ministerio de Comercio Exterior, Ministerio de Relaciones Exteriores y Culto, Ministerio de Economía, Industria y Comercio, Ministerio de Agricultura y Ganadería, Ministerio de Cultura y Juventud, Ministerio de Planificación Económica y Política Económica, Ministerio de Trabajo y Seguridad Social, Ministerio Vivienda y Asentamientos Humanos Además se incluye Instituto de Acueductos y Alcantarillados y ASADAS, Bomberos de Costa Rica, Cruz Roja, Comisión Nacional de Prevención de Riesgos y Atención de Emergencias, Instituto Costarricense de Electricidad (ICE), Compañía Nacional de Fuerza y Luz, 911.
    2. SOC Salud: Ministerio Salud Pública, CCSS (29 dependencias), , Instituto Nacional de Seguros (INS), Cámara de Salud Privada y otras organizaciones.
    3. SOC Transporte: Ministerio de Obras Públicas y Transporte (MOPT): Junta de Administración Portuaria y de Desarrollo Económico de la Vertiente Atlántica (JAPDEVA), operadores de concesiones como por ejemplo los aeropuertos y puertos marítimos.
    4. SOC Financiero: Ministerio Hacienda, la banca pública y privada, Superintendencias, Banco Central de Costa Rica, cooperativas financieras, entre otras instituciones públicas y privadas del sector financiero.
    5. SOC Educación: Ministerio de Educación Pública:, Ministerio de Trabajo, Seguridad Social, Instituto Nacional de Aprendizaje (INA), Universidades públicas y privadas, entre otras instituciones públicas y privadas del sector de la educación.

6. SOC Energía/Telecomunicaciones: Ministerio de Ambiente y Energía y Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, Instituto Costarricense de Electricidad (ICE),Refinadora Costarricense de Petróleo (RECOPE), Operadores privados, Proveedores eléctricos, proveedores de Telecom, entre otras instituciones públicas y privadas del sector de energía y telecomunicaciones.
7. SOC Seguridad: Ministerio de Justicia y Paz, Ministerio de Seguridad, Ministerio de Gobernación y Policía, Policía de Control de Drogas, Dirección de Inteligencia y Seguridad (DIS), Organismo de Investigación Judicial (OIJ), entre otras instituciones públicas y privadas del sector seguridad.

- **CSIRT Nacional**: Centro de Respuesta de Incidentes de Seguridad Informática consiste en un equipo de expertos en seguridad responsable de recibir, analizar y responder a incidentes de seguridad.
  Evaluar la gravedad de la amenaza y el impacto que puede tener en la organización.
  Desarrollar estrategias de seguridad, como también apoyan a otros equipos con la prevención de amenazas.
  Realizar actividades de formación de capacidades en el área de ciberseguridad. Coordinar lo respectivo con la adopción de cursos que se están promoviendo de forma obligatoria relacionados a buenas prácticas de ciberseguridad.

OBJETIVO ESPECÍFICO 3.4
3.4. Fomentar una **red de colaboración** efectiva entre instituciones gubernamentales, operadores de infraestructuras críticas y otros actores relevantes para compartir información y recursos en materia de protección y resiliencia.
Líneas de acción
3.4.1. Promover la cooperación entre los actores responsables de infraestructuras críticas. Fomentar la colaboración entre las instituciones gubernamentales, operadores de infraestructuras críticas y otros actores relevantes para compartir información, experiencias y recursos en materia de protección y resiliencia.

OBJETIVO ESPECÍFICO 3.5
3.5. **Mejorar la capacidad de respuesta y resiliencia** de los actores responsables de infraestructuras críticas mediante la realización periódica de ejercicios y simulacros que evalúen y refuercen sus habilidades y protocolos.
Líneas de acción
3.5.1. Realizar ejercicios y simulacros de respuesta a incidentes. Organizar ejercicios y simulacros periódicos que involucren a los actores responsables de las infraestructuras críticas, con el fin de evaluar y mejorar la capacidad de respuesta y resiliencia frente a incidentes de ciberseguridad.

OBJETIVO ESPECÍFICO 3.6
3.6. Establecer **planes de contingencia y recuperación**.
Líneas de acción
3.6.1. Desarrollar y actualizar planes de contingencia y recuperación para cada infraestructura crítica, garantizando una respuesta organizada, eficiente y rápida en caso de incidentes de ciberseguridad. 3.6.2. Elaborar y mantener planes de contingencia y recuperación para cada infraestructura crítica, que incluyan protocolos de actuación, asignación de recursos y responsabilidades en caso de un incidente de ciberseguridad.

