MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

COSTA RICA
GOBIERNO DE LA REPÚBLICA

Estrategia Nacional de Ciberseguridad de Costa Rica

Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017

350
E82e

Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).

Estrategia Nacional de Ciberseguridad Costa Rica 2017. – San José, C. R.: MICITT, 2017.

ISBN: 978-9968-732-52-9

1. CIBERSEGURIDAD-POLÍTICA GUBERNAMENTAL-COSTA RICA 2. SEGURIDAD EN COMPUTADORAS 3. REDES DE COMPUTADORAS-MEDIDAS DE SEGURIDAD 4.TECNOLOGÍA DE INFORMACIÓN-MEDIDAS DE SEGURIDAD

Tabla de contenidos

Índice de figuras

Índice de gráficos

Índice de cuadros

Siglas y acrónimos

AMERIPOL	*Comunidad de Policías de América*
BCCR	*Banco Central de Costa Rica*
BI	*Inteligencia de Negocios (del inglés Business Intelligence)*
BID	*Banco Interamericano de Desarrollo*
CENFOTEC	*Centro de Formación en Tecnologías de Información y Comunicación*
CGR	*Contraloría General de la República*
CII Infrastructures)	*Infraestructuras Críticas de Información (Critical Information*
COBIT	*Objetivos de Control para Tecnologías de la Información y Relacionadas (Control Objectives for Information and Related Technologies)*
CONARE	*Consejo Nacional de Rectores*
CONESUP	*Consejo Nacional de Enseñanza Superior Universitaria Privada*
CONICIT	*Consejo Nacional para Investigaciones Científicas y Tecnológicas*
CRIX	*Punto de Intercambio de Internet de Costa Rica*
DB	*Base de Datos (del inglés Database)*
DBA	*Administrador de Bases de Datos (del inglés Database Administrator)*
DCFD	*Dirección de Certificadores de Firma Digital*
DDoS Service)	*Denegación Distribuida de Servicio (del inglés Distributed Denial of*
FEM	*Foro Económico Mundial*
FISMA	*Acta Federal de Gestión de Seguridad de la Información*

	(Federal Information Security Management Act)
FONABE	*Fondo Nacional de Becas*
ICE	*Instituto Costarricense de Electricidad*
ICTA	*Autoridad de TIC (Information and Communication Technologies Authority)*
IEC	*Comisión Internacional Electrotécnica (International Electrotechnical Commission)*
IED	*Inversión Extranjera Directa*
IMEI	*Identidad Internacional de Equipo Móvil*
	(International Mobile Equipment Identity)
INTERPOL	*International Police*
ISO	*Organización Internacional para la Estandarización*
ITCR	*Instituto Tecnológico de Costa Rica*
ITU	*Unión Internacional de las Telecomunicaciones*
	(International Telecommunication Unit)
IXP	*Punto de Intercambio de Internet (Internet eXchange Point)*
MEIC	*Ministerio de Economía, Industria y Comercio*
MEP	*Ministerio de Educación Pública*
MICITT	*Ministerio de Ciencia, Tecnología y Telecomunicaciones*
MRREE	*Ministerio de Relaciones Exteriores y Culto de Costa Rica*
NERC	*North American Electric Reliability Corporation*
NIST	*Instituto Nacional de Estándares y Tecnología de EE.UU. (National Institute of Standards and Technology)*

NRI	*Índice de Preparación para la Red (Networked Readiness Index)*
OCDE	*Organización para la Cooperación y el Desarrollo Económico*
OEA	*Organización de los Estados Americanos*
OECD	*Organization for Economic Co-operation and Development*
ONU	*Organización de las Naciones Unidas*
OPES	*Oficina de Planificación de la Educación Superior*
PGR	*Procuraduría General de la República*
RPKI	*Infraestructura de Clave Pública de Recursos (Resource Public Key Infrastructure)*
SCADA	*Sistemas de Control de Supervisión y Adquisición de Datos*
SCI	*Sistemas de Control Industrial*
SCIJ	*Sistema Costarricense de Información Jurídica*
SEI	*Institución de Ingeniería de Software (Software Engineering Institute)*
SINAES	*Sistema Nacional de Acreditación de la Educación Superior*
SUTEL	*Superintendencia de Telecomunicaciones*
TIC	*Tecnologías de Información y Comunicación*
TSE	*Tribunal Supremo de Elecciones*
UIT	*Unión Internacional de Telecomunicaciones*
UNESCO	*Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura*
XML	*Lenguaje de Marcado Extensible (Extensible Markup Language)*

Resumen Ejecutivo

El concepto de Ciberseguridad ha evolucionado desde los albores de los primeros computadores a hoy día, el mayor reto es asegurar los datos, sistemas y procesos que se guardan en éstos y que se comparten a través de redes de datos, como la Internet.

Ya en 1961 aparecen los primeros artículos sobre la creación de una red de datos global, y para 1980 se hace la presentación de la red Internet, basado en dos protocolos IP (Internet Protocol) y TCP (Transmission Control Protocol). Siendo esto el inicio de la red como tal, agregando tiempo después los servicios de la WWW (World Wide Web - 1991).

Cada adelanto tecnológico implica un reto en seguridad, desde evitar el robo de datos de los computadores, acción aplicada directamente a ellos, o bien con las redes de datos globales, evitar los accesos no autorizados y maliciosos con el fin de extraer datos y utilizarlos para fines no éticos.

El mundo no se detiene, en la industria tecnológica, la innovación y el descubrimiento constante son la clave para la supervivencia y el crecimiento de un pueblo.

Los gobiernos se ven afectados por los ataques de diversa índole e intención, desde el simple juego de un joven experimentando y retando al sistema, hasta la clara intención de dañar los sistemas e infraestructura de los países.

Hoy día somos una aldea, como tal enfrentamos retos poderosos, desde la perspectiva del aseguramiento de los datos de los habitantes del mundo, hasta la protección de los valores consagrados en la declaración universal de los derechos humanos.

La inteligencia del ser humano siempre es proactiva, busca nuevas soluciones, busca nuevos caminos; esto no es ajeno a los hackers que desde su perspectiva es un reto vulnerar las diferentes instancias a fin de obtener un logro personal, una gratificación económica o bien coadyuvar con los gobiernos y empresas en el espionaje de las instalaciones e infraestructuras.

Pero estos ataques deben ser repelidos, con inteligencia y acciones coordinadas a fin de que la sociedad, como la estamos estructurando hoy día, no sea presa de pocos, que por diversión o conciencia decidan vulnerarla.

Es por esa razón que esta estrategia y las iniciativas de tener un mundo más seguro, tendrán en el futuro grandes beneficios, pues nuestros pueblos crecerán en confianza y aceptación de las diversas formas de pensamiento y acción, importantes para tener un concierto de las naciones.

En nuestro país, coordinar entre los diversos sectores, buscando soluciones a problemas novedosos es del concurso de todos. Este documento constituye apenas el primer paso en esa búsqueda del saber, es una estrategia que como tal nos marca la pauta a seguir de ahora en adelante en materia de ciberseguridad en nuestro país, vislumbrando principalmente los retos que debemos vencer.

Capítulo 1- Introducción

A nivel mundial se reconoce que las tecnologías digitales y en especial las tecnologías de la información y la comunicación (TIC) son un catalizador para el desarrollo económico, social y cultural, dado que facilitan el acceso a incalculables recursos y que además de la comunicación, promueven la innovación, la eficiencia, la transparencia, y la prosperidad económica de los países.

Costa Rica, consciente de ello, ha apostado a una fuerte promoción del uso de las TIC, para impulsar el desarrollo nacional, fortaleciendo el marco normativo vigente, en aras de favorecer el desarrollo y uso de los servicios de telecomunicaciones/TIC dentro del marco de la sociedad de la información y el conocimiento y como apoyo a sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno electrónico.

Asimismo, la política pública se ha dirigido a impulsar la incorporación de las tecnologías digitales, tanto en los servicios públicos como privados, mejorando la eficiencia de quienes prestan estos servicios y buscando un menor costo para quien los recibe. Aunado a ello se impulsa la inversión en el sector de las telecomunicaciones, mediante un marco jurídico que establece dentro de sus principios garantizar la transparencia, la no discriminación, la equidad, la seguridad jurídica, la neutralidad tecnológica, y la formación de recurso humano en el área de las TIC.

Los resultados de estas acciones se reflejan en la mejora de los indicadores nacionales de acceso y uso de las tecnologías. Por otra parte, en el mapa internacional, Costa Rica continúa en ascenso dentro de las clasificaciones internacionales con base a su desarrollo. Según el Foro Económico Mundial (WEF por sus siglas en inglés) en su informe 2014-2015, el país muestra un perfil muy estable a partir de sus activos tradicionales a pesar de que sufre de algunas debilidades persistentes. Se ha informado que, en términos de fortalezas, el país está bien posicionado para participar en una rápida transición hacia actividades basadas en el conocimiento. El país cuenta con uno de los mejores sistemas educativos de América Latina y el Caribe (en el puesto 21). Además, el informe señala que Costa Rica tiene una asimilación de las TIC alta (puesto 45) con una alta capacidad de ancho de banda de Internet internacional (puesto 36); muchas suscripciones de banda ancha móvil (puesto 20); una capacidad para innovar desarrollada (puesto 36) y un sólido acceso a la tecnología (puesto 39), gracias al papel crucial

que desempeñan la inversión extranjera directa (IED) y la transferencia de tecnología (puesto 5) en el país.[1]

Sin embargo, con los altos índices de conectividad a Internet y acceso de las TIC, así como la generación y almacenamiento masivo de datos sensibles, surgen riesgos y vulnerabilidades que exponen a las personas, al sector empresarial y al mismo gobierno. Los usuarios que acceden a la red con fines ilícitos han aprovechado esa realidad, y muestra de ello es el desarrollo de medios más sofisticados para esconder su identidad y enmascarar sus ataques cibernéticos, lo que dificulta su reconocimiento, así como la recolección oportuna de los elementos probatorios del delito, lo cual limita que se realice el debido proceso por parte de las autoridades correspondientes.

Las ventajas que ofrecen las tecnologías digitales como por ejemplo los servicios en la nube, también se encuentran a disposición de los atacantes, siendo que las nubes públicas no sólo representan blancos más vulnerables, también proporcionan virtualmente cómputo ilimitado y anónimo, y recursos de red para los ataques.

Por tanto, existe una evidente necesidad de desarrollar e implementar soluciones concretas a los riesgos y vulnerabilidades particulares de las TIC que además evolucionan a diario. Ante esa realidad y para poder responder de forma rápida y diligente, se requiere de la colaboración y la cooperación entre los diversos actores nacionales e internacionales.

Un paso decisivo para la explotación de las tecnologías digitales es definir una estrategia que incluya acciones relativas a la seguridad desde una perspectiva holística, que considere todos los elementos, incluidos la identificación de riesgos y amenazas que se puedan materializar y sus posibles mecanismos de prevención, la adecuada atención de incidentes y la implementación de los respectivos procesos correctivos.

La atención de los incidentes y ataques cibernéticos requiere de flexibilidad y rapidez en el desarrollo de una respuesta nacional articulada, considerando los marcos y procesos existentes. Por esta razón se han considerado una serie de elementos que se integran a la estrategia y que buscan aumentar la resiliencia cibernética, el desarrollo de los recursos humanos y tecnológicos necesarios, el fortalecimiento de equipos de respuesta especializados, la cooperación nacional e internacional que permita el intercambio de información y la investigación de los delitos

[1] *Reporte Global de Competitividad 2014-2015. Foro Económico Mundial. Disponible en: http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf*

cibernéticos, así como la protección de la libertad de expresión y la privacidad en la Internet como principio central de seguridad cibernética.

La Estrategia Nacional de Ciberseguridad plantea un esfuerzo conjunto y articulado entre todos los sectores del país, para así garantizar que los objetivos que se establezcan sean equilibrados, eficaces y acordes a la realidad nacional, definiendo los principios generales que marcarán la pauta en esta materia.

Capítulo 2 – Construcción de la estrategia

La seguridad cibernética requiere una visión holística y una atención multisectorial, por ello, en el proceso de construcción de esta estrategia, el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) contó con el apoyo técnico especializado de la Organización de los Estados Americanos (OEA) e hizo partícipes a representantes de los sectores interesados en aportar al desarrollo de esta materia en el país.

El proceso de construcción fue liderado por el MICITT, que a partir del mes de marzo de 2015 llevó a cabo tres mesas de discusión, orientadas por personal especializado de la OEA, cuatro talleres sectoriales y dos consultas en línea.

En estos encuentros, se utilizó una metodología participativa y abierta, con representantes de todos los sectores, a quienes se les realizaron presentaciones sobre la estructura de diseño utilizada por la OEA, así como propuestas de abordaje de la visión del MICITT, posteriormente, los participantes compartieron su visión y puntos de vista sobre los principios, objetivos y líneas de acción prioritarias que se incluirían en la estrategia acorde a la realidad de Costa Rica.

