

Normativa a Contemplar para un Adecuado Abordaje desde los Derechos Humanos de la Ciberseguridad en Costa Rica

Un producto de Sulá Batsú

Consultora: Ana Karen Cortés Víquez
Marzo, 2023



SULÁ BATSÚ
COOPERATIVA



**GLOBAL
PARTNERS**
DIGITAL

Esta investigación fue elaborada
por **Cooperativa Sulá Batsú**
en el marco del proyecto
financiado por **Global Partners Digital**

Sulá Batsú es una Organización de la Sociedad Civil fundada en el año 2005 comprometida con fortalecer el desarrollo local y regional, mediante la apropiación de tecnologías digitales, con enfoque de género, y derechos humanos.

Normativa a contemplar para un adecuado abordaje desde los Derechos Humanos

Marzo, 2023

COORDINACIÓN

KEMLY CAMACHO JIMÉNEZ
CHRISTIAN HIDALGO GARCÍA

INVESTIGACIÓN

ANA KAREN CORTÉS VÍQUEZ

EDICIÓN DE ESTILO

NATALIA VARGAS CAMACHO

DISEÑO

NATALIA VARGAS CAMACHO

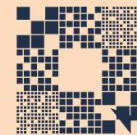
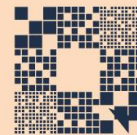


Tabla de contenido

RESUMEN EJECUTIVO DEL CONTENIDO DEL INFORME.....	5
Introducción	7
Convenios e instrumentos internacionales	9
1. Convenio sobre Ciberdelincuencia –Convenio de Budapest.....	9
3. Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108).....	10
4. Estándares Iberoamericanos de Protección de Datos	12
5. Reglas de Heredia	12
Constitución Política	13
Leyes nacionales	14
Normas conexas	25
Decretos y reglamentos.....	27
Políticas.....	30
Conclusiones.....	35



Estrategia Nacional de Ciberseguridad Costa Rica 2022

**Normativa a contemplar para un adecuado
abordaje desde los Derechos Humanos**

COOPERATIVA SULÁ BATSÚ

Elaborado por:
ANA KAREN CORTÉS VÍQUEZ

Costa Rica
Marzo, 2023

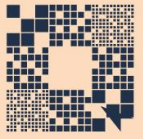
RESUMEN EJECUTIVO DEL CONTENIDO DEL INFORME

El presente estudio se enmarca en el proceso de construcción de la Estrategia Nacional de Ciberseguridad Costa Rica 2022 y pretende aportar una guía respecto de la normativa que se debe contemplar para dar un adecuado abordaje desde los Derechos Humanos.

El informe contiene normativa que ha sido identificada bajo la consideración fundamental de que todas las pautas y procesos relacionados a la ciberseguridad, deben promover no solo el bienestar de las empresas y organizaciones, sino también y, sobre todo, el de las personas. Por ello, será posible apreciar la inclusión de normativa sectorial relacionada a temas de salud, niñez y adolescencia, hacienda, economía y comercio, así como instrumentos internacionales relativos a la materia.

A la luz de este análisis normativo fue posible evidenciar temas clave que se presentan a nivel de conclusiones, así como encontrar comunes denominadores entre las políticas públicas, resultando muchas de ellas, ser omisas en cuanto a la perspectiva de género. Cabe además resaltar, la necesaria concordancia que debe suscitarse entre las diferentes normas y temas que son intrínsecos a la ciberseguridad, un ejemplo concreto de esto es la privacidad y protección de datos personales -un enfoque que suele quedar al margen-. Por lo general, los gobiernos y las empresas conciben la ciberseguridad como un tema separado de la protección de datos personales. No obstante, para controlar y afrontar las filtraciones de datos de manera eficiente, las organizaciones deben adaptar su flujo de trabajo diario combinando la ciberseguridad y la protección de datos personales, así como trabajar en estrategias que unifiquen las competencias de ambas.

Por último, el diagnóstico arroja la necesidad de trabajar bajo una visión integral de la gobernanza digital que promueva que la estrategia de ciberseguridad se formule al servicio del ser humano. Aunado a ello, se evidencia retos, como lo es construir y consolidar una comunidad cibernética en Costa Rica y que dentro del diseño de este tipo de estrategias se incluyan indicadores, metas y objetivos claros donde la sociedad civil pueda colaborar en su seguimiento e implementación a partir de sinergias estratégicas.



Introducción

La cibernsiedad como entorno social estructurado debe funcionar ineludiblemente en apego y resguardo de los derechos fundamentales, entendidos como aquel conjunto de instrumentos basados en la dignidad humana, cuya realización efectiva resulta indispensable para el desarrollo integral de la persona. Hablar de derechos humanos en la era de la cuarta revolución industrial supone que todas las normas, herramientas y políticas incorporen un enfoque que ponga al ser humano en el centro de la discusión.

El marco jurídico relacionado con ciberseguridad en Costa Rica presenta un desarrollo más amplio a partir del año 2000¹ producto del crecimiento en las conexiones de internet y el aumento de delitos cometidos por medios informáticos principalmente en el tema de fraude informático.