OBJETIVO ESPECÍFICO 3.7
3.7. **Fomentar la investigación y el desarrollo** en protección de infraestructuras críticas.
Líneas de acción
3.7.1. Impulsar la innovación y el avance tecnológico en el ámbito de la protección y resiliencia de infraestructuras críticas, mediante el apoyo a la investigación y el desarrollo de soluciones y metodologías avanzadas en ciberseguridad. 3.7.2. Incentivar la investigación y el desarrollo de soluciones tecnológicas y metodologías innovadoras para mejorar la protección y resiliencia de las infraestructuras críticas en el ámbito de la ciberseguridad.

OBJETIVO ESPECÍFICO 3.8
3.8. **Mejorar las capacidades del CSIRT-CR** para enfrentar de manera efectiva y eficiente los incidentes de ciberseguridad.
Líneas de acción
3.8.1. Capacitación y formación continúas del personal del CSIRT-CR. Brindar capacitación y formación técnica regular al personal del CSIRT, asegurando que cuenten con las habilidades y conocimientos necesarios para detectar, prevenir, analizar y responder a incidentes de ciberseguridad. 3.8.2. Fortalecer la infraestructura tecnológica del CSIRT. Invertir en la adopción y actualización de herramientas y tecnologías de vanguardia para el monitoreo, análisis y respuesta a incidentes de ciberseguridad, mejorando la eficiencia y eficacia del CSIRT-CR. 3.8.3. Establecer alianzas y cooperación con otros CSIRTs y organizaciones especializadas. Fomentar la colaboración y el intercambio de información y experiencias con otros CSIRTs, tanto nacionales como internacionales, así como con organizaciones especializadas en ciberseguridad, para mejorar las capacidades del CSIRT-CR y mantenerse al tanto de las últimas tendencias y amenazas. 3.8.4. Desarrollar e implementar protocolos y procedimientos estandarizados. Elaborar y mantener protocolos y procedimientos estandarizados para la gestión de incidentes de ciberseguridad, lo que permitirá al CSIRT-CR actuar de manera rápida, organizada y coherente ante cualquier eventualidad, incluyendo mecanismos de reporte e intercambio seguro de información entre autoridades, entidades y sistema financiero. 3.8.5. Promover la investigación y el desarrollo en ciberseguridad Impulsar actividades de investigación y desarrollo en el ámbito de la ciberseguridad, en colaboración con la academia y la industria, para generar nuevas soluciones y enfoques que mejoren la capacidad del CSIRT-CR para enfrentar incidentes y proteger los sistemas de información. 3.8.6. Desarrollar un modelo de financiamiento a largo plazo para la Agencia Nacional de Ciberseguridad que garantice la asignación de recursos financieros suficientes y sostenibles en el tiempo, permitiendo la contratación de personal capacitado, la adopción de tecnologías de vanguardia y la realización de actividades de capacitación, investigación y colaboración con otras organizaciones. Este modelo podría incluir fuentes de financiamiento diversas, como partidas presupuestarias específicas, contribuciones del sector privado y organismos internacionales, así como la generación de ingresos a través de la prestación de servicios especializados en ciberseguridad a terceros. 3.8.7. Revisar y actualizar la legislación y regulaciones pertinentes para definir de manera explícita el mandato legal, funciones y responsabilidades del CSIRT-CR en materia de ciberseguridad. Asegurar que el alcance de su actuación, sus competencias y sus obligaciones estén claramente establecidos en el marco legal y regulatorio. Además, promover la difusión y comprensión de este mandato entre los actores relevantes, tanto dentro como fuera del CSIRT, mediante campañas de comunicación, talleres y capacitaciones, para garantizar una colaboración efectiva y el cumplimiento de las responsabilidades asignadas en la gestión de incidentes de ciberseguridad.

OBJETIVO ESTRATÉGICO 4: Cultura cibernética y sociedad.