Con base en estas discusiones se extrajeron las recomendaciones de los participantes y se elaboró un borrador final, documento que se mostró en la última mesa de discusión y se puso a disposición de todos los convocados a los distintos talleres por espacio de 14 días, a partir del 21 de junio de 2016 y hasta el 04 de julio de 2016, para su revisión y recepción de comentarios y sugerencias.

Figura 1 Proceso de consulta multisectorial para la construcción de la estrategia

Fuente: Elaboración propia, 2016

Posterior a esta etapa, se incorporaron las observaciones de fondo y forma correspondientes con el fin de lograr un documento robusto y consensuado y se sometió a revisión por parte de los especialistas de la OEA.

Finalmente, el 05 de junio del 2017, a través del Diario Oficial La Gaceta N. 105 se sometió a Consulta Pública no vinculante, proceso del cual se obtuvo este documento.

Por el arduo y comprometido trabajo realizado, agradecemos a cada una de las personas que depositaron su vasto conocimiento al servicio de un instrumento que será la hoja de ruta en materia de Ciberseguridad para los próximos años.

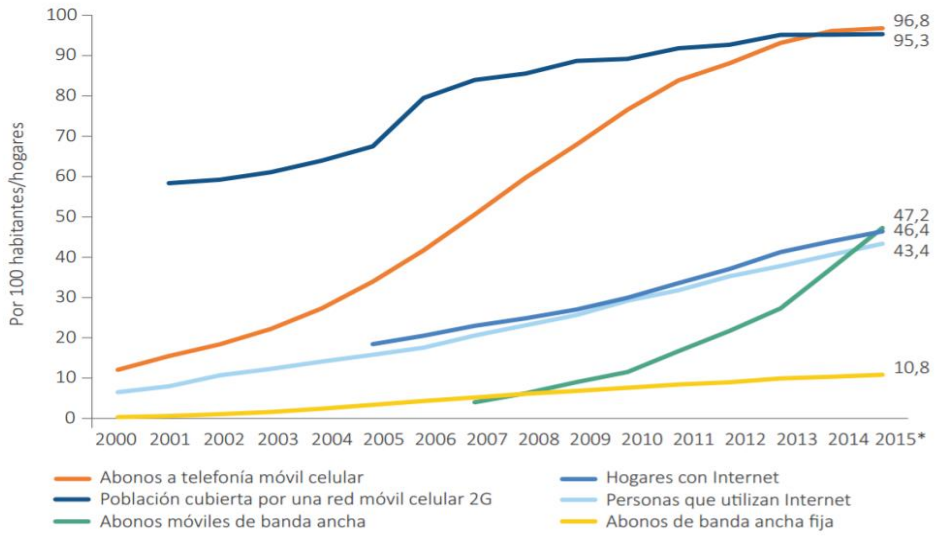
Capítulo 3 – Contexto actual

3.1.1 El impacto de las TIC en el desarrollo económico

El uso de Internet ha revolucionado tanto la forma de interacción entre las personas y de éstas con el mundo exterior. La conectividad resulta hoy día una prioridad para los países, ya que permite el acceso a una plataforma que facilita la colaboración, la innovación y promueve diferentes mecanismos para interactuar en los ámbitos económicos, políticos y sociales.

Según datos del Informe sobre Medición de la Sociedad de la Información 2015 de la Unión Internacional de Telecomunicaciones (UIT) "La proporción de la población mundial cubierta por las redes móviles y celulares es ahora de más del 95 %, mientras que el número de abonados a telefonía móvil celular se ha incrementado de 2.200 millones en 2005 a unos 7.100 millones en 2015".[2]

Gráfico 1 Cambios en las principales TIC a nivel mundial, 2000-2015*



**Estimaciones.*

Fuente: UIT. Tomado del Informe sobre Medición de la Sociedad de la Información 2015.

[2] *Informe sobre Medición de la Sociedad de la Información 2015. Unión Internacional de Telecomunicaciones. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2015-SUM-PDF-S.pdf. Página 1.*

El creciente uso de las telecomunicaciones y las TIC, ha ido paralelo a un aumento considerable de la exposición de los usuarios a riesgos y actividades delictivas relacionadas con la seguridad de los datos, así como la irrupción e interrupción de los equipos.

Según el Informe Ciberseguridad 2016 emitido por la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo, "…el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global"[3]. Entre tanto, el mismo informe indica que para América Latina y el Caribe, este tipo de delitos tiene un costo de alrededor de US$90.000 millones al año[4].

Por otra parte, en el Índice de Conectividad o por su nombre en inglés, Networked Readiness Index (NRI)[5] del Foro Económico Mundial del 2016, Costa Rica ocupa la posición 44 solamente superado por Chile (posición 38) y Uruguay (posición 43) de los países de América Latina.

Aunado a lo anterior, Costa Rica lidera las exportaciones de servicios de valor agregado en América Latina, lo cual incluye: telecomunicaciones, información y otros servicios. Lo anterior representa un 6.8% del PIB según estadísticas del año 2015, estando en segundo lugar Honduras (1.5% del PIB)[6].

De acuerdo con datos presentados en el Informe de Indicadores Nacionales Ciencia, Tecnología e Innovación Costa Rica 2014 "El peso de las exportaciones de bienes TIC, con respecto a las exportaciones de bienes totales del país, mostró que este sector es de suma importancia. En el período 2006- 2014, representó más del 41% y en el 2014, tuvo una participación de 56,6%, del total de exportaciones del país."[7]

---

[3] *BID-OEA. (2016). Informe Ciberseguridad 2016.*

[4] Idem.

[5] *Este índice mide "…la propensión de los países a aprovechar las oportunidades que ofrecen las tecnologías de información y comunicaciones. Se publica anualmente y busca entender mejor el impacto de las TIC en la competitividad de las naciones" Disponible en http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.1_2016.pdf*

[6] *Coalición Costarricense de Iniciativas de Desarrollo (CINDE) (2016). Invirtiendo en Costa Rica: Servicios. Costa Rica. CINDE: Costa Rica. Basado en datos del Banco Central de Costa Rica, del Fondo Monetario Internacional y Trademark.*

[7] *MICITT (2014). Informe Indicadores Nacionales Ciencia, Tecnología e Innovación. Disponible en http://cdn-s3.myvirtualpaper.com/i/intergraphicdesigns-micitt/indicadores-2014-vp/2016101901/upload/indicadores-2014-vp.pdf*

Cuadro 1 Participación de las exportaciones e importaciones del sector TIC respecto al total de exportaciones e importaciones del país, 2006-2014

	2006	2007	2008	2009	2010	2011	2012	2013	2014
Exportaciones TIC/ Total de exportaciones	41,1	42,6	41,9	45,3	47,1	49,2	52,3	54,6	56,6
Importaciones TIC/ Total de importaciones	30,5	26,4	24,6	27,6	25,7	28,2	25,3	29,6	31,3

Fuente: Cifras proyectadas con datos de la Balanza de Pagos 2006-2013, Banco Central de Costa Rica (BCCR).

Fuente: Extraído del Informe de Indicadores Nacionales Ciencia, Tecnología e Innovación Costa Rica 2014

El sector telecomunicaciones ha mostrado un gran dinamismo que ha repercutido en importantes beneficios para los usuarios y el país. Como puede observarse en el siguiente cuadro, tanto los ingresos totales, como el recurso humano empleado en el sector ha venido en aumento constante desde el año 2011.

Cuadro 2 Datos del sector telecomunicaciones 2011-2015

Indicador	2011	2012	2013	2014	2015
Datos agregados del sector					
Ingreso total (millones de colones)**	437.672	501.648	576.742	744.300	802.812
Ingreso total/PIB (porcentaje)	2,3%	2,4%	2,6%	3,1%	3,1%
Inversión total/PIB (porcentaje)	2,1%	2,4%	1,0%	1,0%	1,0%
Recurso humano empleado total	9.618	9.900	10.422	11.002	11.426
Recurso humano empleado total/Población económicamente activa total	0,4%	0,4%	0,5%	0,5%	0,5%

*Notas: ** Estas cifras no incluyen el ingreso asociado al servicio de televisión por suscripción.*
Fuente: Estadísticas del sector de telecomunicaciones 2015. SUTEL. Disponible en:
https://sutel.go.cr/sites/default/files/estadisticas_del_sector_telecomunicaciones_costa_rica_2015.pdf

Como se puede observar en el cuadro a continuación, esto viene aparejado de una adopción cada vez mayor del servicio de acceso a Internet por parte de los costarricenses, tanto de los servicios de Internet fijo como de Internet móvil.

Cuadro 3 Suscripciones al servicio de transferencia de datos 2011-2015

Indicador	2011	2012	2013	2014	2015
Transferencia de datos					
Suscripciones totales acceso a Internet	2.008.763	3.118.155	4.028.302	4.806.217	5.420.554
Suscripciones totales acceso a Internet fijo-alámbrico	414.384	439.043	474.433	503.347	545.813
Suscripciones totales acceso a Internet fijo-inalámbrico	5.398	8.904	10.450	12.493	12.843
Suscripciones totales acceso a Internet móvil	1.588.981	2.670.208	3.543.419	4.290.377	4.861.898
Suscripciones totales acceso a Internet fijo/100 habitantes	9%	10%	10%	11%	12%
Suscripciones totales acceso a Internet fijo/100 viviendas	32%	34%	36%	37%	39%
Suscripciones totales acceso a Internet móvil /100 habitantes	35%	57%	75%	90%	101%
Suscripciones totales acceso a Internet móvil /suscripciones totales telefonía móvil	38%	50%	50%	61%	65%
Cantidad total conexiones de líneas dedicadas	10.273	11.993	16.375	16.286	14.093

Fuente: Estadísticas del sector de telecomunicaciones 2015. SUTEL. Disponible en:
https://sutel.go.cr/sites/default/files/estadisticas_del_sector_telecomunicaciones_costa_rica_2015.pdf

Para el año 2015, los datos muestran que un 39% de las viviendas contaban con conexión fija a Internet y la penetración móvil alcanzó un 101% por lo tanto, es sumamente importante adoptar las medidas necesarias para que el país esté preparado ante posibles ataques y que los usuarios conozcan de los riesgos y acciones que deben tomar para proteger sus datos en el ciberespacio, especialmente porque el país viene haciendo esfuerzos por expandir las redes en todo el territorio y se espera que con el despliegue de las redes que se financian con los recursos del Fondo Nacional de Telecomunicaciones (FONATEL), toda la población cuente con acceso a las tecnologías.

Ante el inminente crecimiento de las redes de banda ancha y el uso y aprovechamiento de las TIC, se vuelve palpable la exposición de datos sensibles y el riesgo de las redes ante posibles ataques cibernéticos.

3.2 Las TIC y la ciberseguridad: perspectiva de la planificación nacional

Las Tecnologías de Información y Comunicación son consideradas herramientas invaluables para el desarrollo del país, lo cual se evidencia en el incremento de los índices de acceso, uso y apropiación de estas. En ese sentido, el Estado costarricense ha procurado incentivar la incorporación de las TIC y la conectividad a Internet en todos los ámbitos del quehacer nacional, lo cual se ve reflejado en la planeación nacional a través de sus instrumentos de planificación. Por lo anterior, resulta relevante hacer mención al contenido de algunos de estos instrumentos sobre estas materias.

3.2.1 Documento "Costa Rica 2030: Objetivos de Desarrollo Nacional"

El documento plantea los objetivos de desarrollo del país con una visión a largo plazo, a la vez que promueve la colaboración intersectorial y el intercambio de información. En el mismo se establece que el desarrollo de las TIC desempeña un papel de apoyo en diversas dimensiones, incluyendo el crecimiento económico, la inversión social y cultural, y la infraestructura. En la "Dimensión Económica" incluye el tema de infraestructura al indicar que "…la infraestructura (carreteras, puertos, aeropuertos, escuelas, colegios, clínicas, hospitales, EBAIS, servicios de electricidad, provisión de agua, manejo de desechos sólidos, servicios de telecomunicaciones, infraestructura comunitaria, etc.) constituye un soporte y una condición ineludible para lograr tasas de crecimiento elevadas en forma sostenida"[8]. Entre los objetivos destaca: "Asegurar telecomunicaciones con diversidad de servicios, cobertura a todos los poblados del país". Este objetivo busca garantizar el acceso universal a la Internet a través de aumentos incrementales en la conectividad a nivel nacional[9].