Para el año 2017 se lanza la *Estrategia Nacional de Ciberseguridad 2017-2021*, política que tiene entre sus metas, promover medidas de educación, prevención y mitigación frente a riesgos informáticos para generar un entorno más seguro y confiable en el país. Además, consta de 8 objetivos que en el 2021 fueron revisados a partir de una metodología que incluía 2 cuestionarios para aplicar a los actores relevantes y representantes de sectores críticos. La respuestas que arrojaron estos instrumentos forman parte del reporte “*Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica 2017*”²

¹ Ciberseguridad en Costa Rica, Capítulo 10. Hacia la Sociedad de la Información y el Conocimiento, PROSIC. Universidad de Costa Rica, 2012

² Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica 2017. Informe disponible en el siguiente enlace: <https://www.micitt.go.cr/wp-content/uploads/2022/05/Revision-de-la-Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-2017.pdf>

Por otro lado, en el Índice de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (ITU) publicado en el año 2020, Costa Rica se ubicó en el puesto número seis de América Latina, por debajo de Brasil, México, Uruguay, República Dominicana y Chile.³ Este índice mide el nivel de compromiso de cada país con la Agenda de Ciberseguridad Global de la ITU, evaluando los siguientes pilares como medidas legales, medidas técnicas, medidas organizativas, desarrollo de capacidades y cooperación.

Si bien, el país cuenta con importantes avances en materia de ciberseguridad, cabe mencionar que aún existen muchas oportunidades de mejora de cara a la formulación e implementación de la *Estrategia Nacional de Ciberseguridad 2022*.

El estudio que se presenta a continuación recoge la normativa que la citada Estrategia debe contemplar para un adecuado abordaje desde los Derechos Humanos, ello de acuerdo a la jerarquía de las normas que se divide en: 1. Convenios internacionales 2. Constitución Política 3. Leyes 4. Decretos y Reglamentos 6. Políticas.

³ Índice Global de Ciberseguridad 2020 de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés). Disponible en: <https://www.itu.int/hub/pubs/>

Convenios e instrumentos internacionales

1. Convenio sobre Ciberdelincuencia –Convenio de Budapest

Se trata de un Tratado Internacional elaborado en el marco del Consejo de Europa, pero abierto a la adhesión de países no miembros de la Unión Europea. Hasta el momento es el único instrumento internacional relativo a delitos informáticos y prueba digital.

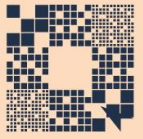
Este Convenio fue aprobado por Costa Rica mediante la Ley No. 9452 publicada el 3 de julio de 2017, y el mismo vino a complementar la ley actual número 9048 de Delitos Informáticos y conexos del título VI del Código Penal para mejorar la lucha contra la ciberdelincuencia y proteger actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como datos personales, identidad y derechos de los niños y niñas.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?pa ram1=NRTC&nValor1=1&nValor2=84360&nValor3=108815&strTipM=TC

2. Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional (Convenio de Palermo, 2000) Nº 8302

Mediante decreto ejecutivo N° 31270 de 01 de julio de 2003, Costa Rica ratifica el presente convenio. La Convención contra la Delincuencia Organizada Transnacional, es un tratado multilateral patrocinado por Naciones Unidas en contra del crimen organizado transnacional, fue adoptado en 2000. Cabe señalar que contiene 3 protocolos, sean:



- Protocolo de las Naciones Unidas para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños.
- Protocolo de las Naciones Unidas contra el Contrabando de Migrantes por Tierra, Mar y Aire.
- Protocolo de las Naciones Unidas contra la fabricación y el tráfico ilícito de armas de fuego

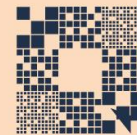
Ha de ser tomado en cuenta por contener protocolos relacionados con la trata de personas, al constituir este un fenómeno perpetrado a través redes e internet, según lo expuesto por Gilberto Zuleta, abogado especializado en derechos humanos y democratización para la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC): *“La segunda modalidad (de trata de personas) es la cacería, que lo que hace es perfilar, el tratante perfila a la víctima a través de lo que publicamos en nuestras redes sociales”*, concluyendo que, internet ofrece una mayor disponibilidad geográfica sin siquiera tener que moverse.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=50810&nValor3=54705&strTipM=TC

3. Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108)

El Convenio del Consejo de Europa -para la protección de las personas con respecto del tratamiento automatizado de los datos de carácter personal- del 28 de enero de 1981 (conocido como el Convenio 108), es admitido como el primer instrumento regional que regula el tema de Protección de Datos Personales ante el tratamiento automatizado de los mismos.



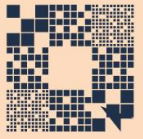
Las ventajas de ser catalogado como un país con un nivel adecuado de protección de datos personales no pueden ser menospreciadas, especialmente cuando se trata de relaciones comerciales e inversiones económicas. Sin embargo, lograr el estándar europeo y su validación consiste en una ardua labor que requiere no sólo de medidas estatales, sino de un marco regulatorio adecuado y un órgano que vele por la ejecución del mismo.

Costa Rica dio inicio al proceso de adhesión en noviembre del año 2019, tras una declaración de voluntad pública manifestada por el Presidente de la República Carlos Alvarado Quesada en el marco del *VIII Encuentro Iberoamericano de Protección de Datos Personales* cuya sede fue Costa Rica.⁴

De acuerdo con información consultada al Bureau del Consejo de Europa en el mes de agosto del año 2022, Costa Rica aún se encuentra en proceso de adhesión a dicho convenio. También fue consultada la autoridad nacional PRODHAB, donde se indicó a través de la Directora Nacional lo siguiente: “(...) *se continua en proceso, en etapas iniciales; cabe indicar que una parte esencial es que se realicen reformas legales. Cabe indicar que el próximo mes tenemos proyectada una reunión con representantes de la Unión Europea con el fin de iniciar el proceso de establecer un plan de trabajo.*”

Norma disponible en: <https://www.coe.int/es/web/data-protection/convention108-and-protocol>

⁴ Encuentro Iberoamericano de Protección de Datos 2018. Nota disponible en: <http://prodhav.go.cr/download/COMUNICADOS/Encuentrodeprotecciondedatosconcluyoconexito.pdf>



4. Estándares Iberoamericanos de Protección de Datos

Estos estándares fueron adoptados por Costa Rica y los países de la región en el año 2017 y tienen como objetivo establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

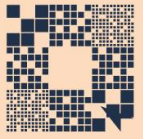
Aunado a ello, estos parámetros buscan facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región. e impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos.