El Objetivo Estratégico 4 se centra en la promoción de una Cultura Cibernética en la sociedad, fomentando la concienciación, educación y responsabilidad en el uso de tecnologías digitales entre ciudadanos, empresas y entidades de gobierno. Este enfoque busca que los usuarios adopten buenas prácticas de ciberseguridad y se conviertan en actores activos en la protección de sus propios datos e información, contribuyendo así a un entorno digital más seguro y resiliente para todos.

OBJETIVO ESPECÍFICO 4.1	
4.1.	**Fomentar la alfabetización digital**, asegurar que todos los ciudadanos tengan acceso a educación y capacitación en habilidades digitales básicas y avanzadas.
Líneas de acción	
4.1.1.	Implementar programas de capacitación en habilidades digitales en comunidades.
4.1.2.	Establecer alianzas con empresas de tecnología para ofrecer cursos y talleres gratuitos o de bajo costo en habilidades digitales.
4.1.3.	Incluir de forma obligatoria en las instituciones públicas el curso de ciberseguridad provisto por el MICITT, el cual debe realizarse una vez al año.

OBJETIVO ESPECÍFICO 4.2	
4.2.	Fomentar la **colaboración entre los diferentes actores**, impulsar alianzas entre el gobierno, la industria, la academia y la sociedad civil para abordar desafíos y oportunidades relacionados con la cultura cibernética.
Líneas de acción	
4.2.1.	Organizar eventos y foros de discusión para fomentar el intercambio de ideas y experiencias entre los diversos sectores involucrados.
4.2.2.	Crear plataformas y mecanismos de colaboración para facilitar la cooperación en proyectos de investigación y desarrollo.

OBJETIVO ESPECÍFICO 4.3	
4.3.	**Apoyar la investigación y la innovación en tecnologías digitales**, invertir en investigación y desarrollo de tecnologías emergentes y aplicaciones que puedan mejorar la vida de las personas y contribuir al bienestar social.

Líneas de acción
4.3.1. Establecer programas de financiamiento para proyectos de investigación en tecnologías emergentes y aplicaciones con impacto social. 4.3.2. Crear incubadoras y aceleradoras para apoyar a emprendedores y startups en el desarrollo de soluciones tecnológicas innovadoras.

OBJETIVO ESPECÍFICO 4.4
4.4. Desarrollar una **conciencia de seguridad cibernética**, crear programas de concientización y educación en seguridad cibernética para proteger a los usuarios y las infraestructuras críticas.
Líneas de acción
4.4.1. Implementar campañas de concientización sobre riesgos cibernéticos y buenas prácticas en la protección de datos personales y sistemas de información.

OBJETIVO ESPECÍFICO 4.5
4.5. Abordar los **desafíos de las redes sociales y la desinformación**, implementar estrategias para combatir la proliferación de noticias falsas y desinformación, promoviendo la verificación de datos y la educación mediática.
Líneas de acción
4.5.1. Proporcionar programas de capacitación y recursos a la sociedad para ayudar a identificar noticias falsas y contenido malicioso, así como educación sobre seguridad en línea y privacidad. 4.5.2. Establecer programas de educación mediática y alfabetización en redes sociales para desarrollar habilidades críticas en los usuarios.

OBJETIVO ESPECÍFICO 4.6
4.6. Potenciar la **creación y difusión de contenidos culturales digitales**, apoyar a creadores y artistas en el desarrollo y difusión de contenidos culturales digitales, fomentar el acceso a la cultura y el patrimonio digital.
Líneas de acción
4.6.1. Crear plataformas y aplicaciones para la promoción y distribución de contenidos culturales digitales. 4.6.2. Establecer programas de financiamiento y apoyo para proyectos de digitalización y conservación del patrimonio cultural.

OBJETIVO ESTRATÉGICO 5: Formación, capacitación, y habilidades de seguridad cibernética.

El Objetivo Estratégico 5 se enfoca en la Formación, Capacitación y Habilidades en Seguridad Cibernética, buscando desarrollar y fortalecer el conocimiento y las competencias necesarias en el ámbito de la ciberseguridad para individuos, empresas y entidades de gobierno. Este objetivo promueve la creación de programas educativos y de capacitación que permitan enfrentar eficazmente los desafíos y amenazas en el entorno digital, potenciando así la seguridad y resiliencia del ciberespacio.