3.2.2 Plan Nacional de Desarrollo 2014-2018 "Alberto Cañas Escalante"

Este plan enuncia las prioridades, objetivos, programas y proyectos que la Administración Solís Rivera, ha trazado sobre tres pilares, a saber: 1) impulsar el crecimiento económico y generar

[8] *Ministerio de Planificación Nacional y Política Económica (MIDEPLAN). (2013). Costa Rica 2030: Objetivo de Desarrollo Nacional. San José: MIDEPLAN. P. 13. Recuperado de, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf*

[9] *Idem, p. 30.*

empleo de calidad; 2) el combate a la pobreza y reducción de la desigualdad; y 3) un gobierno abierto, transparente, eficiente, en lucha frontal contra la corrupción. En este plan las telecomunicaciones son vistas como un servicio básico para el combate a la pobreza y desarrolla una propuesta estratégica sectorial para el sector Ciencia, Tecnología y Telecomunicaciones que plantea "…el desarrollo de proyectos que buscan establecer un ordenamiento a través de instrumentos y normativas jurídicas para potenciar su desempeño, promoviendo la interacción entre los diferentes actores, creando un espacio físico productor y multiplicador de las capacidades científicas tecnológicas de las personas"[10]. Este Plan resalta la importancia de la Ciberseguridad mediante el Programa para impulsar el Gobierno Electrónico.

3.2.3 Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 "Costa Rica: Una sociedad conectada"

Este plan propone concretizar los proyectos de acceso universal, servicio universal y solidaridad, además de facilitar a nivel comercial y residencial el incremento de la calidad de los servicios de telecomunicaciones que se brindan al público, incluyendo la ampliación de la oferta de los servicios asequibles e innovadores. El plan está articulado en tres grandes pilares a saber: Inclusión Digital, Gobierno Electrónico y Transparente y Economía Digital. Su máxima aspiración es: "Transformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones; de forma segura, responsable y productiva"[11].

Los temas citados se trazan a lo largo de tres grandes aspiraciones:

1. Concretizar proyectos de acceso universal, servicio universal y solidaridad de las Telecomunicaciones/TIC.
2. Crear un entorno habilitador que permita la innovación de la radiodifusión sonora y televisiva hacia su digitalización.
3. Construir participativamente las bases del Modelo de Ciudades Digitales a través de un gobierno electrónico cercano.

---

[10] *Ministerio de Planificación y Política Económica (MIDEPLAN). (2013). Plan Nacional de Desarrollo 2014-2018 "Alberto Cañas Escalante". San José: MIDEPLAN. p. 438. Recuperado el 17 de agosto de 2016 de, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/cd1da1b4-868b-4f6f-bdf8-b2dee0525b76/PND%202015-2018%20Alberto%20Ca%C3%B1as%20Escalante%20WEB.pdf*

[11] *Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. Recuperado el 17 de agosto de 2016 de, https://www.micit.go.cr/images/Telecomunicaciones/pndt/PNDT-2015-2021.pdf*

Al igual que en el PND, se destaca la Ciberseguridad como un tema fundamental dentro del pilar de Gobierno Electrónico y Transparente. En este pilar se busca que el país cuente para el año 2021 con el desarrollo de protocolos de Ciberseguridad en los diferentes Ministerios que conforman el Poder Ejecutivo, por lo que, el desarrollo de esta estrategia a nivel nacional es fundamental como una línea base de lo que tales instrumentos persiguen.

3.3 El sector Telecomunicaciones y sus avances

3.3.1 Marco Regulatorio y su vinculación con la seguridad cibernética

Mediante la Ley General de Telecomunicaciones, Ley N° 8642 y la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, Ley N° 8660 se creó el Sector Telecomunicaciones, designando al Ministerio de Ciencia, Tecnología y Telecomunicaciones, como la entidad Rectora del sector, encargada entre otros aspectos de la emisión de la política pública; y se constituye a la Superintendencia de Telecomunicaciones (SUTEL), como órgano de desconcentración máxima adscrito a la Autoridad Reguladora de los Servicios Públicos (ARESEP), encargado de la regulación.

Asimismo, este marco normativo se complementa con una serie de reglamentos que vienen a operacionalizar el mandato de las leyes mencionadas. En particular, en lo que refiere a temas de Seguridad Cibernética, cabe destacar el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones[12], que desarrolla lo dispuesto en el artículo 42 de la Ley General de Telecomunicaciones, Ley N° 8642 y el Reglamento sobre Protección al Usuario Final de los Servicios de Telecomunicaciones.

En el año 2012, la SUTEL promovió el cumplimiento de lo establecido en la legislación costarricense en cuanto a lo dispuesto en el artículo 56 inciso f) del Reglamento sobre Protección al Usuario Final de los Servicios de Telecomunicaciones, el cual contempla el tema de fraudes en contra del usuario, específicamente en el campo de robo y reactivación de celulares. Para atender el citado cumplimiento, durante ese año se efectuaron reuniones con los operadores y proveedores de los servicios de telecomunicaciones, con el fin de determinar las mejores prácticas para la inclusión de IMEIS a las listas negras, siendo la integración con la Groupe Speciale Mobile Association (GSMA) la solución seleccionada, debido a la cantidad de países

[12] *También se puede hacer referencia al decreto ejecutivo DE 35.205 16-04-2009 Reglamento Protección Privacidad de Comunicaciones y el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 publicado en Gaceta N° 72 el 15 de abril de 2010.*

que se integran a esta para el intercambio de información. La GSMA, que agrupa más de 200 países y cerca de 800 operadores de telefonía móvil, pone a la disposición de los operadores el acceso a sus bases de datos de terminales robados (lista negra).

En el mes de marzo del año 2012 se firmó un Memorando de Entendimiento entre los operadores de telefonía móvil del país y la GSMA. En dicho Memorando, se acordó el compromiso público de integrar sus bases de datos de terminales robados a esta organización y así bloquear el uso de dichos terminales a nivel país en la totalidad de países integrados a la GSMA. Con esto, Costa Rica fue el primer país de América Latina en conectar a todos sus operadores a la base de datos de terminales robados de la GSMA. Este hecho marcó la pauta en la región en la lucha contra el robo de terminales[13].

Con el fin de contar con la herramienta para atender el fraude por suscripción, de conformidad con lo dispuesto en el artículo 43 del Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones[14], existe la obligación de realizar un registro adecuado de los usuarios de los servicios prepago. Para esto, la SUTEL ha realizado gestiones para promover la depuración de la información de estos registros, máxime considerando la existencia de un alto número de reportes de usuarios e informes en los cuales se demuestran inconsistencias en el registro por parte de los operadores de los servicios prepago. Asimismo, diversas entidades como el Poder Judicial (PJ) y el Ministerio de Seguridad Pública (MSP) han insistido sobre la necesidad de contar con un registro de usuarios fiable, más aun considerando el deber que tiene la SUTEL de velar por los derechos de los usuarios de las telecomunicaciones tal y como lo establece la legislación vigente.

En cumplimiento de la Ley Nº 8934, Ley de Protección a la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y Otros Medios Electrónicos, el Consejo de la SUTEL adoptó el acuerdo 024-019-2012 que detalla la información y filtros que deben implementar los Internet café para la protección de la niñez, acorde con la búsqueda constante de proteger a esta

[13] *GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Sitio web. [En línea]. Disponible en: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/*

[14] *Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 publicado en Gaceta N° 72 el 15 de abril de 2010: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf*

población, no solo en el mundo físico sino también en el mundo digital, que a pesar de ser virtual tiene consecuencias reales.

En materia de generación de capacidades, SUTEL colabora con la Escuela Judicial brindando charlas y capacitaciones a los jueces en materia de seguridad, en el marco del programa de capacitación en telecomunicaciones que implementa dicha Escuela.

Dentro del marco regulatorio, Costa Rica ha actualizado su normativa nacional creando un desarrollo jurídico de protección para la cibersociedad costarricense, permitiendo que exista la posibilidad que las personas denuncien violaciones que sufrían en el mundo virtual que antes no tenían respuesta jurídica. Entre ellos, se destaca la Ley de Protección de la Persona frente al tratamiento de sus Datos Personales y su Reglamento, creando de esta forma la Agencia de Protección de Datos de los Habitantes (PRODHAB), la cual es el ente rector en esta materia.

También se cuenta con la Ley de Delitos Informáticos Ley Nº 9048 y la Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal instaurando un marco jurídico penal más completo y acorde a los nuevos delitos cometidos por medios tecnológicos.

En busca de mejorar aún más el marco normativo costarricense y lograr un mejor accionar ante la delincuencia informática, Costa Rica concretó el proceso de adhesión a la “Convención sobre el Cibercrimen” conocida como el “Convenio de Budapest” mediante la firma del Decreto Ejecutivo N° 40546-RREE el 3 de julio del 2017 el cual coadyuva en la lucha frente a los delitos informáticos.[15]

Con el objetivo de contar con una unidad encargada de recabar las pruebas para la atención de delitos vinculados con la tecnología, se creó en 1997, la Sección de Delitos Informáticos, como Unidad de Investigación Informática, adscrita al Departamento de Investigaciones Criminales, y nació ante la necesidad de procesar información almacenada en computadores y servidores de casos importantes; en 2002 se constituyó como Sección de Delitos Informáticos.

Esta sección realiza investigaciones de delitos informáticos y de otros delitos relacionados con las tecnologías en los cuales se utiliza esta para cometer un acto delictivo o como medio de prueba. Con esos fines se utilizan técnicas de computación forense, alineadas con estándares

[15] *Ministerio de Relaciones Exteriores y Culto (2017). Decreto Ejecutivo N°40546-RREE. Disponible en http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84643&nValor3=109293&param2=1&strTipM=TC&lResultado=1&strSim=simp*

internacionales, en la recolección, preservación y análisis de indicios, garantizando la cadena de custodia en computadoras, teléfonos, y otros dispositivos de procesamiento y almacenamiento de datos.

3.3.2 Punto de Intercambio de Internet

De acuerdo con estudios del proyecto CEPAL @LIS2: Balances, desafíos y proyecciones "…el 80% del tráfico latinoamericano de internet todavía pasa por las redes de Estados Unidos, la utilización de conexiones internacionales, en algunos países, eleva los precios hasta en un 40%"[16].

En el caso de Costa Rica, para el año 2014 el MICITT y la Academia Nacional de Ciencias (ANC) trabajaron en conjunto para impulsar la creación del Punto de Intercambio de Internet de Costa Rica (CRIX) el cual se constituyó como proyecto de interés público mediante el Decreto Ejecutivo Nº 38388- MICITT, "Declaratoria de Interés Público del Punto de Intercambio de Tráfico de Internet de la Academia Nacional de Ciencias", en La Gaceta Nº 93 del viernes 16 de mayo del 2014[17].

El Punto de Intercambio de Internet de Costa Rica (CRIX), es administrado por el NIC Costa Rica, entidad encargada de la administración del dominio de nivel superior .cr y sus categorías .co.cr, .fi.cr, .or.cr, .sa.cr, .ed.cr, .ac.cr y .go.cr; que ha logrado construir una red de confianza nacional para la infraestructura local de la Internet.[18]

Aunado a ello el país se convirtió en uno de los primeros países en el mundo en implementar la norma de validación de origen (RPKI) en su Punto de Intercambio de Internet (IXP). Esta validación permite el fortalecimiento del tráfico local de Internet evitando a su vez el secuestro de

---

[16] MICITT. Boletín Contacto Digital. IXP Costa Rica: Una oportunidad estratégica. MICITT: Departamento de Sociedad de la Información. Recuperado el 2 de marzo de 2017 de, https://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574

[17] MICITT. Boletín Contacto Digital. IXP Costa Rica: Una oportunidad estratégica. MICITT: Departamento de Sociedad de la Información. Recuperado el 2 de marzo de 2017 de, https://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574

[18] NIC CR. (14 de mayo de 2015). Sitio web NIC CR. "Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)". Recuperado el 24 de Agosto de 2015 de, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp

rutas, en procura, entre otras cosas, de la captura de tráfico con información sensible (como cuentas bancarias, contraseñas, etc.), y ataques distribuidos de denegación de servicio DDoS.[19]

3.3.3 Prácticas de Seguridad Cibernética de los Operadores en Costa Rica

Como parte de la construcción de esta Estrategia Nacional de Seguridad Cibernética, la SUTEL apoyó llevando a cabo una consulta dirigida a los operadores y proveedores sobre las prácticas que implementan en materia de ciberseguridad. Un breve análisis de los resultados se presenta a continuación.

El cuestionario se remitió a 17 empresas del sector en el año 2015[20], el cuál incluía preguntas sobre prácticas frecuentes de seguridad de la información que estarían siendo aplicadas por los operadores y proveedores de servicios de telecomunicaciones; información sobre el tipo de personal asignado a tareas de seguridad; identificación de infraestructura crítica; compartición de información en caso de eventos y documentación de casos. A continuación, se presenta un resumen de las respuestas recibidas.