Norma disponible en: <https://www.redipd.org/es/documentos/estandares-iberoamericanos>

5. Reglas de Heredia

Estas son las reglas mínimas para la Difusión de la Información Judicial en Internet. Se trata de recomendaciones aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), en julio de 2003 con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay.

Norma disponible en:
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=69198&nValor3=83022¶m2=1&strTipM=TC&IResultado=1&strSim=simp



Constitución Política

Artículo 24 Constitución Política:

Derecho a la intimidad, libertad y secreto de comunicaciones.

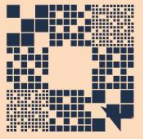
La Constitución Política de Costa Rica reconoce en su Art 24. el derecho a la intimidad, a la libertad y al secreto de las comunicaciones como derechos fundamentales. El segundo párrafo del Art. 24 establece que:

“Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.”

Actualmente, bajo el expediente N° 22.063 se encuentra en estudio por parte de la Asamblea Legislativa de Costa Rica una reforma constitucional a este artículo. El proyecto fue dictaminado en el mes de agosto del 2022 por la Comisión Especial Instalada para el Dictamen del Expediente 22063.

Norma disponible en:

https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871



Leyes nacionales

Las leyes nacionales han sido identificadas tomando en la máxima de que todos los procesos y normas relacionadas a la ciberseguridad, deben promover no solo el bienestar de las empresas y organizaciones, sino también el de las personas, sin distinción. Por ello se incluye normativa sectorial relativa a temas de salud, niñez y adolescencia, hacienda, economía y comercio, entre otras.

1. **Ley N.º 9048, Ley de Delitos Informáticos y la Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal. Diario Oficial La Gaceta de la República de Costa Rica, de 2012.**

Con la Ley 9048 de Delitos Informáticos se establecen reformas y modificaciones al Código Penal, con lo cual se establecieron nuevos tipos penales como suplantación de identidad, suplantación de páginas electrónicas e instalación o propagación de programas informáticos maliciosos.

También se contemplan otros delitos como la violación de correspondencia y datos personales, extorsión, estafa informática, daño informático y espionaje. Con lo anterior, se buscaba no sólo la protección de personas físicas, sino también de personas jurídicas.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?pa ram1=NRTC&nValor1=1&nValor2=5027&nValor3=96389&strTipM=TC



2. Ley N° 9135, Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al código penal

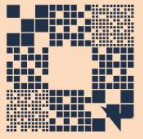
Esta reforma normativa es del año 2013 y vino a reformar los artículos relacionados a los delitos de violación de correspondencia y datos personales, suplantación de identidad, revelación de secretos de Estado, Espionaje y Seducción o encuentros con menores por medios electrónicos.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&strTipM=TC

3. Ley N° 7425, "Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones"

Como establece la Constitución, las excepciones al secreto de las comunicaciones y documentos privados son reglados por una *ley específica*, esta es la Ley sobre Registro, Secuestro, y Examen de Documentos Privados e Intervención de las Comunicaciones del año 1994. La ley trata en su primera parte del registro, secuestro o examen de documentos privados y determina que esto solamente podrá ser autorizado por los Tribunales de Justicia cuando sea absolutamente necesario en investigaciones de naturaleza penal. Además, establece que las órdenes de secuestro deben especificar, entre otras cosas, los documentos que serán objeto del registro, secuestro o examen y que la no observación de este procedimiento puede llevar a su anulación.



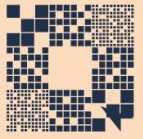
Con relación a las medidas de intervención en las comunicaciones de cualquier tipo, la ley refuerza su carácter excepcional al limitar su aplicación solamente a la investigación de un número limitado de delitos, sean: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas (Ley N° 8204 del 2001). Nuevamente, solo un juez podrá autorizar las intervenciones en las comunicaciones cuando ello pueda servir como prueba indispensable de la comisión de alguno de estos delitos.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=48269&nValor3=51389&strTipM=TC

4. Ley N° 8642, Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones publicada en el año 2008, establece a la privacidad de la información entre sus principios rectores. Esto es, la obligación de los operadores de telecomunicaciones de garantizar el derecho a la intimidad, libertad y secreto de las comunicaciones, además de la confidencialidad de la información que obtengan de los usuarios u otros operadores. La violación de la confidencialidad de las comunicaciones es considerada una infracción muy grave e implica una multa sobre los ingresos brutos del operador en el período fiscal anterior.



Esta ley contiene un capítulo completo dedicado a la privacidad de las comunicaciones y la protección de datos personales.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC#:~:text=N%C2%BA%208642&text=El%20objeto%20de%20esta%20Ley,de%20los%20servicios%20de%20telecomunicaciones

5. Ley N° 8660, Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones

Por medio esta ley se crea el *Sector Telecomunicaciones en Costa Rica* y se desarrollan las competencias y atribuciones que corresponden al Ministro Rector del Sector del Ministerio de Ambiente y Energía, que en adelante se denominará Ministerio de Ambiente, Energía y Telecomunicaciones. Se moderniza y fortalece al Instituto Costarricense de Electricidad y sus empresas y se modifica la Ley de la Autoridad Reguladora de los Servicios Públicos, N.° 7593, de 9 de agosto de 1996, para crear la Superintendencia de Telecomunicaciones, en adelante Sutel, que será el órgano encargado de regular, aplicar, vigilar y controlar el ordenamiento jurídico de las telecomunicaciones.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63786&nValor3=91177&strTipM=TC

6. Ley N°8968, Ley de Protección de la Persona frente al tratamiento de sus Datos Personales y su Reglamento

Costa Rica cuenta con una legislación bastante amplia y una Autoridad Administrativa adscrita al Ministerio de Justicia y Paz: La Agencia de Protección de Datos de los Habitantes (PRODHAB) que tiene el principal propósito garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes, a través del adecuado cumplimiento de la ley y su Reglamento No. 37554-JP y el Decreto Ejecutivo No. 40008-JP del 19 de Julio de 2006 que reforma el citado Reglamento.