OBJETIVO ESPECÍFICO 5.1	
5.1.	Desarrollar **programas de educación y formación en ciberseguridad** para diferentes niveles educativos y profesionales.
Líneas de acción	
5.1.1.	Integrar módulos de ciberseguridad en currículos escolares y universitarios para fomentar el aprendizaje temprano de habilidades básicas en seguridad digital.
5.1.2.	Establecer cursos de especialización y certificaciones en ciberseguridad para profesionales que deseen mejorar sus conocimientos y habilidades en el campo.
5.1.3.	Integrar la enseñanza de seguridad cibernética en programas educativos específicos a nivel escolar y universitario.

OBJETIVO ESPECÍFICO 5.2	
5.2.	**Fomentar la colaboración** entre la academia, la industria y el gobierno en el desarrollo de programas de formación en ciberseguridad.
Líneas de acción	
5.2.1.	Crear alianzas entre instituciones educativas, empresas del sector tecnológico y entidades gubernamentales para desarrollar programas de formación adaptados a las necesidades del mercado laboral y las tendencias en ciberseguridad.
5.2.2.	Organizar eventos, conferencias y talleres en ciberseguridad para promover el intercambio de conocimientos, experiencias y buenas prácticas entre los diferentes actores involucrados.

OBJETIVO ESPECÍFICO 5.3
5.3. Incrementar la **concienciación en ciberseguridad y la adopción de buenas prácticas** entre los usuarios de tecnologías digitales.
Líneas de acción
5.3.1. Implementar campañas de comunicación y concienciación en ciberseguridad dirigidas al público en general, abordando temas como la protección de datos personales, la prevención del fraude en línea y la detección de phishing. 5.3.2. Desarrollar herramientas y recursos educativos en línea, como tutoriales, videos y guías, que permitan a los usuarios adquirir habilidades en ciberseguridad y aplicar buenas prácticas en su vida cotidiana. 5.3.3. Fomentar la cooperación entre los diversos protagonistas estratégicos de la nación con el propósito de expandir la divulgación en numerosos canales de comunicación masiva, buscando impulsar una agenda constante de concienciación y sensibilización. 5.3.4. Ampliar el número de eventos de concientización con enfoques específicos como el ciberbullying, grooming, noticias falsas, privacidad y protección de datos personales, retos virales, seguridad de la información, entre otros. 5.3.5. Desarrollar e implementar programas educativos y de concienciación en ciberseguridad en escuelas y centros de enseñanza, abarcando temas como el uso seguro y responsable de las tecnologías digitales, la protección de datos personales, la prevención del ciberacoso y el reconocimiento de amenazas en línea. 5.3.6. Crear y difundir materiales didácticos y recursos en línea apropiados para la edad, que incluyan juegos, videos, aplicaciones y guías que ayuden a los niños y adolescentes a aprender sobre ciberseguridad de manera interactiva y entretenida.

OBJETIVO ESPECÍFICO 5.4
5.4. Incorporar de forma sostenible la **ciberseguridad en el sistema educativo** y potenciar la academia a nivel universitario para crear habilidades y fortalecerlas en materia de ciberseguridad.
Líneas de acción
5.4.1. Adoptar e incorporar políticas para incentivar a estudiantes y profesionales a desarrollar una carrera profesional en el ámbito de la ciberseguridad. 5.4.2. Realizar programas de becas o de préstamos estudiantiles, pasantías para generar oportunidades de crecimiento y desarrollo a estudiantes en materia de ciberseguridad.

OBJETIVO ESTRATÉGICO 6: Marcos Legales y Regulatorios.

El Objetivo Estratégico 6 aborda los Marcos Legales y Regulatorios en ciberseguridad, enfatizando la importancia de establecer una base normativa sólida y actualizada que

permita prevenir, sancionar y gestionar de manera efectiva los delitos y amenazas cibernéticas. Este enfoque promueve la adaptación y armonización de las leyes y regulaciones a nivel nacional e internacional, garantizando al mismo tiempo el respeto de los derechos fundamentales y las libertades de los usuarios en el entorno digital.

OBJETIVO ESPECÍFICO 6.1
6.1. **Fomento de la transparencia y la participación ciudadana** en la elaboración de normativas.
Líneas de acción
6.1.1. Desarrollo de plataformas digitales para facilitar la consulta pública y la participación ciudadana en la formulación de nuevas leyes y regulaciones. 6.1.2. Implementación de campañas de concientización y educación para mejorar la comprensión pública de los procesos legislativos y regulatorios sobre ciberseguridad 6.1.3. Establecimiento de mecanismos para recibir retroalimentación y propuestas de la sociedad civil y del sector privado en la elaboración de normativas.