[19] NIC CR. (14 de mayo de 2015). Sitio web NIC CR. "Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)". Recuperado el 24 de Agosto de 2015 de, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp

[20] Consulta realizada bajo el oficio 04948-SUTEL-CS-2015 el 24 de julio de 2015.

Cuadro 4 Resumen de las respuestas dadas al cuestionario sobre prácticas de seguridad cibernética realizado por la SUTEL a los operadores y proveedores

¿Su empresa cuenta con políticas/procedimientos por escrito y aprobadas para asegurar la información interna y de sus usuarios?						100%
¿Su empresa cuenta con una certificación de calidad en seguridad de la información?						0%
¿Su empresa ha detectado posibles amenazas o ataques en el último año?						33%
¿Su empresa tiene identificada la infraestructura esencial sensible de sufrir un ciberataque?						100%
¿Su empresa cuenta con procedimientos para controlar y monitorear los cambios aplicados a la configuración de la infraestructura esencial?						83%
¿Con que periodicidad respalda información su empresa?						
	De que forma?				Magnético	83%
					Óptico	50%
					En la Nube	33%
¿Cuál es el perfil de los profesionales encargados de atender asuntos de seguridad de la información o ciberataques?						
					Ingenieros	100%
					Técnicos	50%
¿Qué tipo de capacitación especializada han recibido en el último año?						83%
			De un proveedor de hardware especializado			50%
			De proveedor de software especializado			33%
			Educación formal (Universidades o Institutos locales o internacionales)			33%
			Curso de entidades certificadoras			0%
			Otros			17%
¿En caso de eventos su empresa comparte información con otras empresas para poder mitigar un ataque?						17%
¿Su empresa documenta los casos de ataques que ha sufrido?						67%
¿Su empresa hace análisis de las causas que permitieron que se diera el evento (forensics)?						83%
¿Su empresa realiza actividades de divulgación a sus usuarios sobre cómo protegerse en el ciberespacio?						83%
			Información en la página Web			33%
			Correos electrónicos informativos			83%
			Mensajes de texto			0%
			Puesta a disposición de herramientas para protección			33%
			Capacitación en línea			33%
			Otros			17%

Fuente: Elaboración propia. SUTEL. Consulta realizada bajo el oficio 04948-SUTEL-CS-2015 el 24 de julio de 2015.

Es digno señalar que el 100% de las empresas indicaron que contaban con una política o procedimientos internos para garantizar la seguridad y privacidad de la información interna y de sus usuarios. Lo anterior, demuestra que este es un tema importante para las empresas del sector y que han buscado los mecanismos para asegurar la integridad de esta información.

A pesar de que sólo un tercio de las compañías consultadas afirma haber detectado posibles amenazas o haber sufrido un ataque en el último año, el 100% afirma tener identificada su infraestructura esencial y un 83% cuenta con procedimientos para controlar y monitorear los cambios que se hacen sobre esta. Asimismo, la totalidad de los operadores y proveedores de servicios de telecomunicaciones encuestados, señalan que tienen ingenieros dedicados a labores relacionadas con seguridad cibernética, y en un 83% de los casos, estos han recibido algún tipo de capacitación en el último año. Estos resultados muestran que las empresas han tomado previsiones en este tema y han buscado preparar a su personal.

A pesar de lo anterior, se extrae de las respuestas aportadas, que las empresas no coordinan entre sí frente a ciberataques ni comparten información y, además, no todas documentan los casos que se presentan. Adicionalmente, los esfuerzos para divulgar información entre los usuarios, que hacen los operadores y proveedores son diversos y no responden a un objetivo coordinado, por lo cual, este también es un tema que debe ser contemplado por la estrategia.

3.3.4 Sistema Nacional de Certificación Digital

Con la promulgación de la Ley Nº 8454, de Certificados, Firmas Digitales y Documentos Electrónicos, se dio la base legal para la emisión y uso de certificados de firma digital en el país, brindando la seguridad jurídica necesaria para que los documentos electrónicos firmados digitalmente tengan el mismo valor que los documentos con firma manuscrita.

En agosto de 2009, se realizó el lanzamiento del Sistema de Certificación Digital, el cual ha sido diseñado para propiciar transacciones en línea más seguras. De acuerdo con la Ley, la entidad que emite certificados digitales debe estar registrada ante la Dirección de Certificadores de Firma Digital (DCFD) del MICITT y garantizar el cumplimiento de los estándares de seguridad y operación que dan respaldo a las transacciones electrónicas.

El marco jurídico vigente en el país permite garantizar la seguridad jurídica de las transacciones, la protección de los derechos de los consumidores y la credibilidad del sistema nacional de certificación digital al brindar respaldo a las transacciones a nivel electrónico, permitiendo la equivalencia jurídica entre los documentos físicos y los emitidos por medios electrónicos. La

reglamentación del sistema y las directrices son promulgadas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).[21]

En la actualidad, el Banco Central de Costa Rica tiene constituida una Autoridad Certificadora para la emisión de certificados de firma digital para personas físicas (CA SINPE - Persona Física) y personas jurídicas (CA SINPE- Persona Jurídica), además de facilitar el servicio de estampado de tiempo (TSA SINPE)[22]. El uso de estos certificados ha fortalecido el sector público, así como los servicios que le ofrece, garantizando transacciones en línea más seguras.

3.3.5 Centro de Respuesta a Incidentes de Seguridad Informática: CSIRT-CR

Este centro fue constituido mediante el Decreto Ejecutivo Nº 37052-MICIT del 09 de marzo de 2012[23]. En dicha norma se le designa al CSIRT-CR como la entidad encargada de coordinar todo lo relacionado en materia de seguridad informática y cibernética. Asimismo, se le faculta para contar con un equipo de expertos en seguridad de las Tecnologías de la Información y la Comunicación encargado de prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

El CSIRT-CR busca la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio, de manera que se logre incorporar el sistema de seguridad cibernética y tecnologías de información a la protección del Gobierno Central y las Entidades Autónomas para disminuir los riesgos y amenazas cibernéticas.

El centro se encuentra a cargo de la Dirección de Gobernanza Digital del MICITT, sin embargo, actualmente su operación es limitada dada la carencia de recursos en el sector público. Las tareas que se han realizado a la fecha han consistido principalmente en la generación de capacidades en funcionarios del sector público, a través de diferentes capacitaciones sobre ciberseguridad. Adicionalmente el CSIRT-CR, se ha dado a la tarea de concientizar e informar, con el apoyo de especialistas en diferentes campos, sobre temas de relevancia como Deep Web y seguridad en trámites bancarios.

---

[21] Sitio web Firma Digital. [En línea]. Disponible en: http://www.firmadigital.go.cr/Leyes.html

[22] Sitio web Firma Digital. [En línea]. Disponible en: http://www.firmadigital.go.cr/Leyes.html

[23] Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR, Decreto Nº 37052-MICIT, Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR. Diario Oficial La Gaceta de la República de Costa Rica, 09 de marzo de 2012. Disponible en: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832

Existe la necesidad de contar con un enfoque específico en los aspectos de desarrollo del CSIRT-CR para garantizar una mejor funcionalidad y sostenibilidad. Estas medidas le permitirán operar de manera eficiente y estar equipado para determinar rápidamente las amenazas y aplicar medidas en su contra, para impedir futuras amenazas y recuperarse de las existentes. El CSIRT requerirá una asignación presupuestal explícita y un plan operativo, que le permita concretar las funciones que se le asignaron.

3.3.6 Comisión Nacional de Seguridad en Línea

En el año 2010, mediante Decreto Nº 36274-MICIT se creó la Comisión Nacional de Seguridad en Línea (CNSL)[24], con el objetivo principal de diseñar las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales contribuyendo a generar una cultura de comprensión, análisis y responsabilidad en las personas, que les permita beneficiarse de las ventajas de la utilización de las TIC y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos.

La comisión está liderada por el MICITT y la integran representantes del Ministerio de Educación Pública, Ministerio de Cultura y Juventud, Patronato Nacional de la Infancia, Poder Judicial, SUTEL, CAMTIC, Fundación Omar Dengo y Fundación Paniamor.

De acuerdo con lo señalado por el Decreto Ejecutivo Nº 36274-MICIT muchas de las acciones de la Comisión deben ser dirigidas a las poblaciones vulnerables al uso de las tecnologías en línea, una de estas poblaciones es la niñez y adolescencia de todo el país. En ese sentido la comisión formuló un plan de trabajo, que sustentado en cuatro ejes temáticos principales de los cuales se desprenden una serie de líneas de trabajo, abarcan el fortalecimiento del marco normativo, la consolidación de mecanismos de articulación interinstitucional, el desarrollo de proyectos que promueven la seguridad en línea y el fomento a la investigación como base para la formulación de acciones.

3.3.7 Automatización y digitalización de servicios en línea disponibles a la ciudadanía

En cuanto al desarrollo de proyectos en materia tecnológica, en el país se han desarrollado una serie de iniciativas en diversas áreas como son el acceso a la información pública, la

[24] *Sitio web Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=69239&nValor3=83075&strTipM=TC*

automatización de trámites y seguridad ciudadana donde vale destacar los siguientes:[25] Portal Ciudadano, Datos Abiertos, Registro de Productos de Interés Sanitario, Ventanilla Electrónica de Servicios (VES), Crea Empresa, MuNet e-Gobierno y el más reciente el Sistema de Compras Públicas (SICOP).

En materia de salud, se puede destacar el Expediente Digital Único de Salud (EDUS), el cual es un programa impulsado por la Caja Costarricense de Seguro Social y se define como: "el conjunto de aplicaciones informáticas que automatizan los sistemas de salud de los tres (3) niveles de atención según el modelo de servicios de salud con que opera la institución"[26].

En relación con seguridad ciudadana, el Ministerio de Seguridad Pública (MSP) cuenta con una plataforma para trámites de registro de agentes y empresas de seguridad, así como el Control de Portación de Armas y Seguridad Privada (ControlPas)[27].

En cuanto a la gestión pública de las TIC, es menester destacar los procesos de coordinación interinstitucional, tal es el caso de la gestión de las licencias de conducir y pasaportes en las agencias del Banco de Costa Rica (BCR). Esto gracias a la interoperabilidad de sistemas de la Dirección General de Migración y Extranjería y el Ministerio de Obras Públicas y Transporte (MOPT) con la plataforma del BCR[28]

Otra entidad importante que proporciona servicios administrativos y electorales en línea es el Tribunal Supremo de Elecciones (TSE) que entre los servicios que ofrece se encuentran el manejo de documentos de los ciudadanos y residentes, registros civiles, contratos nupciales y el censo electoral.

Adicionalmente, los costarricenses cuentan con acceso en línea a información jurídica pública en virtud de que un número de entidades del gobierno han adoptado las TIC para brindar sus servicios en forma electrónica. Como parte del proyecto de Modernización de la Administración de Justicia, el Poder Judicial, la Procuraduría General de la República (PGR) y el Banco Interamericano de Desarrollo (BID) se asociaron para el desarrollo del Sistema Costarricense de Información Jurídica (SCIJ)[29]. El sistema contiene información normativa y jurisprudencial del derecho costarricense.

---

[25] Tomado de Informe Técnico IT-DGE-2014-005. Se pueden encontrar referencias actualmente en: http://gob.go.cr/es/

26 Oficio Gerencia Médica GM-42211/GIT-411556-2010 del 20 de octubre del 2010.

27 ControlPAS. Tomado de: https://www.controlpas.go.cr/Inicio/Informacion

28 http://bcrcita.bancobcr.com/cita/RequisitosPasaporte.aspx

[29] Sitio web Sistema Costarricense de Información Jurídica. [En línea]. Disponible en: http://www.pgrweb.go.cr/scij/

El sistema judicial de Costa Rica también está implementando un portal integral de justicia electrónica que ofrece diversos servicios judiciales en línea[30]. Estos incluyen auditorías y registros institucionales disponibles públicamente, personas desaparecidas, listas de los más buscados, informes de convictos prófugos y literatura sobre estatutos y leyes nacionales. El portal también les permite a los ciudadanos presentar informes a la policía, realizar pagos por servicios legales y solicitar consulta legal ante los Tribunales de Circuito del país. Actualmente al menos diecinueve tribunales cuentan con la capacidad de recibir las solicitudes de consulta en línea. Con estos servicios, el sistema judicial tiene como objetivo crear un proceso más transparente y simple para que los ciudadanos busquen asistencia legal.

En materia de obtención de pruebas, el Poder Judicial tiene la autoridad jurisdiccional, de conformidad con el artículo 24 de la Ley N° 7425, "Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones"[31] para intervenir en cualquier comunicación oral, escrita o de otro tipo, incluidas las telecomunicaciones fijas, móviles, inalámbricas y digitales. Este aspecto es muy relevante dado que las pruebas electrónicas implican tanto un componente de seguridad como uno de privacidad.