Además, PRODHAB tiene como una de sus responsabilidades garantizar el derecho de acceso a la información y la rendición de cuentas. El establecimiento de un marco jurídico eficaz para la protección de datos es considerado internacionalmente como un elemento crucial para generar confianza en las relaciones que se desarrollan en línea y como medidas de salvaguarda para reducir medidas destinadas a combatir el ciberdelito. Por lo general, los gobiernos y las empresas conciben la ciberseguridad como un tema separado de la protección de datos personales. **No obstante, para controlar y afrontar las filtraciones de datos de manera eficiente. Las organizaciones deben adaptar su flujo de trabajo diario combinando la ciberseguridad y la protección de datos personales, así como trabajar en estrategias que unifiquen las competencias de ambas.**

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?pa ram1=NRTC&nValor1=1&nValor2=70975&nValor3=85989



Valga anotar que en este momento existen algunas propuestas de reforma a la Ley N° 8968, que se señalan a continuación:

I. Proyecto de reforma integral a la Ley de Protección de Datos N° 22388, presentado por el Partido Acción Ciudadana

Estado del proyecto: Este proyecto fue avalado a inicios del año 2022 por la Comisión de Económicos de la Asamblea Legislativa para ser conocido en plenario, no obstante, el cambio de legislatura impidió continuar su avance.

II. Proyecto N° 23097 denominada “Ley de Protección de Datos Personales” presentado por el Partido Liberal Progresista

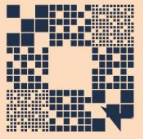
Estado del proyecto: En este momento se encuentra asignado a la Comisión de Ciencia y Tecnología y aún no cuenta con informe de Servicios Técnicos.

7. Ley N° 8131, de la Administración Financiera de la República y Presupuestos Públicos (Asamblea Legislativa de la República de Costa Rica, 2001)

Establece dos artículos relacionados con el tema de ciberseguridad, sentando responsabilidades por acciones realizadas tanto en contra del hardware como del software dentro del ámbito de aplicación del régimen económico-financiero de los órganos y entes administradores o custodios de los fondos públicos.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47258&nValor3=73503



8. Ley N° 8454, Ley de certificados, Firmas Digitales y Documentos Electrónicos y su reglamento.

Esta ley crea un aspecto fundamental en el marco normativo jurídico-informático costarricense: seguridad jurídica y técnica, debido a que se garantiza la autoría e integridad de los documentos digitales, equiparándolos a los documentos realizados en papel, lo cual se denomina equivalencia funcional.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC

9. Ley N° 7975, Ley de Información no divulgada

Su objetivo es proteger la información no divulgada relacionada con los secretos comerciales e industriales y contribuir a promover la innovación tecnológica, transferencia y difusión de la tecnología, en beneficio recíproco de productores y usuarios, de los conocimientos tecnológicos, de modo que favorezcan el bienestar socioeconómico, así como el equilibrio de derechos y obligaciones.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=41810&nValor3=74709&strTipM=TC



10. Ley N° 8934, de protección de la niñez y la adolescencia frente al contenido en internet y otros medios electrónicos.

Esta ley fue publicada el 8 de setiembre del 2011, que, si bien fue diseñada para la época en que proliferaban los “internet café”, nos interesa por el objetivo general que persigue, a saber: proteger a la niñez y la adolescencia de los riesgos que supone el uso de internet.

Merece valor el enfoque protector de esta ley que, si bien considera la necesidad de informar a la población en general de los riesgos que corren los niños, niñas y adolescentes en el ciberespacio, pone su énfasis en el establecimiento de barreras a nivel de software para minimizar su exposición ante contenido y comunicaciones que son consideradas inadecuadas para esta población.

Norma disponible en:

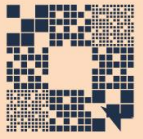
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?pa ram1=NRTC&nValor1=1&nValor2=71024&nVal

11. Reforma a los artículos 173, 173 bis Y 174, y la adición de un artículo 174 bis del código penal, Ley N° 4573, y reforma de inciso 3) y del párrafo final del artículo 61 de la Ley N° 8764, Ley General de Migración

Esta reforma a la Ley General de Migración resulta de importancia en este estudio pues los artículos que reforma refieren a la fabricación, producción o reproducción de pornografía, tenencia y difusión de material pornográfico, así como pornografía virtual y pseudo pornografía.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?pa ram1=NRTC&nValor1=1&nValor2=76102



12. Leyes de Propiedad intelectual

El conocimiento y la innovación son recursos clave en la economía global. La protección de este conocimiento a través de los Derechos de Propiedad Intelectual, se ha convertido en uno de los temas principales en el debate sobre la gobernanza de Internet. Por lo que habrá que analizar las categorías de propiedad intelectual (derechos de autor, marcas registradas, patentes, secretos comerciales, etc.) a la luz de la Estrategia Nacional de Ciberseguridad. En este sentido conviene cruzar información con:

- i. **Ley Nº 6683 de Derechos de Autor y Derechos conexos de 14 de octubre de 1982 y sus reformas.** (Publicado en la Gaceta nº 212 del 4 de noviembre de 1982):
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=3396&nValor3=80724&strTipM=TC
- ii. **Ley Nº 8020 de reforma de la Ley nº 7.978 de Marcas y signos distintivos,** del 6 de septiembre de 2000:
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=45096&nValor3=72368&strTipM=TC

13. Ley Nº 9162, Expediente digital único en salud (EDUS)

El expediente digital único en salud se creó mediante ley como una solución tecnológica para mejorar el acceso a la información por parte de los pacientes y fusionar en una única base de datos información para uso médico y administrativo. Actualmente, más de 3.842.415 personas tienen su expediente digital y pueden descargar la aplicación EDUS para sus teléfonos móviles, donde puede llevar el registro de sus citas, los medicamentos tomados y los diagnósticos confirmados.



A pesar de representar un importante avance para dar acceso fácil y práctico a las personas, en el primer trimestre del 2022 la plataforma EDUS fue hackeada⁵, generando retrasos incluso a la hora de entregar medicamentos. El análisis dado a conocer por la Presidencia Ejecutiva de la Caja Costarricense del Seguro Social señala que, a un mes de esta emergencia institucional, lograron determinar una serie de falencias en materia de seguridad tecnológica. Por eso se vuelve de vital importancia mirar los aspectos relacionados a la plataforma que alberga nuestro sistema de datos de salud y entender que el engranaje de la ciberseguridad nacional debe abordarse de manera integral.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=75700&nValor3=93998&strTipM=TC

En relación al tema de salud, se recomienda también revisar las siguientes normas conexas:

- Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N° 8968) de 2011 y su Reglamento.
- Ley de Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados (N° 8239).
- Ley Reguladora de Investigación Biomédica (N° 9234)
- Reglamento sobre el uso de estándares para datos de la Salud en Atención de Pacientes (Decreto Ejecutivo N° 39652-S-MICIT).
- Reglamento del Consentimiento Informado en la Práctica Asistencial en la Caja Costarricense de Seguro Social, aprobado por la Junta Directiva de la Caja Costarricense de Seguro Social, en el artículo 25o de la sesión 8601, celebrada el 20 de setiembre del año 2012.

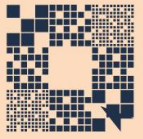
⁵ <https://delfino.cr/2022/05/hackeo-a-la-ccss-fue-un-ataque-excepcionalmente-violento-pero-no-se-vulneraron-bases-de-datos-o-sistemas-criticos>

Proyecto de ley N° 23.292 Ley de Ciberseguridad de Costa Rica

Este proyecto fue presentado en el mes de agosto del año 2022 por el Diputado José Joaquín Hernández del Partido Liberación Nacional. Es una iniciativa que pretende crear una Agencia Nacional de Ciberseguridad adscrita al Ministerio de Ciencia y Tecnología (MICITT) pero a la vez mantener el Centro de Respuesta a Incidentes de Seguridad (CSIRT-CR).

Este es un proyecto que conviene revisar, pues viene a crear una nueva burocracia en lugar de fortalecer la institucionalidad ya existente, y promueve una visión unidimensional de la ciberseguridad, limitando su utilidad únicamente al contexto de la seguridad nacional, dejando de lado el resto de las aristas que integran el marco de ciberseguridad de un país.

Por último, este proyecto viene a quitarle a todas las instituciones del sector público un 1.5% del total de sus recursos presupuestados, para financiar una nueva estructura y una vez creada, le exige a las instituciones cumplir objetivos de ciberseguridad – pero ahora con menos recursos y presupuesto que ya le quita para financiarse-.



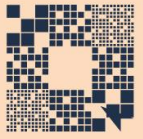
Normas conexas

1. **Art. 47 Código Civil. Derecho a la imagen**

Este numeral refiere a que la fotografía o imagen de una persona no puede ser publicada, reproducida, expuesta ni vendida en forma alguna si no es con su consentimiento. A menos que la reproducción esté justificada por la notoriedad de aquélla, la función pública que desempeñe, las necesidades de justicia o de policía, o cuando tal reproducción se relacione con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público. Las imágenes y fotografías con roles estereotipados que refuercen actitudes discriminantes hacia sectores sociales no pueden ser publicadas, reproducidas, expuestas ni vendidas en forma alguna.

2. **Art.615 Código de Comercio. Secreto bancario**

Este artículo reviste importancia ya que las cuentas corrientes bancarias son inviolables y los bancos solo podrán suministrar información sobre ellas a solicitud o con autorización escrita del dueño, o por orden de autoridad judicial competente. Se exceptúa la intervención que en cumplimiento de sus funciones determinadas por la ley haga la Superintendencia General de Entidades Financieras, o la Dirección General de Tributación autorizada al efecto.



3. Art. 27 y 41 Ley Orgánica OIJ. Carácter confidencial e interno del OIJ de investigaciones

En su artículo 27 nos indica que los agentes de investigación deberán actuar con discreción, procurando mantener en la mayor reserva su identidad; deberán además guardar absoluto secreto con respecto a las investigaciones en que intervengan, para evitar que éstas trasciendan al público. Los informes a la prensa, relativos a las investigaciones que el Organismo realiza, se darán exclusivamente a través de la Dirección General o de la oficina que señale el respectivo reglamento.

Por otro lado, el artículo 41 de la misma norma, indica que toda la información que contenga el Archivo Criminal tendrá carácter confidencial y será para uso exclusivo del organismo y de las demás autoridades.

Decretos y reglamentos

1. Decreto Ejecutivo N.º 37052-MICIT del 09 de marzo de 2012- Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR)

Este decreto viene a crear el *Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR)* que entre sus objetivos busca: Promover a nivel nacional la cultura de la seguridad cibernética e informática, coordinar acciones que permitan el mejoramiento general de la seguridad cibernética e informática. Apoyar a las autoridades administrativas y judiciales en los casos que corresponda para la investigación y procesamiento de perpetradores de delitos cibernéticos e informáticos y promover las iniciativas públicas y privadas conducentes a lograr un adecuado desarrollo del país en el campo de la seguridad de las tecnologías de la información y la comunicación, esfuerzos orientados a lograr una mayor protección del ciudadano.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC

2. Decreto N.º 36274-MICIT Comisión Nacional de Seguridad en Línea (CNSL)

Este decreto viene a crear la *Comisión Nacional de Seguridad en Línea (CNSL)* cuyos objetivos son: 1. Crear proyectos dirigidos a la sensibilización y formación de niños, niñas y adolescentes, así como a sus familias en el uso adecuado de Internet y las Tecnologías Digitales. 2. Proponer acciones que permitan prevenir los riesgos derivados del acceso indiscriminado por parte de las personas menores de edad a los contenidos inapropiados, ilícitos o lesivos para su desarrollo.

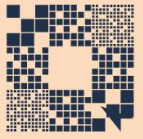


3. Promover el acceso seguro del Internet y las Tecnologías Digitales en el caso de jóvenes y adultos. 4. Diseñar proyectos para el desarrollo de estrategias que eviten el uso inadecuado de Internet y otras Tecnologías Digitales en instituciones y organizaciones públicas y privadas. 5. Revisar o proponer legislación que fortalezca los derechos de los individuos, comunidades e instituciones frente al acceso de Internet y las Tecnologías Digitales. 6. Proponer mecanismos de coordinación con toda la Administración Pública costarricense en la prevención del uso inadecuado de Internet y las Tecnologías Digitales.

Norma disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=69239&nValor3=83075&strTipM=TC

- Por otro lado, se debe trabajar a la luz del **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 y en materia de comercio electrónico observarse la reforma N° 40703 al **Reglamento a la Ley de Promoción y Competencia y Defensa Efectiva del Consumidor** (Ley N°7472) del Ministerio de Economía, Industria y Comercio (MEIC) https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=85162&nValor3=110031&strTipM=TC



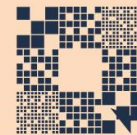
4. Decreto Ejecutivo N° 40199-MP de Apertura de Datos Públicos

(Modificado por Decreto N° 41190-MP- MIDEPLAN-MICIT-MC, de 26 de junio de 2018)

Mediante Decreto Ejecutivo N° 38994-MP-PLANMICITT del 29 de abril de 2015, denominado Fomento del Gobierno Abierto en la Administración Pública y Creación de la Comisión Nacional para un Gobierno Abierto, se crea la **Comisión Nacional por un Gobierno Abierto** con el objetivo de coordinar y facilitar la implementación del Gobierno Abierto en la Administración Pública, acompañando la formulación y evaluación de los planes nacionales de acción que sobre la materia se determinen necesarios.

Por otro lado, el Decreto Ejecutivo N° 40199-MP del 27 de abril de 2017, denominado **Apertura de Datos Públicos**, se crea la **Comisión Nacional de Datos Abiertos** y tuvo como objetivo la aplicación e implementación de la Política Nacional de Apertura de Datos de Carácter Público en el país, así como promover la transparencia gubernamental, la lucha contra la corrupción, la colaboración con la ciudadanía, la innovación y el crecimiento económico en la era digital.

Se contempla esta variable porque los datos abiertos requieren de protocolos de seguridad cibernética que protejan y promueven la características únicas que los datos abiertos presentan a la ciudadanía.



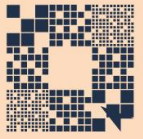
Políticas

1. Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación 2018-2027 PICTIC

La Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de los productos de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación 2018-2027, tuvo como objetivo reconocer que los estereotipos de género modelan las preferencias profesionales y los requerimientos están directamente relacionados con la permanencia de las mujeres en la formación y la capacitación profesional. No obstante, tras hacer la revisión del documento se observan muchas oportunidades de mejora en cuanto a la inclusión de acciones concretas que contemplen la perspectiva de género.

Un plan cuyo título sostenga tanto peso debería de ir más allá de las premiaciones y galardones, debería contener líneas y planes de trabajo para promover la formación, capacitación de mujeres en STEM, así como prever el impulso de cuotas paritarias en espacio de incidencia para formular políticas públicas relacionadas a Ciencia, Tecnología, Telecomunicaciones e Innovación.

Documento disponible en:
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=86602

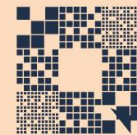


2. Plan Nacional de Ciencia, Tecnología e Innovación (2022-2027)

Este plan se expone en medio de un contexto marcado por la pandemia del Covid-19 y una coyuntura económica muy particular. Nace en una etapa en la cual nuestro país requiere más que nunca de la ciencia, la tecnología y la innovación para la reactivación económica y la generación de bienestar en un marco de solidaridad, inclusividad, equidad y desarrollo con especial énfasis en las regiones fuera de la Gran Área Metropolitana. Se plantean las acciones concretas para los próximos cinco años, reflejando la primera etapa de implementación de una visión plasmada en la actualización de la Política Nacional de Sociedad y Economía Basadas en el Conocimiento 2022-2050. Asimismo, se complementa con elementos de política pública tales como la Política Nacional para la Igualdad entre Mujeres y Hombres en la Formación, el Empleo y el Disfrute de los Productos de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación (PICTTI) 2018-2027, la Estrategia Nacional de Bioeconomía, Estrategia Económica Territorial para una Economía Inclusiva y Descarbonizada 2020-2050 en Costa Rica, el Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027, entre otros instrumentos.

Documento disponible en:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC¶m2=1&nValor1=1&nValor2=96799&nValor3=129868&strTipM=T&Resultado=2&nValor4=1&strSelect=sel#:~:text=En%20el%20PNCTI%202022%2D2027,en%20el%20Conocimiento%202022%2D2050.



3. Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0

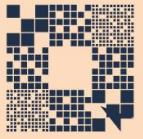
Esta estrategia buscaba transformar digitalmente las instituciones públicas y la sociedad, con el fin de potenciar el desarrollo socioeconómico del país y mejorar la calidad de vida. En el año 2020 la Contraloría General de la República emitió un informe de opiniones y sugerencias, que tenía el objetivo de aportar un abordaje integral de la transformación digital.⁶

Uno de los hallazgos más significativos que reporta La Contraloría General de la Republica es que previo a la pandemia del COVID-19 Costa Rica mantenía niveles muy incipientes en la transformación y desarrollo de procesos internos, con una planificación institucional baja relacionada a tecnologías de la información y capacitación de personas encargadas de brindar los servicios públicos. Sin embargo, durante la emergencia nacional por este virus COVID-19 el aprovechamiento de la tecnología ha sido clave para la continuidad de muchos servicios y la operativa de las instituciones, lo que ha incentivado pasos hacia la transformación digital de muchas instituciones costarricenses.

4. Plan Nacional de Desarrollo de las Telecomunicaciones. PNDT 2015 – 2021

La crisis provocada por la pandemia COVID-19 ha impactado enormemente al sistema educativo costarricense, generando la suspensión de las clases presenciales desde el 16 de marzo del 2020.

⁶Transformación Digital de la Administración Pública. Desafíos de la Gobernanza para un modelo eficiente e integrado. Informe Contraloría General de la Republica sobre la Estrategia de Transformación Digital del Bicentenario 4.0: https://cgrfiles.cgr.go.cr/publico/docs_cgr/2020/SIGYD_D/SIGYD_D_2020016855.pdf



El cierre de los centros educativos, principalmente en el sistema educativo público, ha imposibilitado que una importante cantidad de niños y jóvenes continúen recibiendo clases de manera remota producto de la falta de conectividad o del equipo tecnológico necesario para un aprendizaje virtual.

Por otro lado, La Contraloría General de la Republica en Informe (DFOE-IFR-IF-00001-2020) señaló atrasos en la ejecución de algunos proyectos del Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT 2015 – 2021) por parte de los operadores. Por ejemplo, que en el Programa 1 del Fonatel, que se llama “Hogares Conectados”, solo se ha avanzado en un 40%, a pesar de ser uno de los de mayor tiempo en ejecución. Este programa da una computadora portátil, conexión a Internet y pago mensual de la factura del servicio por cinco años a familias de escasos recursos.

Asimismo, se suponía que para el 2018 ese programa debía estar avanzado en un 42% en Territorios Indígenas, pero a la fecha de la auditoría tenía un 0% de avance.

El Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027 se encuentra en construcción.

Información disponible en:

<https://sutel.go.cr/normatica/plan-nacional-de-desarrollo-de-las-telecomunicaciones-2015-2021>

<https://www.micitt.go.cr/plan-nacional-de-desarrollo-de-las-telecomunicaciones/>

5. Proyecto Hacienda Digital

El Proyecto Hacienda Digital, se enmarca en la *“Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario”*, en una propuesta por posicionar al país y al Ministerio de Hacienda, como líder en el aprovechamiento de las tecnologías digitales y en el desarrollo de soluciones innovadoras, que permitan hacer de Costa Rica, un Estado más transparente y eficiente, así como a construir, una sociedad más cohesionada, atendiendo a los retos del futuro, de manera sostenible. El Proyecto tiene como **objetivo, dar respuesta a la necesidad de facilitar el pago de impuestos, reducir la evasión fiscal, mejorar la eficiencia del gasto público, la gestión de la deuda y la transformación de la cultura institucional**, con el fin de que permee el concepto de, concebir al ciudadano como cliente. El PHD contempla tres elementos sustanciales:

- a. Modernización de la gestión actual a una basada en procesos
- b. Sistemas de información modernos e interoperables que favorezcan su integración
 - Fortalecimiento de las capacidades y cambios en la cultura organizacional

Actualmente Hacienda Digital se encuentra en proceso, se espera que para este año 2023 empiece a funcionar en su fase inicial.

Conclusiones

1. Marco general de Derechos Humanos en Costa Rica

Según el artículo 7 de la Constitución Política de Costa Rica, los convenios internacionales tienen rango superior a las leyes. En este sentido país ha ratificado tratados de derechos humanos relevantes para la protección de la privacidad, seguridad y dignidad de la persona como lo son la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, y el Convenio sobre Ciberdelincuencia (Convenio de Budapest). No obstante, este engranaje jurídico no impide que existan grandes falencias en materia de ciberseguridad, ejemplo de esto fue el ataque por medio de hackeos, a diferentes instituciones públicas en el primer trimestre del año 2022, mismos que impidieron el funcionamiento normal de los sistemas y pusieron en riesgo la integridad y la información de muchos costarricenses.

2. Común denominador: Políticas omisas de perspectiva de género

En varias de las normas y políticas analizadas, así como en el discurso se suele indicar que la perspectiva de género se aborda como un “eje transversal” no obstante, después del análisis de la normativa es posible concluir que dicha perspectiva termina por omitirse. Con el paso del tiempo, la ciberseguridad va cobrando mayor importancia en las labores informáticas de las empresas, los Gobiernos y las vidas cotidianas de las personas. Por esta razón, es necesario emplear la perspectiva de género para que las mujeres tengan presencia en el sector y puedan desarrollar sus habilidades y carreras profesionales.

Para cerrar estas brechas de género entre mujeres y hombres que existen en el ámbito de la ciberseguridad es necesario incluir en las políticas públicas:

1. *Promoción de la educación y formación* de mujeres en carreras STEM desde los primeros años de formación.
2. *Atracción de talento desde otras disciplinas*, ya que la ciberseguridad no solo es de utilidad para profesionales o entidades relacionadas con la tecnología.
3. *Inversión en la promoción de las mujeres* en las empresas y entidades para que puedan romper con el techo de cristal.

3. El gran reto: Construir comunidad cibernética

El reto fundamental en materia de los delitos cibernéticos, descansa en los problemas de investigación, perseguibilidad y procesamiento de personas delincuentes que, aprovechando el anonimato y las posibilidades de actuación que ofrecen las TIC, logran con frecuencia alcanzar la impunidad de sus acciones.

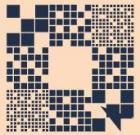
Por lo que se requiere de políticas que promuevan un componente preventivo entendido este como **educación digital** desde edades tempranas, preferiblemente mediante la inclusión de alguna materia en los programas escolares del Ministerio de Educación Pública. Y en materia represiva, Costa Rica urge de una verdadera especialización de los órganos que imparten justicia, especialmente las policías administrativas, operadores judiciales y fiscalías. Por otro lado, muchas investigaciones sobre delitos informáticos, requieren de la cooperación de la empresa privada, sin embargo, no se cuenta con protocolos de actuación ni alianzas publico privadas que viabilicen estos procesos.

Ante el reconocimiento de esta dificultad, es preciso considerar detenidamente la complejidad introducida por las tecnologías, con el objetivo de crear **mecanismos procesales y tecnológicos** capaces de responder eficazmente al fenómeno delictivo en la red, posibilitando la identificación de material ilícito, así como la recolección y almacenamiento de la prueba. Por ello, se recomienda también **dotar a las autoridades competentes de las facultades y tecnologías necesarias para perseguir e investigar los delitos cibernéticos**.

4. Indicadores, metas y seguimiento

En el informe N° DFOE-CAP-IF-00012-2021 del 30 de junio, 2021 emitido por la Contraloría General de la República, en relación a la rectoría de gobernanza digital, se determinó que no se cuenta con mecanismos de seguimiento y control para determinar el grado de implementación de los proyectos y líneas de acción de la Estrategia de Transformación Digital 2018-2022. Sabemos que esta falencia se repite en otras políticas relacionadas, lo que impide medir si se están alcanzado los objetivos propuestos.

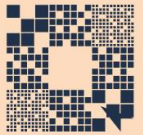
Por lo que desde sociedad civil se hace un vehemente llamado para que en la formulación de las estrategias se definan elementos propios de un plan de acción como **indicadores, metas, líneas base, estimación de recursos, responsables y periodos para la ejecución de cada proyecto, así como los riesgos que pueden afectar su implementación**.



5. Visión integral de la gobernanza digital

En el año 2012 Costa Rica se incorporó en la iniciativa multilateral Alianza para el Gobierno Abierto, la cual busca promover un estilo de gobernanza basado en la transparencia, la participación ciudadana y el trabajo colaborativo interinstitucional y ciudadano. En el marco de esta iniciativa, se firmó en el año 2015 la Declaratoria para la **Creación de un Estado Abierto en Costa Rica** por parte del Presidente de la República, el Presidente de la Asamblea Legislativa, la Presidente de la Corte Suprema de Justicia y el Presidente del Tribunal Supremo de Elecciones.

El sector público ha realizado esfuerzos en materia de gobernanza digital mediante la definición de estrategias, estándares y lineamientos para impulsar la transformación digital; así como, la creación de la Dirección de Gobernanza Digital, la Comisión de Alto Nivel de Gobierno Digital y la Comisión Nacional de Gobierno Abierto. No obstante, conviene analizar el mecanismo de Estado Abierto y ver si es posible trabajar una **Política de Estado Digital, donde exista una visión integral de la gobernanza digital desde los distintos poderes de la república y sobre todo un trabajo articulado, que disminuya la duplicidad de tareas y permita mejores resultados en el corto plazo.** Como parte de los desafíos principales a los que se enfrenta el proceso de transformación digital se requiere la adaptación del marco normativo que fomente la **interoperabilidad**, no solo a nivel técnico, sino también en términos semánticos y organizacionales, y que a su vez contribuya a la implementación de los lineamientos y estándares emitidos por la rectoría de gobernanza digital en esta materia.



6. Ciberseguridad al servicio del ser humano

La tecnología hace mucho tiempo dejó de ser una aspiración y se convirtió en una necesidad, razón por la cual Costa Rica debe fijarse metas ambiciosas, establecer mecanismos de dotación de recursos y generar programas de apoyo en coordinación con los distintos poderes, pero también con una mirada hacia los gobiernos locales, que fomente una implementación vertical y horizontal de estrategias concretas para los procesos de transformación digital.

La ciberseguridad va más allá de un tema técnico, debe tener un enfoque de derechos humanos, ya que la ciberseguridad no concierne únicamente a las empresas y los gobiernos, concierne también y, sobre todo, a las personas.