OBJETIVO ESTRATÉGICO 7: Fomento de Cooperación Internacional.

El Objetivo Estratégico 7 se centra en el Fomento de la Cooperación Internacional, destacando la relevancia de un enfoque conjunto y coordinado entre naciones para enfrentar los desafíos y amenazas en ciberseguridad. Esta meta promueve la colaboración y el intercambio de información, conocimientos y recursos entre países y organizaciones internacionales, con el fin de fortalecer la capacidad para prevenir, detectar y responder a incidentes cibernéticos y proteger a los usuarios en el entorno digital.

OBJETIVO ESPECÍFICO 7.1
7.1. Establecer **acuerdos y alianzas internacionales** en materia de ciberseguridad.
Líneas de acción

7.1.1. Participar en foros, conferencias y eventos internacionales para fomentar el diálogo y la cooperación en temas de ciberseguridad.
7.1.2. Firmar acuerdos bilaterales y multilaterales con otros países para establecer mecanismos de colaboración en la prevención y respuesta a incidentes de ciberseguridad.
7.1.3. Unirse a organizaciones y redes internacionales de ciberseguridad para compartir información, recursos y buenas prácticas.

OBJETIVO ESPECÍFICO 7.2
7.2. Cooperar en la **lucha contra el cibercrimen y la ciberdelincuencia** a nivel global.
Líneas de acción
7.2.1. Establecer mecanismos de cooperación en la investigación y persecución de delitos cibernéticos con organismos de seguridad y justicia internacionales. 7.2.2. Intercambiar información sobre ciber amenazas, vulnerabilidades y ataques con países aliados para mejorar la capacidad de prevención y respuesta ante estos incidentes. 7.2.3. Participar en operaciones conjuntas y colaborativas para desmantelar redes de cibercriminales y proteger a las víctimas de ciberdelitos.

OBJETIVO ESPECÍFICO 7.3
7.3. Impulsar la **armonización de políticas, regulaciones y estándares** en ciberseguridad a nivel internacional.
Líneas de acción
7.3.1. Participar en la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio seguro y confiable. 7.3.2. Adaptar las leyes y regulaciones nacionales a los estándares internacionales de ciberseguridad, facilitando así la cooperación y el cumplimiento de las normativas entre países. 7.3.3. Compartir experiencias y lecciones aprendidas en la implementación de políticas y marcos regulatorios de ciberseguridad con otros países y organizaciones internacionales.

OBJETIVO ESPECÍFICO 7.4
7.4. Fomentar la **cooperación en el desarrollo y transferencia de tecnologías y conocimientos** en ciberseguridad.

Líneas de acción
7.4.1. Establecer acuerdos y proyectos conjuntos de investigación y desarrollo en ciberseguridad con instituciones académicas y empresas internacionales. 7.4.2. Facilitar la transferencia de tecnologías y conocimientos en ciberseguridad mediante programas de formación, intercambio de expertos y colaboración entre centros de investigación. 7.4.3. Apoyar iniciativas y programas internacionales de desarrollo y asistencia en ciberseguridad, especialmente en países en desarrollo y economías emergentes.

OBJETIVO ESPECÍFICO 7.5
7.5 Promoción de la **cooperación internacional en el ámbito regulatorio**.
Líneas de acción
7.5.1 Establecimiento de alianzas y acuerdos con organismos internacionales y entidades extranjeras para compartir experiencias y buenas prácticas en materia de regulación. 7.5.2 Participación activa en foros internacionales y regionales sobre políticas y normativas, con el fin de promover la armonización y la cooperación transfronteriza. 7.5.3 Fomento de la colaboración entre entidades nacionales y extranjeras en la aplicación y supervisión de normativas internacionales y regionales en materia de marcos legales y regulatorios.

EJES TRANSVERSALES

Los ejes transversales de la estrategia de ciberseguridad representan elementos clave que atraviesan y refuerzan todos los objetivos estratégicos, asegurando un enfoque integral y coherente para abordar los desafíos en el entorno digital.

Ilustración 6 - Ejes Transversales

Fuente: Elaboración propia, 2023.