Con el aumento del número de casos de pruebas digitales, debe tenerse en cuenta la interoperabilidad al interior del sistema judicial para pronunciarse sobre estas, y así garantizar su seguridad e integridad.

Aunado a ello y en aras de dar a conocer la información judicial, el Poder Judicial realiza ese proceso tomando como referencia lo establecido por la Ley Nº 8968 “Ley de protección de la persona frente al tratamiento de sus datos personales” y el documento Reglas Mínimas para la Difusión de Información Judicial en Internet con lo cual implementan las mejores prácticas para encontrar un equilibrio entre privacidad y transparencia al momento de poner datos judiciales a disposición del público[32].

---

[30] Sitio web del Poder Judicial de la República de Costa Rica. [En línea]. Disponible en: http://www.poder-judicial.go.cr/

[31] Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones Nº 7425. Diario Oficial La Gaceta de la República de Costa Rica, 09 de agosto de 1994. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

[32] Reglas de Heredia: Reglas mínimas para la Difusión de la Información Judicial en Internet, Seminario Internet y Sistema Judicial, Heredia, 09 de julio de 2003. [En línea]. Disponible en: http://www.iijusticia.edu.ar/heredia/Heredia_Rules.htm

3.4 Formación en Seguridad Cibernética

El país es reconocido por la importante inversión que se realiza en el sector educación, por mandato constitucional el país dedica el 8% del Producto Interno Bruto (PIB) a la educación. Siendo un área de gran relevancia para el país, la incorporación de las TIC en la educación, también se ha considerado una prioridad nacional, y se tienen diversos proyectos desde finales de los años 80.

Actualmente, el MEP, el MICITT y la SUTEL, en conjunto con otras organizaciones públicas, no gubernamentales, privadas, académicas y de la sociedad civil han implementado proyectos para cerrar las brechas en la educación a través del uso de las TIC, utilizando los recursos del Fondo Nacional de Telecomunicaciones (FONATEL). El objetivo de estas iniciativas ha sido transformar los procesos de enseñanza y aprendizaje a través del acceso universal a la conectividad de banda ancha, las tecnologías móviles y las herramientas de apoyo educativo de las TIC para profesores y estudiantes.

Actualmente el 63% de las instituciones educativas de nivel secundario tiene un laboratorio de computación, en comparación con el 23% de las escuelas primarias[33] y se están haciendo gestiones para mejorar estas cifras.

En lo que refiere a la formación de profesionales, tanto universidades públicas como privadas ofrecen carreras con niveles de grado, posgrado y especializaciones[34] en temas vinculados con TIC, sin embargo, no necesariamente incluyen especializaciones en Seguridad Cibernética, a excepción de un centro educativo privado que ofrece formación a nivel de maestría.

El programa de este post grado en Ciberseguridad, está orientado a la formación de profesionales de seguridad de la información y comunicación, tanto en el desarrollo de habilidades técnicas y de gestión, así como en la introducción de aspectos teóricos necesarios para este campo. Para completar el programa, los estudiantes deben llevar a cabo dos proyectos de investigación aplicada, mediante la incorporación de los conceptos que han aprendido, para resolver un problema de seguridad cibernética en el mundo real. Este programa cuenta con el apoyo de una serie de empresas multinacionales de TIC, sin embargo, dado que esta carrera se

[33] *Uso de TIC en educación en América Latina y el Caribe - Análisis regional de la integración de las TIC y de la aptitud digital (e-readiness) - Instituto de Estadística de UNESCO: http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-sp.pdf*

[34] *En diversos temas como: computación e informática, telemática y redes, sistemas de información, gestión de TI, gestión de proyectos, auditoría de TI e ingeniería de sistemas de bases de datos.*

da en el sector privado de educación, se limitan las posibilidades de acceder a ella por la inversión económica que requiere.

Al considerar la asociación con instituciones de educación superior, se requiere tomar en cuenta diversos enfoques basados en la naturaleza de la constitución de cada uno. Por ejemplo, las universidades públicas son autónomas, aunque tienen normas comunes y se coordinan entre sí (Consejo Nacional de Rectores (CONARE) / Oficina de Planificación de la Educación Superior (OPES)); el Consejo Nacional de Enseñanza Superior Universitaria Privada (CONESUP) autoriza y supervisa las universidades privadas y el Sistema Nacional de Acreditación de la Educación Superior (SINAES) acredita programas académicos públicos y privados autorizados.

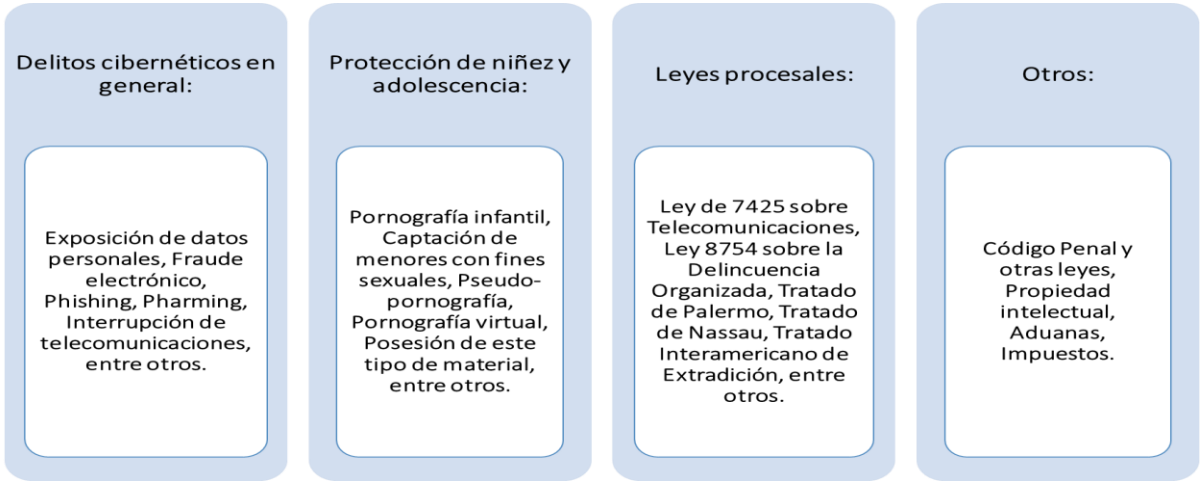
En razón de lo anterior, hay una necesidad de trabajar en conjunto con diversas instituciones educativas y organismos de acreditación para abrir cursos que cubran aspectos relevantes de la seguridad de la información/cibernética. Adicionalmente, es importante tomar en consideración la red de colegios científicos y aquellos que tengan laboratorios de cómputo, para fomentar la enseñanza de aspectos fundamentales de la seguridad cibernética desde la educación secundaria.

3.4.1 Fortalecimiento del marco legal para la atención del delito cibernético

A menudo es complejo prevenir un delito cibernético y a veces es aún más difícil identificar al autor. Los delitos cibernéticos pueden ser descritos de dos maneras: los delitos contra un sistema informático (por ejemplo, daño o acceso sin autorización a datos, programas o redes) y los delitos facilitados a través de un sistema informático (por ejemplo, la publicación de pornografía infantil). En esa línea, existen varias leyes en Costa Rica[35] que se ocupan de la delincuencia cibernética directa e indirectamente. La siguiente figura resume los temas que abarcan.

[35] *Ley de Delitos Informáticos y Conexos, Ley N° 9048. Diario Oficial La Gaceta de la República de Costa Rica, 06 de noviembre de 2012. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&param2=1&strTipM=TC&lResultado=1&strSim=simp*
Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal, Ley N° 9135. Diario Oficial La Gaceta de la República de Costa Rica, 26 de abril de 2013. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&param2=1&strTipM=TC&lResultado=1&strSim=simp

Figura 2 Temas tratados por leyes de Costa Rica relativas a delitos informáticos



Fuente: Elaboración propia, 2016.

La legislación sobre delincuencia cibernética debe tener en cuenta el contexto nacional, los convenios internacionales, los mecanismos para facilitar la investigación inter-institucional y multi-jurisdiccional y la mayor complejidad de avances tecnológicos. Costa Rica cuenta con legislación relacionada con delitos informáticos, no obstante, a medida que cambia la sofisticación de estos crímenes, debe haber un proceso dedicado para su revisión y actualización para asegurar que existe la autoridad necesaria para investigar y procesar eficazmente. La adhesión al Convenio sobre Delincuencia Cibernética (también conocido como Convenio de Budapest) es un hecho y las discusiones están en curso dentro del Poder Judicial para la formación de jueces y fiscales en materia de delincuencia cibernética.

Sin embargo, en la consecución de estos objetivos, debe hacerse una distinción entre la capacidad técnica para detectar e identificar una vulnerabilidad y las herramientas procesales necesarias para que las fuerzas del orden investiguen con eficacia los delitos cibernéticos (teniendo en cuenta la velocidad y la naturaleza transitoria de los datos digitales). Se deben considerar los roles y las responsabilidades de los proveedores de servicios de Internet, así como de cualquier otro actor activo en el ciberespacio, además de equilibrar estas acciones con la necesidad de respetar los derechos humanos fundamentales en la recolección de la evidencia digital. Por lo tanto, dada la naturaleza del entorno digital es necesario contar con mecanismos pertinentes para asegurar la revisión y actualización de las leyes de delitos informáticos periódicamente.

Capítulo 4 - Principios rectores

Esta estrategia está motivada en los siguientes principios rectores:

- Las personas son la prioridad
- Respeto a los Derechos Humanos y la Privacidad.
- Coordinación y corresponsabilidad de múltiples partes interesadas.
- Cooperación Internacional

4.1 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.

4.2 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.

4.3 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.

4.4 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.

Capítulo 5 – Marco Estratégico para la Seguridad Cibernética

Las ventajas de la conexión a Internet y el uso de las TIC son innegables, ya que nos brindan una plataforma que potencia cada uno de los sectores económicos del país y que puede ser aprovechada para el mejoramiento de la gestión de la administración pública, la competitividad del sector empresarial y la calidad de vida de los habitantes del país, por lo que debemos procurar el desarrollo de una infraestructura digital ágil, moderna, robusta y segura.

En ese contexto y dado la rápida evolución de las tecnologías digitales, la Estrategia Nacional de Ciberseguridad de Costa Rica debe ser considerada como un documento vivo que establece la visión del país en estas materias a partir de la definición de un objetivo general y una serie de objetivos específicos que comprenden varias líneas estratégicas, que deberán ser desarrolladas en planes de acción en el corto plazo y que en su conjunto se convierten en el marco de seguridad cibernética nacional.

La estrategia buscará contar con el apoyo y la participación de entidades tanto públicas como privadas, así como de organizaciones no gubernamentales, comunidad técnica, academia y sociedad civil. Como entidad responsable principal estará el MICITT y para los aspectos relacionados con incidentes, se contará con la participación del CSIRT-CR.

Por la naturaleza de las líneas de acción se busca una participación activa de los poderes del estado, así como del sector empresarial, organizaciones de sociedad civil, organizaciones no gubernamentales, academia, comunidad técnica, colegios profesionales y cualquier otro actor que se encuentre interesado en participar en la implementación de la estrategia.

Una vez que se efectúe el lanzamiento oficial de la Estrategia Nacional de Ciberseguridad, el MICITT contará con el plazo de tres meses para conformar, convocar y reunir un Comité Consultivo, que estará compuesto 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

Además, se establecerá una figura de coordinación nacional que recaerá en el MICITT, con la responsabilidad de supervisar la aplicación de la estrategia, incluyendo la coordinación con las diversas entidades involucradas en el cumplimiento de las líneas de acción establecidas.

El Comité Consultivo, en conjunto con el Coordinador Nacional en Ciberseguridad, se encargará de disponer todas aquellas acciones necesarias para iniciar el proceso de implementación, mediante planes de acción para cada uno de los objetivos planteados en esta estrategia, previa definición de metas, plazos y responsables.

5.1 Objetivo General

Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.

5.2 Objetivos Específicos

Objetivo específico 1: Coordinación Nacional

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

La coordinación, colaboración y el intercambio de información entre todas las partes interesadas es fundamental para el éxito de cualquier programa nacional de seguridad cibernética. Estas partes interesadas incluyen al sector público [36], la academia, las organizaciones no gubernamentales, al sector privado, la sociedad civil y la comunidad técnica[37].