1. Alianza público-privada

1. Identificar los objetivos que se quieren lograr mediante la cooperación, como por ejemplo el intercambio de información, la colaboración en investigaciones o el fortalecimiento de capacidades técnicas.
2. Identificar a los socios de cooperación que se ajusten a los objetivos definidos, considerando su experiencia, recursos y alcance geográfico.
3. Definir las áreas específicas de cooperación, como la promoción de buenas prácticas de ciberseguridad, el fortalecimiento de la respuesta a incidentes, la capacitación y el intercambio de información.
4. Establecer los marcos de cooperación necesarios para formalizar las relaciones con los sectores, incluyendo acuerdos de intercambio de información, protocolos de comunicación y otros aspectos relevantes.
5. Planificación de proyectos conjuntos: Planificar proyectos conjuntos para abordar las áreas específicas de cooperación definidas, con objetivos claros, plazos y responsabilidades asignadas.

6. Implementación de proyectos: Implementar los proyectos planificados, asegurando una buena coordinación y comunicación entre los socios, y monitoreando y evaluando los resultados obtenidos.
7. Evaluación y mejora continua: Realizar evaluaciones periódicas de la cooperación, identificando fortalezas y oportunidades de mejora, y actualizando los planes y proyectos en consecuencia.

2. Fortalecimiento del marco legal en ciberseguridad y TIC

Es importante analizar e identificar necesidades de adaptación y/o armonización del marco legal y regulatorio relacionadas con la ciberseguridad en el país, que permita promover un espacio cibernético seguro que garanticen el bienestar socioeconómico de la ciudadanía. Esto también se debe hacer considerando los compromisos adquiridos en instrumentos internacionales como el Convenio de Budapest.

3. Convenios internacionales

La naturaleza transfronteriza de las tecnologías digitales hace que la temática de la ciberseguridad deba ser atendida desde una perspectiva global 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 conjuntas que ayuden a incrementar la confianza y la seguridad del ciberespacio. Por tanto, la construcción articulada de alianzas, acuerdos y estrechamiento de relaciones con organizaciones nacionales e internacionales será un elemento clave dentro de esta estrategia.

4. Colaboración y coordinación interinstitucional

La ciberseguridad es un tema que abarca a muchas agencias gubernamentales y sectores privados, por lo que es importante establecer mecanismos de colaboración y coordinación para garantizar una respuesta efectiva en caso de incidentes.

Establecer convenios que garanticen el acceso a recursos adicionales, fomentar la colaboración, garantizar una respuesta rápida y coordinada en situaciones de emergencia, y que ayuden a cumplir con las leyes y regulaciones de ciberseguridad. En este se pueden establecer protocolos de comunicación interinstitucionales,

Las entidades gubernamentales pueden proporcionar orientación y asesoramiento sobre las mejores prácticas y los requisitos legales para proteger la información y garantizar la privacidad de los datos.

Capítulo 8 – Reflexiones finales

Costa Rica continuará avanzando en su desarrollo y empleará las oportunidades de optimización para reforzar su estrategia en la lucha contra los ataques informáticos, fomentando de esta manera una sociedad y economía estable y segura al definir áreas clave para la implementación de su Estrategia Nacional de Ciberseguridad. La inversión en soluciones de Tecnologías de la Información y Comunicación (TIC) no solo mejorará la calidad de vida de los ciudadanos, sino que también cambiará radicalmente nuestra percepción del mundo y nuestras interacciones.

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

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

Glosario

Este apartado resume los principales conceptos para la elaboración del ENC.

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

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

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

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

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

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

Ciberseguridad: Es la práctica de proteger sistemas críticos e información confidencial de ataques digitales, que involucran tecnología, personas y procesos

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

Clúster: son grupos de servidores que se gestionan juntos y participan en la gestión de carga de trabajo. Un clúster puede contener nodos o servidores de aplicaciones individuales. (IBM,2022)

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

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

Incidentes: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

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

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

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

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

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

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

Transformación digital: La transformación digital es el proceso de sustitución total de métodos manuales, tradicionales y heredados de hacer negocios con las últimas

alternativas digitales. Este tipo de reinvención toca todos los aspectos de un negocio, no solo la tecnología.

Referencias

Calzadilla, C. M. (2023, January 9). *Estos son los 7 tipos de amenazas cibernéticas mas frecuentes*. Mundo Posgrado. Recuperado de https://www.mundoposgrado.com/amenazas-ciberneticas-mas-frecuentes/

Cybercrime to cost the world $10.5 trillion annually by 2025. (2020, November 13). Cybercrime Magazine. Recuperado de https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Decreto Ejecutivo 37052-MICITT Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR. (2012). Sistema Costarricense de Información Jurídica. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TCparam1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC

Decreto Ejecutivo Nº 31659-MP-RE-SP-H-J-MOPT de 2004. (2004). Sistema Costarricense de Información Jurídica Crea la Comisión Interinstitucional sobre Terrorismo. Recuperado de https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=52453&nValor3=56927&strTipM=TC

Decreto Ejecutivo Nº 36274 de 2010 Creación de la Comisión Nacional de Seguridad en Línea. (2010). Sistema Costarricense de Información Jurídica. Recuperado de www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=69239&nValor3=83075&strTipM=TC

ENISA threat landscape 2021. (2021). ENISA. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Escuela Permanente de Pensamiento Universitario de la Universidad Nacional de Colombia: Escuela Permanente de Pensamiento Universitario. Recuperado de https://pensamiento.unal.edu.co/fileadmin/recursos/focos/desarrollo-sostenible/Simposio_4a_Revolucion/8_Francisco_javier_valencia/9_Francisco_Javier_Valencia.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2017). *Estrategia Nacional de Ciberseguridad Costa Rica*. Recuperado de https://www.micitt.go.cr/wp-content/uploads/2022/05/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-Oficial.pdf

IBM documentation. (n.d.). IBM - United States. Recuperado de https://www.ibm.com/docs/es/was-zos/9.0.5?topic=servers-introduction-clusters

INCIBE (2021) Glosario de términos de ciberseguridad. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ITU publications. (2021). The UN specialized agency for ICTs. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

ITU. (2020). Global Cybersecurity Index. Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Keeping a close watch: Trend micro specialized cybersecurity report for Latin America and the Caribbean. (2022). #1 in Cloud Security & Endpoint Cybersecurity | Trend Micro. Recuperado de https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/trend-micro-specialized-cybersecurity-report-for-latin-america-and-the-caribbean

Ley 8968 de 2011 de Protección de la Persona frente al tratamiento de sus datos personales. (2011). Sistema Costarricense de Información. Recuperado de www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

Ley 4573 de 2013 Código Penal. (2013). Sistema Costarricense de Información Jurídica. Recuperado de https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=96389&strTipM=TC

Ley 7169 de 1990 Promoción Desarrollo Científico y Tecnológico y Creación del MICIT (Ministerio de Ciencia y Tecnología). (1990). Sistema Costarricense de Información Jurídica. Recuperado de www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=11908&nValor3=91174&strTipM=TC

Ley 8934 de 2011 relativa a la protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. (2011). Sistema Costarricense de Información Jurídica. Recuperado de https://www.pgrweb.go.cr/

ManageEngine. (n.d.). *Escaneo de vulnerabilidades | Herramientas de escaneo de vulnerabilidades Y análisis de vulnerabilidad - ManageEngine vulnerability manager plus*. ManageEngine - IT Operations and Service Management Software. Recuperado de https://www.manageengine.com/latam/vulnerability-management/analisis-de-vulnerabilidades.html#:~:text=El%20an%C3%A1lisis%20de%20vulnerabilidades%20es,errores%20de%20configuraci%C3%B3n%20del%20sistema

National Cybersecurity index (NCSI). 2022. https://ncsi.ega.ee/country/cr/

Justia. (2022, October 13). *Preguntas Y Respuestas Sobre Delitos Informáticos*. Recuperado de https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/#q2

EcuRed. (n.d.). *Sistemas de notificaciones Y alertas*. https://www.ecured.cu/Sistemas_de_notificaciones_y_alertas

Revista Seguridad 360. (2022). *El Modelo de Madurez de la Capacidad de Ciberseguridad. Recuperado de https://revistaseguridad360.com/noticias/capacidad-de-ciberseguridad/*

¿Qué es la transformación digital? | Glosario. (n.d.). Recuperado de https://www.hpe.com/es/es/what-is/digital-transformation.html

¿Qué es un ataque cibernético? (n.d.). IBM - United States. Recuperado de https://www.ibm.com/cl-es/topics/cyber-attack