[36] *Entendido como "…el conjunto total de las organizaciones públicas. Lo integran los Poderes de la República, las instituciones autónomas, las municipalidades, los Bancos del Estado, las empresas públicas y otras instituciones públicas no estatales". De acuerdo a Ministerio de Planificación y Política Económica (MIDEPLAN) (2007). Manual explicativo de los organigramas del sector público costarricense. [En línea]. Recuperado el 16 de agosto de 2016 de, https://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/237a1427-b5f7-4b41-be16-8993ca567e32/organigrama_del_sector_publico.pdf?guest=true*

[37] *Como parte de las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) se insta a la participación de la comunidad técnica con el fin de evitar la toma de decisiones alejada de los estándares de la industria. Ejemplo: el IETF, la IAB, los RIR, los ccTLD, los RO, la ICANN, la ISOC y el W3C."The Internet technical community underlines its role as a source of independent advice regarding the potential intended and unintended consequences of planned policy decisions on the Internet and the way it functions, and stresses that policy makers*

El MICITT como Coordinador Nacional supervisará la eficacia y la eficiencia de las líneas de acción para la implementación y recomendará, en consulta con las partes interesadas pertinentes, medidas que optimicen las políticas y procedimientos de la seguridad cibernética en Costa Rica.

Lo anterior, incluye el establecimiento de políticas claras para definir, regular y promover el intercambio de información entre las diversas entidades interesadas y los grupos de trabajo de cada uno de los sectores, creando un ambiente de confianza y fortaleciendo las líneas de comunicación existentes.

El diálogo y la cooperación entre el sector privado y el Estado son requisitos esenciales para lograr los objetivos de la estrategia, por ello, se promoverá el intercambio de información respaldado mediante acuerdos de confidencialidad para cimentar la confianza necesaria durante el tratamiento eficaz y oportuno ante incidentes.

Adicionalmente, el Estado se reserva la facultad de crear comisiones ad-hoc como mecanismo de estudio, análisis y recomendación en temas puntuales de seguridad cibernética. La representación de los sectores y la conformación de estas comisiones serán determinadas por el tema particular y los sectores pertinentes o afectados.

Línea Estratégica 1.1. Coordinador Nacional

- Designar un coordinador nacional que tendrá la responsabilidad de articular las acciones en materia de seguridad cibernética y darle seguimiento al cumplimiento de esta estrategia. La figura de coordinación nacional, que recaerá en el MICITT, será el punto focal a nivel nacional e internacional para cualquier tema relacionado con seguridad cibernética.

Línea Estratégica 1.2. Colaboración del Sector Público y Sector Privado

- Mantener el diálogo cordial y fluido con el sector privado para el desarrollo de iniciativas a fin de atraer la atención nacional hacia la seguridad cibernética e involucrar una amplia representación de las partes implicadas.

---

should seek such advice as early as possible in the policy development process in order to avoid pursuing technologically flawed decisions." Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2012). Cybersecurity policy making at a turning point. [En línea]. Disponible en: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Objetivo Específico 2: Conciencia pública

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

Se deben tomar medidas para la toma de conciencia sobre la seguridad cibernética, tanto entre los ciudadanos, los funcionarios públicos y las empresas, para asegurarse de que estén informados y educados sobre los riesgos que existen. La seguridad cibernética es uno de los retos económicos y nacionales de mayor importancia, que impacta a todos los actores de la sociedad. Educar a nuestros ciudadanos es un paso fundamental hacia una fuerte resiliencia cibernética como Nación, reconociendo que muchos costarricenses utilizan herramientas de seguridad disponibles en el mercado abierto (por ejemplo, antivirus y firewalls) y son responsables de las medidas de seguridad de sus sistemas informáticos personales. Además, los ciudadanos también usan computadoras y otros terminales móviles en sus lugares de trabajo y tienen acceso a datos sensibles que deben ser protegidos.

Línea Estratégica 2.1. Concienciación - Público en general

- Desarrollar campañas de concienciación en ciberseguridad para los habitantes de Costa Rica de modo que se habitúen y acojan buenas prácticas como parte de su cultura, considerando el fortalecimiento de acciones para la protección de grupos poblacionales en condición de vulnerabilidad como niñez y adolescencia, adultos mayores, población indígena, población con discapacidad. Todo ello en alianza con el sector privado, sociedad civil y organizaciones no gubernamentales dedicadas a la protección de la infancia y adolescencia.

Línea Estratégica 2.2. Sector público

- Desarrollar campañas de concienciación y educación dirigidas a los funcionarios públicos y focalizadas al tipo de institución en el que se desempeñan, que enfaticen las mejoras prácticas de protección y aseguramiento de datos de acceso a sistemas de información y datos sensibles o personales contenidos en estos sistemas.

Línea Estratégica 2.3. Micro, Pequeña y Mediana Empresa

- Desarrollar conversatorios y foros de intercambio de información sobre temas de seguridad cibernética, específicamente para las Micro, Pequeña y Mediana Empresa.

Objetivo Específico 3. Desarrollo de la Capacidad Nacional de Seguridad Cibernética

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

Muchas organizaciones no han podido abordar la seguridad cibernética integralmente, ya sea porque no le han asignado la función de seguridad de la información a una persona o unidad determinada, no han abordado adecuadamente la necesidad de incluirla en sus operaciones comerciales o simplemente no cuentan con los recursos necesarios para asignarla.

Una parte integral de la estrategia será la implementación de medidas destinadas a la alfabetización, concienciación y formación del recurso humano en temas de seguridad cibernética. Es de suma importancia el nivel de competencia de todo el personal en las instituciones públicas, especialmente los administradores y los responsables de la toma de decisiones, ya que muchas veces se realizan ataques bajo la modalidad de ingeniería social dirigidos a empleados o funcionarios estratégicos para poder tener acceso a sistemas de información protegidos.

El propósito fundamental de una cultura de seguridad cibernética es la protección de sistemas informáticos y la adopción de buenas prácticas cibernéticas por parte de estos usuarios.

Línea Estratégica 3.1. Formación de recurso humano especializado

- Fomentar la divulgación y promoción de oportunidades de especialización o capacitación en seguridad cibernética disponibles local o internacionalmente para funcionarios del sector público.
- Proponer e impulsar adecuaciones en la oferta académica que permitan desarrollar planes de estudio de seguridad cibernética o añadir módulos de ciberseguridad a los programas pertinentes de pregrado, posgrado y doctorado.
- Promover la inclusión del tema de ciberseguridad en al menos un curso de carreras no tecnológicas.

Línea estratégica 3.2. Investigación y Desarrollo

- Gestionar alianzas con universidades públicas y privadas para desarrollar proyectos de investigación sobre las amenazas emergentes y el desarrollo de soluciones innovadoras a los incidentes cibernéticos.

Objetivo Específico 4. Fortalecimiento del marco jurídico en Ciberseguridad y TIC

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

La delincuencia informática evoluciona tan rápidamente como la tecnología, lo que significa que las disposiciones legales deben ser revisadas y adaptadas de forma permanente para tener en cuenta los nuevos tipos y metodologías utilizadas por los delincuentes a la hora de cometer delitos informáticos.

Es necesario un diálogo nacional, sobre los acuerdos internacionales de cooperación en lo que respecta a seguridad cibernética, con el fin de generar una mayor conciencia de la necesidad de facilitar un proceso más expedito para la aplicación de las normas vigentes, dado el rápido ritmo de desarrollo y cambio en las TIC.

El marco jurídico de Costa Rica deberá tener en cuenta la naturaleza transfronteriza del ciberespacio, la necesidad de que los responsables de aplicar la ley investiguen con eficacia los delitos cibernéticos (teniendo en cuenta la velocidad y la naturaleza transitoria de los datos digitales), la necesidad de que los equipos de respuesta a incidentes puedan detectar un incidente de manera oportuna, y dotar a las entidades correspondientes de la autoridad necesaria para poder disuadir las amenazas identificadas.

Línea estratégica 4.1. Fortalecer el marco normativo y procesal en ciberdelincuencia

- Crear una comisión especializada para la revisión de la normativa vigente para garantizar que existan herramientas procesales adecuadas en materia de delincuencia cibernética.

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

- Identificar las áreas claves del sistema penal de justicia que requieren fortalecer sus capacidades y conocimientos en materia de Ciberseguridad.
- Colaborar en la generación de capacidades para las áreas claves identificadas.

Línea estratégica 4.3. Fomentar redes de confianza para el Intercambio de información entre los socios interesados en el sistema penal de justicia

- Generar redes de confianza apoyadas mediante un instrumento jurídico de confidencialidad para el intercambio seguro de información relevante vinculada con delitos cibernéticos.
- Diseñar procedimientos expeditos para el intercambio de información confidencial.

Objetivo Específico 5: Protección de Infraestructuras Críticas

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

Se entiende por infraestructuras críticas como el conjunto de instalaciones, sistemas, equipos, redes, datos y servicios cuya interrupción o destrucción tendrían un alto impacto negativo en los servicios esenciales de un país, afectando seriamente el bienestar social y económico de todos los habitantes. La cadena de suministro de bienes y servicios que apoya las operaciones de las infraestructuras críticas es un riesgo que debe ser evaluado teniendo en cuenta las medidas en seguridad implementadas por estos proveedores.

Considerando lo anterior, este objetivo busca definir un conjunto de actividades para asegurar la continuidad, funcionalidad e integridad de las infraestructuras críticas; con el fin de prevenir, gestionar, mitigar y/o restaurar sus funciones ante un eventual ataque cibernético.

Es de suma importancia que los operadores de infraestructuras críticas utilicen marcos de seguridad específicos para gestionar la evolución de los riesgos de seguridad en la adquisición de bienes y servicios de TIC. Por ejemplo, la externalización de operaciones de red puede aumentar los riesgos si los proveedores de esos servicios no están dispuestos a estar de acuerdo con el nivel mínimo de prestación, incluyendo un tiempo de respuesta aceptable y aplicación de medidas mínimas de seguridad.

Como parte del proceso para asegurar la infraestructura crítica se deberá examinar específicamente el uso de Sistemas de Control Industrial (SCI) y Sistemas de Control de Supervisión y Adquisición de Datos (SCADA). Los sistemas industriales están ahora diseñados con más capacidad de conexión, por lo tanto, representan una amenaza mayor a la ciberseguridad. Es crucial que las entidades reguladoras de los sectores clasificados como de infraestructura crítica asuman un papel más protagónico y comiencen a definir y dictar lineamientos claros sobre el tema de seguridad cibernética y a los fines de que las entidades

reguladas cumplan con la normativa, estándares y buenas prácticas vigentes tanto de su sector en particular, como aquellas de acatamiento nacional.

Es vital la implementación de directrices y una mayor cooperación entre los operadores de infraestructuras críticas, proveedores de servicios TIC, proveedores de sistemas y el Estado. Además, se debe mitigar cualquier transgresión de seguridad que tenga un impacto significativo en las operaciones del proveedor de servicios, para lo cual se alentará a los operadores de SCI y de SCADA a implementar políticas de seguridad que establezcan el abordaje de los riesgos identificados y las posibles vulnerabilidades.

Se tomarán en cuenta algunas normas en la construcción de la resiliencia en este sector, por ejemplo, se incluirán las normas ISO 27001 e ISO 27002, NERC CIP-002-3 a través de CIP-009-3[38], Publicación Especial NIST 800-82 y Marco de Mejora de la Seguridad Cibernética de Infraestructuras Críticas[39], entre otros.

Línea estratégica 5.1 Identificación y clasificación de las Infraestructuras Críticas

- Identificar las infraestructuras críticas del país como paso crucial para la aplicación de medidas de seguridad.
- Crear una comisión para la generación de política pública conformada por un representante y un suplente de cada una de las instituciones públicas y entidades privadas identificadas, con el fin de garantizar la operatividad y estabilidad continua de estos servicios.

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

- Diseñar protocolos de ciberseguridad para los Ministerios del Poder Ejecutivo, acorde al estado de madurez de cada una de las instituciones y según las necesidades existentes en el sector público.

El Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR) del MICITT tendrá la función de colaborar y asesorar en el diseño de dichas herramientas.

---

[38] North American Electric Reliability Corporation (NERC). CIP Standards. [En línea]. Recuperado el 27 de agosto de 2015 de, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[39] National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. [En línea]. Recuperado el 27 de agosto de 2015 de, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (actualizado diciembre 5 2014).

Objetivo Específico 6: Gestión del Riesgo

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

La adopción de un proceso de gestión del riesgo es esencial, para la revisión, a nivel directivo de cualquier organización, de los riesgos importantes relacionados con tecnologías de información, que podrían ocurrir de manera regular, y que proporcionaría un enfoque coherente en la apropiación de esta gestión. Muchas entidades tienen problemas y deficiencias en esta área, por lo que no evalúan, ni miden, ni comunican de manera adecuada en qué medida sus operaciones se ven afectadas por ataques cibernéticos, ni las gestiones que adelantan para construir su resiliencia cibernética. Este entendimiento es clave para poder abordar el riesgo cibernético de manera efectiva.

Un régimen de seguridad cibernética eficaz adopta o desarrolla un marco con un ciclo continuo de actividad de evaluación del riesgo, control del riesgo, desarrollo de políticas de seguridad generales, garantía de continuidad del negocio, asignación de responsabilidades, promoción de concienciación y seguimiento de la eficacia de los controles implementados. La planificación de Continuidad Empresarial es una medida proactiva que asegura que, en caso de emergencias, fallos del sistema o desastres es posible recuperar y mantener las funciones normales del negocio en caso de ocurrir algún riesgo grave. La incertidumbre es un tema central en Riesgos de Tecnologías de la Información y por ello se requiere la implementación de las mejores prácticas para su gestión. [40]

Es por ello que se tomará en consideración el Modelo de Gestión del Riesgo del Software Engineering Institute (SEI), el Marco de Gestión del Riesgo de la Federal Information Security Management (FISMA) y las normas ISO/IEC INTE 27000, entre otros.

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

- Promover de forma prioritaria la implementación de normas de seguridad para la operación de las organizaciones públicas y privadas, tomando en cuenta las normas internacionales tales como NIST, INTE/ISO/IEC, COBIT, recomendaciones de la

[40] *Tripton, H. y Krause, M. (2004). Handbook of Information Security Management. USA: CRC Press. Disponible: http://index-of.co.uk/Computer-Security/CRC%20Press%20-%20Information%20Security%20Management%20Handbook,%20Fifth%20.pdf*

Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT).

- Generar negociaciones con entidades certificadoras de manera que se facilite la certificación de instituciones y organizaciones interesadas.

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

- Coordinar con el ente regulador del sector financiero para generar un marco de seguridad específico para las entidades de esta naturaleza, tomando en cuenta los diferentes niveles de madurez y tamaño de cada organización del sector.
- Crear un mecanismo de comunicación constante con las diferentes instituciones que conforman el sistema financiero, para analizar las oportunidades de mejora y retos en el fortalecimiento de la ciberseguridad.

Línea estratégica 6.3. Adopción de medidas de seguridad de referencia

- Promover la incorporación de medidas apropiadas de seguridad, privacidad y propiedad de los datos, para aquellos servicios que se prestan a la ciudadanía, favoreciendo el uso de certificados digitales de autenticación y enfatizando la implementación de normas estrictas para la protección de datos en servicios de almacenamiento como los de computación en la nube.

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

- Facilitar y promover el intercambio de información entre los responsables de seguridad de la información del gobierno a través de una red de confianza, donde se apliquen altos niveles de confidencialidad y profesionalismo. Los ataques y eventos a menudo afectan múltiples organizaciones. Una comunicación y coordinación adecuadas podrían reducir los riesgos y minimizar el posible impacto.
- Desarrollar un instrumento jurídico que permita establecer el alcance y las condiciones de los participantes de la red.

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

- Fortalecer y mejorar la resiliencia contra disturbios e incidentes informáticos.
- Asignar recursos exclusivos, que permitan atender todos los componentes del CSIRT-CR.

- Promover y apoyar la creación de CSIRT sectoriales que coordinen con el CSIRT Nacional, de manera que puedan proporcionar soluciones específicas para cada sector y contribuir de esta forma a una recuperación más rápida y eficaz ante sus incidentes.

Objetivo Específico 7: Cooperación y Compromiso Internacional

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

Internet es una herramienta mundial para la colaboración y el desarrollo, y por ello, es necesario establecer lazos de colaboración y cooperación en estas materias que coadyuven al crecimiento y desarrollo de las capacidades nacionales en ciberseguridad.

Se promoverá la integración del país en los esfuerzos a nivel bilateral y multilateral, desplegados por varios Estados y organizaciones internacionales, para trabajar en el campo de la seguridad cibernética. El diálogo mundial sobre el ciberespacio le dará forma a nuestro futuro como Nación y permitirá un esfuerzo como Estado para contribuir a esta discusión.

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

- Fomentar la participación en foros especializados tanto a nivel nacional como internacional con el fin de fortalecer la cooperación en ciberseguridad con otros aliados.
- Gestionar cooperación nacional e internacional que permita fortalecer los recursos y la infraestructura esencial de ciberseguridad del país a través de pasantías, capacitaciones, talleres, entre otros.

Objetivo Específico 8: Implementación, Seguimiento y Evaluación

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

La Internet es un ecosistema altamente cambiante, por lo que deben aplicarse mecanismos para mantenerse al tanto de los cambios y cerrar tan pronto como sea posible las brechas que puedan surgir como consecuencia de los cambios y nuevos riesgos.

Las deficiencias de seguridad cibernética son a menudo el resultado de la asignación inadecuada de recursos tanto humanos como financieros. En el país existen muchas capacidades para

abordar eficazmente los asuntos de seguridad cibernética, pero se requiere la definición de responsabilidad y la asignación eficiente de recursos. El concepto de un enfoque basado en la gestión del riesgo asegura que el proceso de construcción de resiliencia de la seguridad cibernética sea interactivo y se realice seguimiento.

Por tanto, para medir el progreso y el éxito de esta estrategia, el MICITT tendrá la facultad de solicitar a los diferentes actores, informes sobre el avance de las tareas que le hayan sido asignadas. Consecuentemente, como Coordinador Nacional evaluará el avance de las actividades, propondrá recomendaciones al respecto e informará anualmente al Presidente de la República y al Consejo de Gobierno sobre el avance de la implementación de la estrategia.

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

- Diseñar la metodología para el monitoreo sistemático de las acciones que operan la Estrategia Nacional de Ciberseguridad.
- Especificar en el plan de acción los mecanismos de control para darle seguimiento a los avances y la eficacia de los objetivos planteados en la presente estrategia

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

- El Comité Consultivo tendrá la responsabilidad de analizar la estrategia y emitir informes que contengan recomendaciones debidamente justificadas para efectuar las modificaciones que sean necesarias.

Capítulo 8 – Reflexiones Finales

Costa Rica iniciará el establecimiento de una base sólida para las próximas generaciones mediante la delimitación de las áreas de interés para la aplicación de la Estrategia Nacional de Ciberseguridad.

Las inversiones en soluciones de TIC no sólo continuarán mejorando la calidad de vida de los habitantes, sino que también transformarán significativamente la manera en que vemos el mundo y la forma en que interactuamos.

A través de la aplicación sistemática de las líneas de acción, se pretende que Costa Rica continúe siendo un líder en el área de la investigación y el desarrollo en TIC, como también una fuente de recursos humanos calificados en el ámbito de la seguridad cibernética y de la información.

Desde una perspectiva nacional, solo se puede implementar la seguridad cibernética a partir de un enfoque de múltiples fases y perspectivas. Esto asegurará que se desarrollen simultáneamente las áreas clave necesarias para la resiliencia cibernética nacional.

Reconociendo el hecho que la amenaza informática no es un fenómeno futuro sino una realidad actual, Costa Rica destinará los recursos necesarios en el gobierno para garantizar el éxito de esta estrategia y hará alianzas con todas las partes interesadas para avanzar en los objetivos y metas de la misma. El Poder Ejecutivo promoverá a nivel de sector público una cultura de ciberseguridad con el fin de que se establezca la asignación presupuestaria para este tema.

Glosario

Término	Definición
Academia	Institución oficial constituida por personas destacadas en las letras, las artes o las ciencias, que realizan colectivamente determinadas actividades.
Amenaza cibernética	Acción, en o a través de un sistema de información que puede resultar en un esfuerzo no autorizado para afectar negativamente la seguridad, confidencialidad, integridad o disponibilidad de un sistema o de la información que transita en éste o se almacena o procesa.
Ataque cibernético	Acción que tiene por propósito interrumpir, desactivar, destruir o controlar malintencionadamente un entorno/infraestructura informática; o destruir la integridad de los datos o el robo de información controlada. Sinónimo de ciberataque.
Brecha digital	La separación que existe entre las personas (comunidades, estados, países…) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que, aunque las tengan no saben cómo utilizarlas.
Ciberdelincuencia	Conjunto de personas y organizaciones que cometen delitos mediante la Internet o alguna red de computadoras.
Ciberespacio	Entorno complejo resultante de la interacción de personas, software y servicios en el internet por medio de dispositivos tecnológicos y redes conectadas a este, que no existe en forma física.
Ciberseguridad	Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.
Computación en la nube	Según la IUT, la computación en nube es un modelo que permite ofrecer al usuario de servicio un acceso ubicuo, práctico, a la demanda y a través de la red a un conjunto

	compartido de recursos informáticos configurables: redes, servidores, almacenamiento, aplicaciones y servicios suministrados rápidamente y liberados con una labor de gestión mínima o una interacción mínima con el proveedor de servicio.
Crimen Organizado	Es aquel grupo de tres o más personas que no fue formado de manera aleatoria; que ha existido por un periodo de tiempo; actuando de manera premeditada con el objetivo de cometer un delito punible; con el fin de obtener, directa o indirectamente, un beneficio financiero o material.
Crisis de Ciberseguridad	Un acontecimiento extraordinario que difiere de la normal y consiste grave perturbación o riesgo de perturbación de las funciones vitales de la sociedad y en el que median las tecnologías de la información y la comunicación.
Ciber-resiliencia (Cyber resilience)	La habilidad de prepararse para, adaptarse, soportar, y rápidamente recuperarse de interrupciones resultantes de ataques deliberados, amenazas o incidentes accidentales u ocurridos naturalmente.
Red profunda (Deep web)	La parte de la World Wide Web (www), que no es indexada o catalogada por medio de motores de búsquedas estándares (como google.com), e incluye páginas dinámicas o protegidas por contraseña y redes encriptadas.
Hackeo	Acceso intencional a un sistema computacional sin la autorización del usuario o dueño.
Hacker	Una persona que se interesa en comprender de forma avanzada el funcionamiento interno de un sistema, computadoras, y redes de computadoras en particular.
Hacker ético	Un hacker ético [certificado] es un profesional con habilidades que entiende y conoce como buscar debilidades y vulnerabilidades en sistemas objetivos y usa el mismo conocimiento de un hacker malicioso, pero en una manera legítima y legal para evaluar la postura de seguridad de un sistema(s) objetivo(s).
Hacktivismo	Uso de tecnologías de la computación para lograr una agenda política mediante medios ambiguamente legales y

	que generalmente obstruyen la actividad computacional en algún modo, y no causan daño o pérdida monetaria significativa.
Incidente de Seguridad Cibernética	Acción a través del uso de redes de computadores que tiene como resultado un efecto real o potencialmente adverso en un sistema de información y/o la información que existe en el mismo.
Infraestructura de información crítica	Sistemas de TI que apoyan los bienes y servicios clave en la infraestructura nacional, cuando un incidente que ocurre causa o pueda causar un grave daño a la seguridad nacional, la economía nacional o el bienestar social.
Infraestructuras críticas	Sistemas y redes de información que en ocasión de fallo podrían tener un impacto serio en la salud, seguridad física y operacional, economía y el bienestar de los ciudadanos, o el efectivo funcionamiento del gobierno y la economía del país.
Intercambio de información	Intercambio abierto y confiable de datos, ideas y contenidos entre diversos actores y tecnologías.
Prueba digital	Información electrónica almacenada o transferida en forma digital.
Punto de Intercambio de Internet	Un punto de intercambio de Internet (IXP o IX) es una infraestructura física a través de la cual los proveedores de servicios de Internet (ISP) y las redes de distribución de contenidos (CDN) intercambian tráfico local de Internet entre sus redes.
Resiliencia cibernética	Habilidad de prepararse para, adaptarse, soportar, y rápidamente recuperarse de interrupciones resultantes de ataques deliberados, amenazas o incidentes accidentales u ocurridos naturalmente. Sinónimo o equivalente a ciber-resiliencia.
Sector privado	Es la parte de la economía que no está controlada por el Estado, y está dirigida por los individuos y las empresas con fines de lucro.

Sector público	Conjunto de las organizaciones públicas. Lo integran los Poderes de la República, las instituciones autónomas, las municipalidades, los Bancos del Estado, las empresas públicas y otras instituciones públicas no estatales.
Seguridad cibernética	Conservación, a través de políticas, tecnología y educación, de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de preservar la seguridad de las personas tanto en línea como fuera de línea. Se considera análogo o sinónimo de ciberseguridad y seguridad digital
Seguridad digital	Término recomendado por OCDE en su documento de Perspectivas de la OCDE sobre la economía digital 2015. Se considera análogo o sinónimo de ciberseguridad y seguridad cibernética.
Seguridad de información	La protección de la información y sistemas de información del acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de garantizar la confidencialidad, integridad y disponibilidad.
Sociedad civil	Grupo de sujetos que, asumiendo su rol de ciudadanos, desarrollan ciertas acciones para incidir en el ámbito público.
Terrorismo	Es la dominación por medio del terror y el control que se busca a partir de actos violentos cuyo fin es infundir miedo. El terrorismo, por lo tanto, busca coaccionar y presionar a los gobiernos o la sociedad en general para imponer sus reclamos y proclamas.

Referencias

- Aguilera, R. (05 de enero de 2014). The World Post. “Costa Rica: life after Intel”. Recuperado de, http://www.huffingtonpost.com/rodrigo-aguilera/costa-rica-life-after-int_b_5246788.html
- Aguilera, R. (05 de enero de 2014). The World Post. “Costa Rica: life after Intel”. Recuperado de, http://www.huffingtonpost.com/rodrigo-aguilera/costa-rica-life-after-int_b_5246788.html
- Artículo 59. Ley de la Autoridad Reguladora de los Servicios Públicos (ARESEP), Ley N° 7593. Diario Oficial La Gaceta de la República de Costa Rica, 05 de setiembre de 1996. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=26314&nValor3=80920&strTipM=TC ´
- Asamblea General de las Naciones Unidas. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Consejo de Derechos Humanos, Decimoséptima sesión Punto 3 del orden del día. UN. Recuperado el 21 de agosto de 2015 de, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Asamblea General de las Naciones Unidas. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Consejo de Derechos Humanos, Decimoséptima sesión Punto 3 del orden del día. UN. Recuperado el 21 de agosto de 2015 de, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Bermúdez, M. (24 de agosto de 2015). Gobierno CR. “Costa Rica se potencia como un país exportador de tecnología”. Recuperado de, http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/
- Bermúdez, M. (24 de agosto de 2015). Gobierno CR. “Costa Rica se potencia como un país exportador de tecnología”. Recuperado de, http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/
- BID-OEA. (2016). Informe Ciberseguridad 2016. Banco Interamericano de Desarrollo.
- Chief Judge Stein Schjølberg (2008). REPORT OF THE CHAIRMAN OF HLEG. Norway: ITU. Recuperado el 01 de agosto de 2016 de, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
- Chief Judge Stein Schjølberg (2008). Report of the Chairman of HLEG. Norway: ITU. Recuperado el 01 de agosto de 2016 de, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
- Chief Judge Stein Schjølberg (2008). Report of the Chairman of HLEG. Norway: ITU. Recuperado el 01 de agosto de 2016 de, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

- Coalición Costarricense de Iniciativas de Desarrollo (CINDE) (2016). Invirtiendo en Costa Rica: Servicios. Costa Rica. CINDE: Costa Rica. Basado en datos del Banco Central de Costa Rica, del Fondo Monetario Internacional y Trademark.
- CONICIT-Fundación Paniamor-MICITT. Sitio web Crianza Tecnológica. [En línea]. Disponible en: http://crianzatecnologica.paniamordigital.org/index.html
- CONICIT-Fundación Paniamor-MICITT. Sitio web Crianza Tecnológica. [En línea]. Disponible en: http://crianzatecnologica.paniamordigital.org/index.htm l
- Contraloría General de la República (CGR). (2009). Normas Técnicas en Tecnologías de Información y Comunicaciones. San José: CGR. Recuperado de, https://cgrfiles.cgr.go.cr/publico/jaguar/Documentos/cgr/Sistemas/Normas_Tecnicas/Informe%20NTI_doc.pdf
- Contraloría General de la República (CGR). (2009). NTP3: Evaluación de Riesgos de Tecnologías de Información. San José: CGR. Recuperado de, https://cgrfiles.cgr.go.cr/publico/jaguar/Documentos/cgr/Sistemas/Normas_Tecnicas/Informe%20NTI_A_3.pdf
- Contraloría General de la República (CGR). (2012). R-DC-120-2012: Marco General para la Gestión de la Calidad en TIC. San José: CGR. Recuperado de, http://cgrw01.cgr.go.cr/pls/portal/docs/PAGE/PORTAL_FUNCIONARIOS_2008/SECCIONES%20FUNCIONARIOS/DOCUMENTOS/TECNOLOGIA/R-DC-120-2012%20GESTION%20CALIDAD.PDF
- Creación de la Comisión nacional de seguridad en línea, Decreto N° 36274. Diario Oficial La Gaceta de la República de Costa Rica, 09 de diciembre de 2010. Disponible en: http://www.pgrweb.go.cr/TextoCompleto/NORMAS/1/VIGENTE/D/2010-2019/2010-2014/2010/10E77/69239_83075-1.html
- Creación de la Comisión nacional de seguridad en línea, Decreto N° 36274. Diario Oficial La Gaceta de la República de Costa Rica, 09 de diciembre de 2010. Disponible en: http://www.pgrweb.go.cr/TextoCompleto/NORMAS/1/VIGENTE/D/2010-2019/2010-2014/2010/10E77/69239_83075-1.html
- Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR-CR, Decreto N° Nº 37052-MICIT. Diario Oficial La Gaceta de la República de Costa Rica, 09 de marzo de 2012. Disponible en: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832
- Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR-CR, Decreto N° Nº 37052-MICIT, Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR-CR. Diario Oficial La Gaceta de la República de Costa Rica, 09 de marzo de 2012. Disponible en: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832
- Decreto ejecutivo DE 35.205 16-04-2009 Reglamento Protección Privacidad de Comunicaciones y el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 de 18 de marzo de 2010.

- Decreto No. 7425. Diario Oficial La Gaceta de la República de Costa Rica, 09 de agosto de 1994. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp
- Deibert, R. (s.f.). Towards a cyber security strategy for global civil society? [En línea]. http://www.giswatch.org/sites/default/files/gisw_-_towards_a_cyber_security_strategy.pdf
- Foro Económico Mundial (FEM). (2014). Informe de Competitividad Global 2014-2015. Ginebra: FEM. Recuperado el 19 de agosto de 2015 de, http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf
- Foro Económico Mundial (FEM). (2014). Informe de Competitividad Global 2014-2015. Ginebra: FEM. Recuperado el 19 de agosto de 2015 de, http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf
- Fundación Karisma (traductor). (2013). Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en: https://karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf
- Fundación Karisma (traductor). (2013). Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en: https://karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf
- Green, N. y Rosinni, C. Cyber Security and Human Rights. USA: Public Knowledge. Disponible en: https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf
- GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Sitio web. [En línea]. Disponible en: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/
- GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Sitio web. [En línea]. Disponible en: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/
- http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/Normas%20t%C3%A9c%20en%20TI%20y%20comunics.pdf
- INTERPOL. (30 de enero de 2015). Capacidad policial de Costa Rica impulsada con nueva tecnología de la INTERPOL. [En línea]. Sitio web. Recuperado el 14 de septiembre de 2015 de, http://www.interpol.int/News-and-media/News/2015/N2015-008
- Kovacs, A. y Hawtin, D. (2013). Un enfoque de derechos humanos para la seguridad cibernética. [En línea]. Disponible en: http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
- Ley de Delitos Informáticos y Conexos, Ley N° 9048. Diario Oficial La Gaceta de la República de Costa Rica, 06 de noviembre de 2012. Disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&param2=1&strTipM=TC&lResultado=1&strSim=simp

- Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones
- MICITT. Boletín Contacto Digital. IXP Costa Rica: Una oportunidad estratégica. MICITT: Departamento de Sociedad de la Información. Recuperado el 2 de marzo de 2017 de, http://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574
- Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Op. Cit. PNDT. [En línea]
- Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). (2014). Indicadores Nacionales de Ciencia, Tecnología e Innovación. San Jos: MICITT.
- Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. Recuperado el 17 de agosto d 2016 de, http://micit.go.cr/images/Telecomunicaciones/pndt/PNDT-2015-2021.pdf
- Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021. San José: MICITT. Recuperado de, http://pncti.micit.go.cr/
- Ministerio de Planificación Nacional y Política Económica (MIDEPLAN). (2013). Costa Rica 2030: Plan Nacional de Desarrollo. San José: MIDEPLAN. P. 13. Recuperado de, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf
- Ministerio de Planificación Nacional y Política Económica (MIDEPLAN). (2013). Costa Rica 2030: Plan Nacional de Desarrollo. San José: MIDEPLAN. P. 30. Recuperado de, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf
- Ministerio de Planificación y Política Económica (MIDEPLAN) (2007). Manual explicativo de los organigramas del sector público costarricense. [En línea]. Recuperado el 16 de agosto de 2016 de, https://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/237a1427-b5f7-4b41-be16-8993ca567e32/organigrama_del_sector_publico.pdf?guest=true
- Ministerio de Planificación y Política Económica (MIDEPLAN). (2013). Plan Nacional de Desarrollo 2014-2018 “Alberto Cañas Escalante”. San José: MIDEPLAN. p. 438. Recuperado el 17 de agosto de 2016 de, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/cd1da1b4-868b-4f6f-bdf8-b2dee0525b76/PND%202015-2018%20Alberto%20Ca%C3%B1as%20Escalante%20WEB.pdf
- Ministerio de Planificación y Política Económica (MIDEPLAN). Op. Cit. PND. [En línea]. En el Programa Gobierno Electrónico establecido en el Plan Nacional de Desarrollo se establece la meta que reza: “50% de cumplimiento del Programa de Gobierno Electrónico (Una Estrategia Nacional de Ciberseguridad y 9 Ministerios con un Protocolo de Ciberseguridad implementado)”

- National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. [En línea]. Recuperado el 27 de agosto de 2015 de, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (actualizado diciembre 5 2014).
- NIC CR. (14 de mayo de 2015). Sitio web NIC CR. “Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)”. Recuperado el 24 de Agosto de 2015 de, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp
- North American Electric Reliability Corporation (NERC). CIP Standards. [En línea]. Recuperado el 27 de agosto de 2015 de, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Oficio 04948-SUTEL-CS-2015 del 24 de julio de 2015
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2012). Uso de TIC en educación en América Latina y el Caribe –Análisis regional de la integración de las TIC y de la aptitud digital (e-readiness) – Instituto de Estadística de UNESCO-. Recuperado de, http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-en.pdf
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2012). Cybersecurity policy making at a turning point. [En línea]. Disponible en: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
- Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos, N° 8934, Diario Oficial La Gaceta de la República de Costa Rica, 08 de setiembre de 2011. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71024&nValor3=86030&param2=1&strTipM=TC&lResultado=2&strSim=simp
- Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal, Ley N° 9135. Diario Oficial La Gaceta de la República de Costa Rica, 26 de abril de 2013. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&param2=1&strTipM=TC&lResultado=1&strSim=simp
- Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 publicado en Gaceta n° 72 15 de abril de 2010: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf
- Reglas de Heredia: Reglas mínimas para la Difusión de la Información Judicial en Internet, Seminario Internet y Sistema Judicial, Heredia, 09 de julio de 2003. [En línea]. Disponible en: http://www.iijusticia.edu.ar/heredia/Heredia_Rules.htm

- Sala Constitucional de la Corte Suprema de Justicia, de Costa Rica. (2010). Sentencia N.º 2010012790. San José: Corte Suprema. Recuperado de, http://200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_texto_sentencia.asp?nValor2=483874&tem1=013141&param7=0&lResultado=3&nValor1=1&strTipM=T&strLib=LIB
- Secretaría Técnica de Gobierno Digital. (2011). Plan Maestro de Gobierno Digital 2011-2014. San José: Secretaría Técnica de Gobierno Digital. P. 81.
- Sitio web del Poder Judicial de la República de Costa Rica. [En línea]. Disponible en: http://www.poder-judicial.go.cr/
- Sitio web Firma Digital. [En línea]. Disponible en: http://www.firmadigital.go.cr/Leyes.html
- Sitio web Sistema Costarricense de Información Jurídica. [En línea]. Disponible en: http://www.pgrweb.go.cr/scij/
- SUTEL. (6 de abril de 2010), Reglamento sobre el Régimen de Protección del Usuario Final de los Servicios de Telecomunicaciones. Disponible en: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf
- Tripton, H. y Krause, M. (2004). Handbook of Information Security Management. USA: CRC Press. Disponible: https://imcs.dvfu.ru/lib.int/docs/Networks/Security/Information%20Security%20Management%20Handbook,%20Fifth%20Edition.pdf
- Uso de TIC en educación en América Latina y el Caribe –Análisis regional de la integración de las TIC y de la aptitud digital (e-readiness) – Instituto de Estadística de UNESCO- http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-sp.pdf
- Unión Internacional de Telecomunicaciones (UIT). (2014).Actas Finales de la Conferencia de Plenipotenciarios (Busán, 2014). Busán: UIT. Recuperado el 01 de agosto de 2016 de, https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-es.pdf
- Unión Internacional de Telecomunicaciones (UIT). (2014).Actas Finales de la Conferencia de Plenipotenciarios (Busán, 2014). Busán: UIT. Recuperado el 01 de agosto de 2016 de, https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-es.pdf
- Unión Internacional de Telecomunicaciones. (2015). Informe sobre Medición de la Sociedad de la Información 2015. Ginebra: UIT. Recuperado en, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf