
CENTROAMÉRICA
CIBERSEGURA

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Autoría: Abdías Zambrano y Lia Hernández

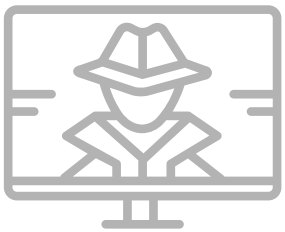
Agradecemos a nuestros colaboradores en Centroamérica y el Caribe
por su colaboración con este estudio:
Guatemala: Estefanía Román
Honduras: Eduardo Tomé
Nicaragua: Cristina Morales
Costa Rica: Yawri Carr
Dominicana: César D. Moline

Febrero 2020.

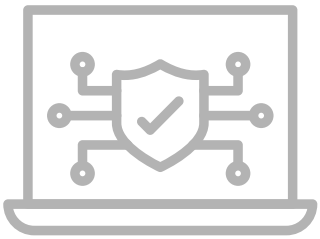
IPANDETEC CENTROAMÉRICA

IPANDETEC Centroamérica es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

Desde los inicios de la humanidad, el mal ha sido castigado una y otra vez. Primero, las costumbres judeocristianas, forjadoras de la cultura occidental, castigaban duramente los pecados contenidos en los mandamientos. Posteriormente, con el pasar de los siglos, los seres humanos alejados de la religión vieron nacer leyes y codificaciones, y con ellas los delitos o crímenes, que han ido mutando a través de los últimos 50 años a un ritmo rápido, según las características de cada sociedad.



La **ciberdelincuencia**, o los delitos en Internet, nace como resultado de los avances tecnológicos. Este método de delinquir se define como aquellos atentados a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos. Para contrarrestar esta nueva forma de delinquir se crean mecanismos de seguridad en la red mejor conocidos como seguridad cibernética o ciberseguridad.



La seguridad cibernética o **ciberseguridad** es definida por la Unión Internacional de Telecomunicaciones como el 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 ciber entorno.

Este tipo de seguridad en la red vio su máximo crecimiento en el año 2001 en el Tratado No. 185, mejor conocido como Convenio de Budapest o Convenio de Cibercriminalidad, cuando el Comité de Ministros de Consejo de Europa creó el primer tratado internacional que busca hacerle frente a los delitos informáticos o delitos en la red, mediante la cooperación entre naciones y la adecuación de la legislación nacional a los estándares internacionales.

El Convenio establece mediante sus cuatro capítulos los distintos cambios y adecuaciones que deberán hacer cada país signatario en su legislación doméstica. En su capítulo segundo se regulan los distintos delitos y adecuaciones en el plano penal que deberán adoptarse a nivel nacional como los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, los delitos informáticos, los delitos relacionados con el contenido, aquellos delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines. Este capítulo también establece formas de responsabilidad y sanción, al igual que normas a aplicar en el derecho procesal.

El capítulo tres establece los principios que deben seguirse para una mejor cooperación internacional entre signatarios, tales como la extradición, asistencia mutua, intercambio de información y los procedimientos que deben seguirse para este tipo de asistencia. Se pondera la confidencialidad y los términos de uso

Por último, el capítulo cuatro detalla su firma, proceso de adhesión, efectos del convenio y reservas, entre otros temas concernientes a la aplicación y funcionamiento del convenio.

Actualmente, el Convenio de Budapest tiene 63 países firmantes de los cuales República Dominicana, Panamá y Costa Rica son los únicos de la región centroamericana en ratificar el mismo. Guatemala, El Salvador y Honduras se encuentran en proceso de firma y adecuación de sus legislaciones. El poco o muy poco compromiso de los centroamericanos quedó demostrado en el Informe Global de Ciberseguridad, en el cual solamente Panamá fue calificado como un país con un compromiso mediano, mientras que los demás fueron categorizados como países poco comprometidos.

El mismo estudio calificó a Panamá cómo la nación más comprometida de la zona central de América, quedando en el puesto #13 de América y #97 a nivel global. Seguido de Panamá, Guatemala fue calificado con el puesto #16 de la región y #112 global. Costa Rica es el estado #18 de América y el #115 global. Los demás estados centroamericanos quedaron últimos en la lista[1].

En el marco regional, la Organización de los Estados Americanos (OEA) realizó una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, en el que el organismo reconoce la necesidad de desarrollar una cultura cibernética en las Américas; idear medidas de prevención eficaces para prever, tratar y responder ataques cibernéticos, entre otros métodos contra el cibercrimen. Igualmente se siguen los lineamientos de las recomendaciones para instaurar una red hemisférica de CSIRT y el intercambio eficaz de información entre estados miembros.

Los distintos estados de la región han introducido distintas regulaciones para contrarrestar la ciberdelincuencia y hacer más seguros sus espacios cibernéticos, sin embargo, siempre está presente el peligro de que sus legisladores propongan iniciativas que atenten a los derechos humanos.

METODOLOGÍA DE EVALUACIÓN

En este estudio analizaremos las buenas prácticas en el entorno digital de cada país centroamericano mediante la formulación de preguntas divididas entre dos temáticas: la ciberseguridad y la ciberdelincuencia.

CIBERSEGURIDAD

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Un equipo de respuesta a ataques cibernéticos es un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas; estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red; publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas. Fue creado en 1988 en respuesta al incidente del "gusano Morris". Es comúnmente conocido como CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas en español) o CERT (Computer Emergency Response Team, Equipo de Respuesta ante Emergencias Informáticas en español).

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Una estrategia de ciberseguridad o seguridad cibernética nacional es el marco que establece los distintos mecanismos de acción o planes de contingencia que deben ser seguidos e implementados por una nación con el fin de proteger a sus ciudadanos en el ámbito digital.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

Los datos personales son cualquier información concerniente a personas naturales, que las identifica o las hace identificables. Los datos personales pueden ser el nombre de la persona, su dirección, número celular, entre otros.

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

La tecnología o tecnologías de la información y la comunicación (TIC) son un conjunto de servicios de redes y aparatos que tiene como objetivo mejorar la calidad de vida del ser humano dentro de un entorno. La tecnología de la información incluye aquellas herramientas computacionales e informáticas que procesan, almacenan y recuperan información, y pueden ser una herramienta muy útil para estudiantes por ejemplo, ya que podrían beneficiarse con el flujo de información que permiten[1] acceder más allá del uso común de las redes sociales. Gracias a su creciente uso, los países han desarrollado diferentes entes gubernamentales para poder proteger a sus ciudadanos, educar a la población y sacar provecho de ella.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

La retroalimentación y el poder intercambiar información entre organismos de cada país siempre es importante para el avance de las diversas materias en las que un estado muestre interés. Esta pregunta califica la participación de agentes del Estado en reuniones o foros regionales multisectoriales sobre ciberseguridad.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Muchas veces los países y sus legisladores crean leyes que tratan la ciberseguridad; sin embargo, estas no se encuentran dentro de un capítulo llamado "Seguridad cibernética" o algo parecido. También sucede que no existe una legislación centralizada, sino diferentes leyes que regulan.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Para poder participar en encuentros en el exterior y exportar experiencias y/o conocimientos debe existir un robusto intercambio entre los diferentes sectores del país. Esta pregunta califica si entes estatales, sociedad civil, academia, entre otros actores mantienen constante comunicación mediante grupos de trabajo o coaliciones.

CIBERDELINCUENCIA

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

El Convenio de Budapest, o Convenio sobre Cibercriminalidad, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes[2].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

El Convenio sobre Cibercriminalidad enmarca los diferentes tipos penales que deben ser adheridos por cada país firmante. Sin embargo, muchos países sin firmar el convenio y por iniciativa propia, o buscando regular los ciberdelitos antes de su formal entrada a los países signatarios del Convenio proponen y sancionan iniciativas de ley que buscan incluir los delitos cibernéticos a la legislación penal.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Investigar o juzgar delitos cibernéticos requiere personal altamente calificado, con las herramientas necesarias y todos los recursos posibles para una adecuada investigación.

FORMA DE CALIFICACIÓN

Cada país calificado deberá ser analizado mediante la metodología de evaluación y las preguntas contenidas en el mismo en una infografía. Si el país obtuvo un análisis favorable, será calificado con un visto o diplosoma (también conocido como marca de verificación, verificado, marca chequeado). Esta es la calificación máxima que puede obtener en cada pregunta un país.

De obtener un análisis medianamente favorable según la metodología de evaluación, la nación será calificada con un visto o diplosoma cruzado por una raya.

Por último, de no obtener un análisis favorable por parte de la metodología, será calificado con una equis como símbolo de incorrecto.

COSTA RICA

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

En el año 2012 se crea el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR)[3], equipo constituido por expertos encargados de prevenir y responder ante ataques y peligros cibernéticos que afectaran a las instituciones gubernamentales. El CSIRT-CR está bajo el mando de la Dirección de Gobernanza Digital del MICITT.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

El país cuenta desde el año 2017 con una Estrategia Nacional de Ciberseguridad. Este documento marcó la pauta a seguir en materia de ciberseguridad en el país, vislumbrando principalmente los retos que se deben vencer y las áreas a fortalecer. El documento empezó a discutirse el mes de marzo de 2015 mediante tres mesas de discusión, orientadas por personal especializado de la OEA, cuatro talleres sectoriales y dos consultas en línea. 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[4].

3. ¿Cuenta el país con una legislación que proteja los datos personales?

Costa Rica es uno de los países pioneros en la protección y tratamiento de los datos personales de sus habitantes a nivel centroamericano mediante la ley No. 8968 "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales"[5] de 2011. Además de legislar sobre diversos mecanismos de protección a los datos personales, en esta ley se crea el ente rector órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los Habitantes (Prodhab).

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

Costa Rica cuenta con un Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) encargado dictar la política pública de ciencia, tecnología y telecomunicaciones que permita al país potenciar el aprovechamiento del conocimiento y la innovación, para priorizar y dirigir las iniciativas del sector hacia la competitividad, el bienestar y la prosperidad. [6]

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Costa Rica, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Costa Rica y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Igualmente, el Programa de Seguridad Cibernética de la Organización de Estados Americanos ha capacitado a diversos servidores públicos y a público en general en capacitaciones, tales como talleres para el desarrollo de una estrategia de seguridad digital[7].

Por último, miembros de la Asamblea Nacional de Costa Rica participaron de la XII Reunión de la Comisión Interparlamentaria de Seguridad Ciudadana y Administración de Justicia

(CISCAJ) y IX Reunión de la Comisión Interparlamentaria de Asuntos internacionales e Integración Regional del Foro de Presidentes de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL). En esta reunión participaron representantes del Proyecto de Acción Mundial Extendida Contra la Ciberdelincuencia (GLACY+ por sus siglas en inglés). Los parlamentarios firmaron una resolución donde se comprometen a redoblar esfuerzos, a favor de la respectiva integración del tema de ciberdelito y prueba electrónica, en las agendas de los parlamentos[8].

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Costa Rica tiene algunas leyes conexas que regulan la ciberseguridad[9].

- Modificación del Código de Normas y Procedimientos Tributarios, Ley No. 4755, de 3 de mayo de 1971, y sus reformas (Arts. 94-97).
- Ley General de Aduanas (Arts. 219-223).
- Administración financiera de la República y Presupuestos Públicos (Art. 111).

Disposiciones específicas:

- Acceso ilícito: Artículo 94 del Código de Normas y Procedimientos Tributarios (Ley No.4755 de 3 de mayo de 1971), Artículo 221 de la Ley General de Aduanas (No. 7557 de 20 de octubre de 1995), y Artículo 196 bis del Código Penal.
- Interceptación ilícita: Artículo 196 bis del Código Penal.
- Interferencia en los Datos: Artículo 229 bis del Código Penal.
- Interferencia en el Sistema: Artículo 229 bis del Código Penal.
- Falsificación Informática: Artículo 217 bis del Código Penal.
- Fraude Informático: Artículo 217 bis del Código Penal.
- Propiedad Intelectual: Artículo 51 de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual (No. 8039 de 12 de octubre de 2000).

Disposiciones específicas:

- Registro y Confiscación: Artículos 198 y 199 del Código Procesal Penal y Artículo 1 de la Ley Sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.
- Interceptación de Datos sobre el Contenido: Artículo 9 de la Ley Sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

En el año 2010 se crea la Comisión Nacional de Seguridad en Línea (CNSL), ente encargado de diseñar las políticas necesarias sobre el buen uso del Internet y las Tecnologías Digitales. Esta comisión está liderada por el MICITT e integrada por el Ministerio de Educación Pública, el Órgano Judicial, Ministerio de Cultura y Juventud, SUTEL, CAMTIC, diversas fundaciones, entre otros organismos. Esta comisión creó un plan de trabajo compuesto por tres ejes fundamentales: reducir el uso de medios tecnológicos en la comisión de crímenes, promover mecanismos de seguridad en línea y resguardar los menores de edad que se conectan al Internet.

Costa Rica tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos y otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC).

La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Producto de sus múltiples iniciativas contra la ciberdelincuencia, Costa Rica se convierte en el segundo país de Centroamérica en adherirse al Convenio de Budapest en el año 2017[10]. Esta adhesión los convirtió en uno de los países hub de la Acción Mundial contra los Delitos Cibernéticos Extendido (GLACY+).

La Cámara de Bancos e Instituciones Financieras de Costa Rica, la Cámara de Tecnologías de Información y Comunicación de Costa Rica y el Colegio de Abogados y Abogadas de Costa Rica se han adherido al Llamamiento de París para la confianza y la seguridad en el ciberespacio. Es de importancia aclarar que el Estado no se ha adherido[11].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Los delitos cibernéticos están tipificados en la Ley No. 9048 de Delitos Informáticos y conexos que reforma el título VI del Código Penal. Esta ley busca mejorar la lucha contra la ciberdelincuencia y protege actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como datos personales, la identidad y los derechos de los niños y niñas.

Actualmente, el parlamento costarricense mantiene en su agenda la discusión del Proyecto de Ley No. 21187 para combatir la Ciberdelincuencia, apoyado por numerosos diputados. La iniciativa busca adecuar el marco penal a las exigencias del Convenio de Budapest. Algunos de los delitos tipificados en esta reforma son: el acoso cibernético, la captación de actos o partes íntimas, ingeniería social, ciberacoso sexual, difusión de noticias falsas, acceso ilícito y abuso de dispositivos.

Uno de los principales problemas del Código Penal de Costa Rica es la correcta interpretación de los tipos penales al utilizarse un lenguaje muy técnico. Se establece cooperación de los proveedores de servicios electrónicos en el marco de una investigación de delitos informáticos y remoción de contenido en casos de acoso cibernético o pornografía infantil dentro de las primeras 24 horas posteriores a la denuncia.

Igualmente, el proyecto propone la creación de una Comisión Nacional de lucha contra la Ciberdelincuencia, que será una plataforma de enlace entre la empresa nacional y extranjera a fin de mejor y afianzar las relaciones de cooperación en la investigación criminal. Esta comisión deberá crear una Estrategia Nacional contra la Ciberdelincuencia, sugerir protocolos de actuación para la investigación de delitos informáticos, elaborar un informe en el que se analice la eficacia del ordenamiento jurídico costarricense contra la ciberdelincuencia cada dos años, entre otras responsabilidades. El texto se discute en la Comisión Permanente Especial de Seguridad y Narcotráfico.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Costa Rica creó en el año 1997 la sección de Delitos Informáticos como Unidad de Investigación Informática adscrita al Departamento de Investigaciones Criminales del Ministerio Público, resultado de la necesidad de recabar las pruebas para la atención de delitos vinculados con la tecnología[12].

EL SALVADOR

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

El Salvador, igual que sus vecinos, es poseedor de un equipo en el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (CESIRT). Este equipo es parte del Ministerio de Justicia y Seguridad Pública, y está conformado por un equipo multidisciplinario y capacitado para la investigación y reacción de eventos contra la seguridad informática.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

El Salvador no cuenta con una estrategia nacional de ciberseguridad.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

El Salvador no cuenta con una legislación que proteja los datos personales. Sin embargo, en los últimos meses se ha discutido en la Asamblea Nacional una propuesta de ley para proteger los datos de los ciudadanos y encargar a la Defensoría del Consumidor como ente rector[13]. La Ley de Acceso a la Información Pública[14] es actualmente la norma más amplia en lo que respecta al derecho a la protección de datos personales en El Salvador.

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

El Salvador cuenta con un viceministerio dedicado a la ciencia y a la tecnología, bajo el organigrama del Ministerio de Educación.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

El Salvador, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet

de El Salvador y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Por último, El Salvador fue sede de la XII Reunión de la CISCAJ y IX Reunión de la Comisión Interparlamentaria de Asuntos internacionales e Integración Regional del FOPREL. En la reunión, los parlamentarios firmaron una resolución donde se comprometen a redoblar esfuerzos, a favor de la respectiva integración del tema de ciberdelito y prueba electrónica, así mismo se comprometieron a priorizar la adhesión al convenio de Budapest, en aquellos países que aún no lo han suscrito y adaptarlo a la legislación nacional[15].

6. ¿Cuenta el país con una legislación conexa que regule la materia?

La legislación conexa en ciberseguridad salvadoreña[16] contiene las siguientes disposiciones:

Disposiciones específicas:

- Acceso ilícito: Artículos 184, 185.
- Interferencia en los Datos: Artículos 186.
- Interferencia en el Sistema: Artículo 222.
- Fraude Informático: Artículo 216.
- Pornografía Infantil: Artículo 173, Código Penal.

Derecho Procesal:
Procedimientos para la investigación de Delitos Informáticos

- Código Procesal Penal

Disposiciones específicas:

- Obtención en tiempo real de datos sobre el tráfico: Artículo 201, Código Procesal Penal.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

El Salvador tiene un capítulo nacional de la Sociedad de Internet (ISOC, por sus siglas en inglés). Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC).

La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y

fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Sus autoridades han planteado su intención de adherirse al Convenio de Budapest. En una reunión reciente del FOPREL, sus parlamentarios se comprometieron a poner en primer lugar de sus agendas la adhesión al Convenio y a legislar por la adaptación de las leyes nacionales a los estándares internacionales[17].

Por parte de la sociedad civil, la American Chamber of Commerce de El Salvador es signataria del Llamamiento de París para la confianza y la seguridad en el ciberespacio, documento con una visión de la regulación en el ciberespacio. El estado es igualmente signatario[18].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

La Asamblea Nacional salvadoreña aprobó en el año 2016 una Ley Especial contra los delitos informáticos y conexos. Esta ley tipifica distintos delitos como el acceso indebido a sistemas informáticos, violación de la seguridad de sistemas, la utilización de datos personales, las estafas informáticas, manipulación fraudulenta de tarjetas inteligentes, entre otros. Lastimosamente, esta ley a pesar de ser un gran avance en materia de ciberseguridad, solamente regula los delitos informáticos y deja en el limbo jurídico la protección de infraestructura crítica, la colaboración intersectorial en el intercambio de datos de ciberseguridad, entre otros.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

La Fiscalía General de El Salvador tiene personal especializado para responder e investigar hechos que ocurran en la red. Sin embargo, no tiene una fiscalía especializada en este tema. Los miembros de este ente son entrenados y capacitados mediante seminarios y conferencias con la ayuda de organismos internacionales[19]. Si se tratan de delitos contra la mujer, como pornografía no consentida en redes, se remite a la Unidad de Delitos Relativos a la Niñez, Adolescencia y a la Mujer de la Fiscalía General de la República. [20] Igualmente, el país cuenta con una Unidad de Investigaciones de Delitos Informáticos de la División Central de Investigaciones de la Policía Nacional Civil[21]

GUATEMALA

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Actualmente Guatemala, no cuenta con ningún equipo estatal para enfrentar ataques cibernéticos.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Guatemala cuenta con una Estrategia Nacional de Seguridad Cibernética. El documento, que data del año 2018, confeccionado por el Ministerio de Gobierno en colaboración con más de 160 representantes de los distintos sectores de la sociedad guatemalteca. El documento nace de la necesidad de contar con un plan estratégico para hacer frente a los diferentes ataques al país por la red.[22]

3. ¿Cuenta el país con una legislación que proteja los datos personales?

En el año 2009 se presentó en el Congreso de la República la Iniciativa 4090[23] que dispone aprobar la Ley de Protección de Datos Personales, que ya posee dictamen favorable emitido por la Comisión de Economía y Comercio Exterior pero que desde el año 2010 se encuentra pendiente del tercer debate y aprobación final por el Pleno del Congreso.

El Decreto Número 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública[24], fue emitido el 23 de septiembre del 2008 y entró en vigencia 20 de abril del 2009.

Es importante destacar que, a pesar que no existe una legislación específica sobre protección de datos personales, la Ley de Libre Acceso a la Información Pública actualmente es la única que regula lo referente a los datos personales y datos sensibles, así como establecer un mecanismo de protección de estos y tipifica delitos en la materia.[25]

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

El Ministerio de Gobernación, por medio del IV Viceministerio de Tecnologías de Información y Comunicaciones es el ente gubernamental especializado en tecnologías de la información.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Guatemala es miembro del Foro Mundial de Ciber Expertos (Global Forum on Cyber Expertise, o GFCE por sus siglas en inglés). El Viceministerio de Tecnología del Ministerio del Interior representa al país ante este organismo. El GFCE es una plataforma global para que países, organizaciones internacionales y empresas privadas intercambien mejores prácticas y experiencia en el desarrollo de capacidades cibernéticas. El objetivo es identificar políticas, prácticas e ideas exitosas y multiplicarlas a nivel global. Junto con socios de ONG, la comunidad tecnológica y los miembros académicos de GFCE desarrollan iniciativas prácticas para desarrollar la capacidad cibernética.

Guatemala, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Guatemala y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Además, el país pertenece al FOPREL, por lo que recientemente se reunieron con representantes de GLACY+. Esta reunión tuvo como fin el intercambio de ideas, el análisis de las ventajas de adherirse al Convenio de Budapest, el estudio de las brechas existentes y el establecimiento de compromisos en pro de la adhesión de los países miembros del FOPREL al Convenio.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

El código penal, decreto 17-73, en el artículo 274 de la literal ”A” a la “H”, se encuentra tipificado el delito de destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos, entre otros. y la ley contra la violencia sexual, explotación y trata de personas, en el cual contempla que ciertos delitos sobre indemnidad sexual, puedan ser utilizados medios incluyendo tecnológicos para ubicar o comunicarse con la víctima.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

La política de ciberseguridad no define particularmente los grupos de trabajo, pero usualmente realizan consultas entre las instituciones estatales y la sociedad civil con apoyo de organismos internacionales para discutir y aportar temas relacionados.
Guatemala tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC). La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

En el año 2016, Guatemala le expresó al Consejo de Europa su manifestación de interés en adherirse al Convenio de Budapest. Recientemente en 2019, parlamentarios reunidos con el GLACY+ se comprometieron a priorizar la adhesión al Convenio[26]. Por otro lado, es signatario del Llamamiento de París para la confianza y la seguridad en el ciberespacio publicado en el Foro de Gobernanza de Internet (IGF) celebrado en la ciudad de París en el año 2018. Por parte de la sociedad civil, el Observatorio Guatemalteco de Delitos Informáticos es signatario[27].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Actualmente, el Código Penal Decreto No. 17-33 es el único antecedente que tipifica algunos delitos informáticos como la destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación. De la misma forma, el delito de pornografía infantil no está incluido como un delito cibernético, sino dentro de la ley contra la violencia sexual, explotación y trata de personas. La no debida tipificación de los delitos informáticos puede llevar a Guatemala ser un destino de delincuentes cibernéticos. En el mes de agosto de 2019, se presentó una iniciativa ante el Congreso de Guatemala para tipificar otros 11 delitos informáticos mediante la “Ley de prevención y protección contra la Ciberdelincuencia en Guatemala”.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

No existen tribunales que sean especializados para el juzgamiento de casos sobre delitos informáticos. Sin embargo, el Ministerio Público cuenta con la Dirección de Investigaciones Criminalísticas y de técnicos informáticos especializados para procesar las evidencias digitales. Asimismo, la Policía Nacional Civil cuenta con un departamento especializado para brindar apoyo al Ministerio Público al momento de realizar investigaciones sobre posibles delitos informáticos.

HONDURAS

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Honduras no cuenta con un equipo nacional de ciberseguridad que defienda a la población de la ciberdelincuencia.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Honduras no cuenta con una política nacional cibernética que les permita asegurar el espacio cibernético de su país.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

En Honduras actualmente no existe una ley vigente que regule la protección de datos personales,

no obstante, se han hecho esfuerzos en este sentido. En el año 2015, un proyecto de Ley de Protección de Datos Personales fue impulsado por el entonces vicepresidente del Congreso Nacional, el diputado Antonio Rivera Callejas. Este proyecto se basó en el anteproyecto que fue presentado por el Instituto Nacional de Acceso a la Información Pública en el año 2013 con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID). Actualmente, el proyecto sigue en proceso de debate en el hemiciclo legislativo. El último debate se llevó a cabo en el mes de abril del año 2018. Sin embargo, este proceso se ha retrasado más de lo esperado, considerando que solo se han aprobado 19 de los 97 artículos que contiene el proyecto.

A falta de una legislación especial, los datos personales en Honduras cuentan con al menos una protección que se reconoce en la Ley del Instituto de Acceso a la Información Pública, Decreto Legislativo No. 170 – 2006. En los artículos 24 al 26 de esta ley se reconoce el Hábeas Data, la protección de los datos personales y presenta la figura del Comisionado Nacional de Derechos Humanos como una oficina facultada para incoar acciones para la protección de datos personales; además establece una prohibición en la cual ninguna persona puede solicitar a otros datos personales que puedan generar algún tipo de discriminación o poner en riesgo los derechos morales y patrimoniales de ese individuo[28].

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

Honduras, dentro de su organigrama estatal, mantiene el Instituto Hondureño de Ciencia, Tecnología y la Innovación (IHCIETI)[29], el cual forma parte del Sistema Nacional de Ciencia, Tecnología e Innovación. El IHCIETI organiza actividades que promueven la armonización de la relación gobierno-academia-sector privado, la mejora de políticas y programas, el desarrollo de las capacidades y competencias del capital humano, el establecimiento de la infraestructura necesaria para el avance de la ciencia y la tecnología, la mejora de la competitividad del sector productivo y el acceso a mercados regionales y globales.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Honduras, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Honduras y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Recientemente, participaron de una reunión de alto nivel entre el FOPREL y el GLACY+, referente al estado de ciberseguridad en el país y la posible adhesión al Convenio de Budapest.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Honduras tiene diferentes disposiciones conexas relativas a la ciberseguridad[30]:

Disposiciones específicas:

- Interferencia en los Datos: Artículos 214, Código Penal.
- Abuso de Dispositivos: Artículo 254, Código Penal.

Derecho Procesal

Procedimientos para la investigación de Delitos Informáticos:

- Código Procesal Penal

Disposiciones específicas:

- Interceptación de Datos sobre el Contenido: Artículo 223, Código Procesal Penal.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Honduras tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC). La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Honduras no es signataria del Convenio de Budapest. Sin embargo, recientemente congresistas de la comisión especial multipartidaria del Congreso Nacional para la aprobación de una ley de ciberseguridad recomendaron la adhesión al Convenio[31]. Esta recomendación es efectuada

después de una reunión entre congresistas con miembros del GLACY+ en reunión de FOPREL en San Salvador[32].

La American Chamber of Commerce in Honduras es signataria del Llamamiento de París para la confianza y la seguridad en el ciberespacio, consistente en impulsar iniciativas acerca de nuevas cuestiones cuya regulación es por ahora insuficiente, trabajando desde distintos sectores[33].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Actualmente, el Congreso hondureño se apresta a aprobar en Tercer Debate una Ley de Ciberseguridad y Medidas de Protección ante los actos de Odio y Discriminación en Internet. La iniciativa ha sido objeto de rechazo por parte de diversos sectores porque establece censura previa y pretende imponer obligaciones a los administradores de sitios web [34].
Inclusive el Relator para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), instancia de la Organización de Estados Americanos, lamentó y criticó los matices del proyecto, los cuales podrían ser claros violadores de la libertad de expresión, expresó[35].

La iniciativa legisla sobre delitos ya legislados y su regulación del odio en las redes sociales es muy general, lo que podría conllevar a interpretaciones ambiguas por parte del juzgador. La Ley continúa siendo ambigua, imprecisa y desproporcionada para determinar qué contenido digital debe entenderse como "amenaza, calumnia e injuria", debido a que en el contexto actual de Honduras esto puede ser utilizado para retirar y bloquear contenido.

Se regula la creación de un Comité Interinstitucional de Ciberseguridad, el cual será el encargado de desarrollar e implementar la Estrategia Nacional de Ciberseguridad. Sin embargo, únicamente se integrará con entidades de Gobierno. La ausencia del enfoque de múltiples partes interesadas es una debilidad, la falta de coordinación y colaboración con otros sectores como sociedad civil, sector privado, comunidad técnica y académica es un peligro, porque la Estrategia será la base para la creación de futuras políticas públicas relacionadas a ciberseguridad[36].

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Honduras tiene una Fiscalía Especial de Protección a la Propiedad Industrial y Seguridad Informática (FEPROSI, por sus siglas en español), encargada de realizar investigaciones y formular cargos a quienes se presuman hayan quebrantado la ley penal.

NICARAGUA

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Actualmente Nicaragua no cuenta con un equipo de respuesta a ataques cibernéticos

2. ¿Cuenta el país con una estrategia de ciberseguridad?

Hasta la fecha no se ha desarrollado una estrategia de ciberseguridad nacional.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

La Ley No.787, de Protección de Datos Personales[37], publicada en La Gaceta, Diario Oficial 61 el 29 de marzo del 2012, consta de proyecto 9 capítulos, distribuidos de la siguiente manera: Disposiciones Generales; Responsables de los Ficheros de Datos; Derechos de los Titulares de Datos; el cuarto Ficheros y Responsables de los Ficheros de Datos Personales; Dirección de Protección de Datos Personales; Infracciones y sanciones; Acciones de Protección de Datos Personales; Disposiciones Transitorias y Disposiciones Finales. La Ley No.787 tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa. Las disposiciones de esta Ley serán aplicables al tratamiento de los datos personales que se encuentran en los ficheros de datos públicos y privados[38].

Existen disposiciones específicas en otras leyes, tal es el caso de la Ley No.621, de Acceso a la Información Pública[39], publicada en La Gaceta No.118 del 22 de junio del 2007. Esta Ley tiene por objeto normar, garantizar y promover el ejercicio del derecho de acceso a la información pública existente en los documentos, archivos y bases de datos de las entidades o instituciones públicas, las sociedades mixtas y las subvencionadas por el Estado, así como las entidades privadas que administren, manejen o reciban recursos públicos, beneficios fiscales u otros beneficios, concesiones o ventajas. Por su parte la Ley No.842 de Protección de los Derechos de las Personas Consumidoras y Usuarias[40] establece que las personas proveedoras están obligadas a proteger la información que recibe de las personas consumidoras y usuarias y no podrán compartirla con terceros, salvo cuando estos lo autoricen de manera voluntaria y en forma expresa a través de

una adenda al contrato. Se hace también mención a la protección de los datos personales en otras leyes como la Ley No.561 General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros[41], en la cual se impone la obligación a los distintos entes financieros regulados a través de esta Ley de no brindar informes de las operaciones pasivas que celebren con sus clientes sino, según fuere el caso, a sus representantes legales o a quienes tengan poder para retirar los fondos o para intervenir en la operación de que se trate, salvo cuando lo autorice expresamente el cliente o cuando lo pidiese la autoridad judicial en virtud de causa que estuviere conociendo, mediante orden escrita en la que se debe expresar dicha causa respecto a la cual esté vinculado el depositante, ahorrador o suscriptor. En este mismo sentido, la Ley General de Las Telecomunicaciones[42] establece que se debe de garantizar y proteger la privacidad y la inviolabilidad de la correspondencia y las comunicaciones y la seguridad de la información transmitida.

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

El Consejo nicaragüense de Ciencia y Tecnología (Conicyt) y Comisión de Gobierno Electrónico de Nicaragua (GobNic) son las principales instituciones del Estados que impulsan la seguridad digital y prevención para ciberdelitos[43].

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Nicaragua, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Nicaragua y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés). En el año 2017 se realizó en Managua el TIC Forum 2017, organizado por Telefónica Business Solutions, en donde se abordó como tema “Ciberseguridad: Protegiendo sus activos digitales”.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Nicaragua tiene las siguientes disposiciones relacionadas a la ciberseguridad[44]:

- Código Penal (Art. 417 – Intrusión) Disposiciones específicas:
- Acceso ilícito: Arts. 197 y 198, Código Penal.
- Interferencia en los Datos: Art. 275, Código Penal.
- Pornografía Infantil: Art. 175, Código Penal.
- Fraude Informático: Art. 229, Código Penal.
- Falsificación Informática: Arts. 245 y 246, Código Penal.

Derecho Procesal

Disposiciones específicas:

- Interceptación de Datos sobre el Contenido: Art. 214, Código Procesal Penal.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Nicaragua tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC).

La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Nicaragua no es signatario de convenios o tratados relacionados a la materia.

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

No, pero existen otras figuras en el código penal de Nicaragua que tratan de regular la materia.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

Por el momento no se cuenta con ello. El Ministerio Público de Nicaragua es el ente encargado de investigar los supuestos delitos que suceden en el país. Sin embargo, no tiene una sección encargada de delitos informáticos. Por su parte, el Órgano Judicial no tiene tribunales especializados en delitos informáticos.

PANAMÁ

1.¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

Panamá tiene un equipo de expertos en respuesta a incidentes o ataques de expertos. Este grupo de trabajo fue creado en el año 2011 por el Ministerio de la Presidencia, bajo la supervisión de la Autoridad Nacional para la Innovación Gubernamental (ANTAI). El decreto ejecutivo No. 709 de 26 de septiembre de 2011[45] crea el CSIRT Panamá, el Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño, dotando de las facultades de investigación relacionadas con los incidentes que afecten la seguridad de los sistemas informáticos y de comunicaciones de las entidades del Estado.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

En 2013, mediante resolución No. 21[46] se aprueba la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, documento en el que se plantean diversas estrategias a seguir por el Estado panameño. En el documento se mencionan los diferentes riesgos que afronta Panamá en el uso de las TIC's y a quienes se pueden dirigir estos ataques. Así mismo dedica un apartado al desarrollo de la estrategia: protección de la información sensible de las personas, la lucha contra el delito cibernético y el uso delictivo de las TIC, desarrollo de una cultura de seguridad cibernética, entre otros.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

El 24 de octubre de 2018, la Asamblea Nacional de Diputados de Panamá aprobó en Tercer Debate el proyecto de ley No. 665 "Sobre Protección de Datos Personales", posteriormente convirtiéndose en la Ley No. 81 de 26 de marzo de 2019, Ley sobre Protección de Datos Personales. La Ley No. 81 entrará en vigencia en el año 2021.

Algunas otras leyes que regulan los datos personales son Ley No.6 de 2002 sobre Transparencia y Acceso a la Información Pública[47], Ley No.24 de 2004 que regula el servicio de información sobre el historial de crédito[48], Ley No. 51 de 2009 para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones[49] y Ley No. 3 de 2000 sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida[50].

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

El estado panameño inició su interés por la ciberseguridad en el año 2009, con la creación de la Autoridad para la Innovación Gubernamental (AIG), ente rector encargado de planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las tecnologías de la información y comunicaciones en el sector gubernamental para la modernización de la gestión pública, así como recomendar la adopción de políticas, planes y acciones estratégicas nacionales relativas a esta materia. En esta misma ley se crea el Consejo Nacional para la Innovación Gubernamental, organismo multisectorial que más adelante creará un plan para defender al país de ataques cibernéticos. Panamá no cuenta con ministerio TIC.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Panamá está representado ante el GFCE por IPANDETEC en calidad de socio. Igualmente, el país al ser miembro de la OEA, recibe apoyo y participa en talleres del Programa de Seguridad Cibernética del organismo[51]. Así mismo, forma parte de un acuerdo para adoptar los Principios de Resiliencia Cibernética desarrollados por el Foro Económico Mundial, con la ayuda de más de 50 expertos, investigadores y académicos, de todo el mundo.

Panamá, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) que la Organización de Naciones Unidas (ONU) realiza anualmente. Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Panama y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés)

6. ¿Cuenta el país con una legislación conexa que regule la materia?

Panamá cuenta con diferentes disposiciones alternas que regulan la ciberseguridad[52].

Disposiciones específicas:

- Acceso ilícito: Artículo 283 del Código Penal.
- Interceptación ilícita: Artículo 284 del Código Penal.
- Interferencia en el Sistema: Artículo 284 del Código Penal.
- Falsificación Informática: Artículos 362 y 364 del Código Penal; Artículo 61, Ley 51 de 2008. Documentos y Firmas Electrónica.
- Fraude Informático: Artículos 216 y 222 del Código Penal.
- Pornografía Infantil: Artículos 181 y 182 del Código Penal.

Derecho Procesal

Procedimientos para la investigación de Delitos Informáticos

- Código Judicial

Disposiciones específicas:

- Registro y Confiscación de datos informáticos almacenados: Artículo 2178 Código Judicial.
- Obtención en tiempo real de datos sobre el tráfico: Artículo 16 – Ley 16/2004.
- Interceptación de Datos sobre el Contenido: Artículo 16 – Ley 16/2004.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Panamá tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios y sinergia de opiniones en favor de la ciberseguridad de la nación. Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC).

La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013, que fue publicada en la Gaceta Oficial No. 27403-A del 25 de octubre del mismo año. Panamá aprobó el texto del Convenio de Budapest sin reservas ni modificaciones y depositó el instrumento de adhesión en marzo del 2014 ante la Secretaría del Consejo de Europa, convirtiéndose así en el segundo país latinoamericano en ratificar el Convenio de Budapest, después de la República Dominicana[53].

Panamá también es signataria del Llamamiento de París para la confianza y la seguridad en el ciberespacio, lanzado por el presidente de la República Francesa en ocasión de la celebración del Foro de Gobernanza de Internet de la Organización de Naciones Unidas en París, Francia. Este mecanismo invita a bordo para tratar temas de ciberseguridad y mediante un frente unido

contrarrestar su daño, no solamente a estados sino a multinacionales, empresas y asociaciones profesionales, organizaciones de la sociedad civil, entre otros sectores. La sociedad civil de Panamá, mediante diversas organizaciones, reafirman el compromiso del estado panameño al ser signatarias del Llamado[54].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Desde la fecha de ratificación del Convenio de Budapest se han introducido tres iniciativas legislativas ante la Asamblea Nacional para la adecuación de la normativa legal vigente en materia penal a lo preceptuado en el Convenio sobre Ciberdelincuencia de Budapest. El primer anteproyecto legislativo fue presentado en 2013, seguido de uno en el año 2014 y, el último y más reciente proyecto, en el mes de septiembre del 2017.

En el año 2017, el Ministerio Público presentó un paquete de reformas al Código Penal mediante un anteproyecto de ley "Que modifica y adiciona artículos al Código Penal, relacionados con el Cibercrimen", este proyecto de ley pretendía tipificar diversos cometidos en el plano digital.

Sin embargo, un mes después de su presentación ante la Asamblea Nacional, el Ministerio Público retiró el proyecto alegando que se buscaba consensuar algunas otras normas con los comunicadores sociales, que permitan presentar una nueva propuesta legislativa sobre Cibercrimen. Igualmente se propuso iniciar mesas de diálogos para consensuar las propuestas y presentarlo a la Asamblea Nacional; hasta la fecha no se ha cumplido esta propuesta y Panamá sigue sin adecuar su legislación al convenio.

El Código Penal de la República de Panamá, aprobado mediante Ley 14 del 18 de mayo de 2007, en su Título VIII, sobre los delitos contra la "Seguridad Jurídica de los Medios Electrónicos" regula los delitos contra la seguridad informática. Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas: a) ingresar o utilizar de bases de datos, red o sistemas informáticos; y, b) apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión. Además, determina ciertas conductas como circunstancias agravantes que aumentan la pena de prisión.

La carencia en la categorización adecuada de tipos penales que exigen la gran demanda de nuevas conductas que no se encuentran debidamente reglamentadas, como consecuencia no se puede cumplir con el desarrollo de investigaciones dentro procesos penales en los que se analizan delitos que utilizan alta tecnología y lograr la imposición de una sanción acorde al responsable de dicha conducta.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

El Ministerio Público de Panamá, ente investigador estatal, cuenta con una Fiscalía de Propiedad Intelectual y Seguridad Informática encargada de investigar aquellos delitos que se generen en la esfera cibernética. Por parte de las autoridades judiciales, los juzgados que recibirán investigaciones y procesos relacionados a la informática dependen del tipo de proceso que instaure el afectado. Actualmente no existen juzgados informáticos.

REPÚBLICA DOMINICANA

1. ¿Cuenta el país actualmente o en proceso con un equipo de respuesta a ataques cibernéticos?

En el año 2018 se creó el Centro Nacional de Ciberseguridad[55], en el que mediante el Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana se da respuesta a las emergencias cibernéticas. Este centro depende directamente del Ministerio de la Presidencia y fue creado mediante Decreto 230-18 del 19 de junio de 2018[56]. Este decreto establece claras responsabilidades al centro, además de las facultades de ambos equipos enfocados en el mundo cibernético y los peligros que atañen a este sector.

2. ¿Cuenta el país con una estrategia de ciberseguridad?

La Estrategia Nacional de Ciberseguridad 2018-2021 de la República Dominicana fue promulgada mediante decreto 230-18. Esta estrategia nace posterior al Programa República Digital, concebido como un conjunto de políticas y acciones que promueven la inclusión de las tecnologías de la información y de las comunicaciones en determinados procesos que tienen como eje la ciberseguridad para el desarrollo de un Estado digital.

3. ¿Cuenta el país con una legislación que proteja los datos personales?

Los datos personales en República Dominicana están protegidos específicamente por la Ley No. 172-13[57] que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Igualmente, la Constitución de la República reconoce como un derecho fundamental la intimidad y el respeto al honor personal. El ente regulador es la Superintendencia de Bancos. Esta ley sólo es aplicable a las Sociedades de Información Crediticia, dejando en completa desprotección al manejo de datos en otras entidades[58].

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

El Instituto Dominicano de las Telecomunicaciones (INDOTEL)[59] junto con la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)[60] son los entes encargados del manejo de las tecnologías de la información en el país.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Dominicana, por medio de su gobierno, academia, sociedad civil, entre otros sectores, acude y es representado anualmente en el Foro de Gobernanza de Internet (IGF) que la Organización de Naciones Unidas (ONU) realiza anualmente.

Este evento es un espacio neutral donde los actores preocupados por Internet y su futuro pueden compartir sus ideas sobre los asuntos relacionados con la política y el desarrollo de Internet, sin importar su procedencia. Este Foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de República Dominicana y el Latin American and the Caribbean Internet Governance Forum (Foro de Gobernanza de Internet de Latinoamérica y el Caribe LAC IGF, por sus siglas en inglés).

Cabe destacar que el país recibe asesoría del Global Action on Cybercrime Extended (GLACY)+, proyecto conjunto de la Unión Europea y el Consejo de Europa[61].

6. ¿Cuenta el país con una legislación conexa que regule la materia?

República Dominicana cuenta con diversos mecanismos de regulación que son los siguientes[62]:

Delitos Informáticos

- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.

Disposiciones específicas:

- Acceso ilícito: Artículo 6 de la ley 53/07.
- Interceptación ilícita: Artículo 9 de la Ley 53/07.
- Interferencia en los Datos: Artículo 10 de la Ley 53/07.
- Interferencia en el Sistema: Artículo 11 de la Ley 53/07.
- Abuso de Dispositivos: Artículo 8 de la Ley 53/07.
- Falsificación Informática: Artículo 18 de la Ley 53/07.
- Fraude Informático: Artículos 13 - 16 de la Ley 53/07.
- Pornografía Infantil: Artículo 24 de la Ley 53/07.
- Infracciones de la Propiedad Intelectual y de los Derechos afines: Artículo 25 de la Ley 53/07.

Derecho Procesal
Procedimientos para la Investigación de Delitos Informáticos

- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.

Disposiciones específicas:

- Conservación Rápida de Datos Informáticos Almacenados: Artículo 54(b) de la Ley 53/07.
- Conservación y Revelación Parcial rápidas de datos sobre el tráfico: Artículo 56 de la Ley 53/07.
- Orden de Presentación: Artículo 54(a) de la Ley 53/07.
- Registro y Confiscación: Artículo 54(b), (e), (f) y (j) de la Ley 53/07.
- Obtención en tiempo real de datos sobre el tráfico: Artículo 54(k), e (l)de la Ley 53/07.
- Obtención en tiempo real de datos sobre el contenido: Artículo 54(l) de la Ley 53/07.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

A través del CNCS se realizan mesas de trabajos sectoriales para áreas específicas como energía, telecomunicaciones, puertos aeropuertos, financiero etc.

República Dominicana tiene un capítulo nacional de la Sociedad de Internet (ISOC). Esta organización se dedica al desarrollo de internet y dentro de sus grupos de trabajo se encuentra el Observatorio sobre Ciberseguridad Global (GCO), un Grupo de Interés Especial (SIG) de la Internet Society (ISOC).

La GCO-SIG fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, la prosperidad y la seguridad en Internet, equilibrar las cuestiones de seguridad nacional con los derechos humanos y fundamentales (tales como, la privacidad, la libertad de expresión, etc.) y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Es el país signatario de convenios o tratados contra la ciberdelincuencia?

Si. La República Dominicana es signataria del Convenio sobre Ciberdelincuencia del Consejo de Europa. Fue el primer país de la región centroamericana en formar parte de este tratado internacional.

Por otro lado, se adhirió al Llamamiento de París para la confianza y la seguridad en el ciberespacio. Este Llamamiento propone una visión multisectorial de la regulación en el ciberespacio y de los grandes principios relacionados a ella. República Dominicana es uno de los 75 países firmantes, uno de los pocos de América Latina[63].

9. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

La Ley 53-07 contra crímenes y delitos de alta tecnología prevé la tipificación de los delitos cibernéticos[64]. Esta ley tipifica delitos de contenido, delitos de propiedad intelectual, delitos contra las telecomunicaciones, entre otros.

10. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

La República Dominicana cuenta con agencias especializadas como la Departamento de Investigaciones de Crímenes de Alta Tecnología (DICAT) de la Policía Nacional, encargada de ayudar al combate de la cibercriminalidad[65] en la División de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones (DNI), y una Procuraduría Especializada en Delitos de Alta Tecnología en el Ministerio Público (PEDATEC).

CONCLUSIONES

Después de analizar detalladamente la situación de ciberseguridad en la región de Centroamérica y República Dominicana, llegamos a la conclusión que nos encontramos ante un subcontinente muy inmaduro en materia de ciberseguridad.

Nuestro primer hallazgo es que muchos de los países no cuentan con una Estrategia Nacional de Ciberseguridad o un Equipo de Respuesta ante ataques cibernéticos (Csirt). Esta falencia deja indefensos a los entes estatales y ciudadanos de cada estado ante cualquier avanzada de la ciberdelincuencia.

El segundo hallazgo va muy relacionado al primero. Al no contar con lo anteriormente mencionado, es imposible obtener una hoja de ruta en cuanto a políticas públicas enfocadas en aumentar la ciberseguridad y disminuir la ciberdelincuencia. Son muy poco los países de la región que cuentan con equipos de investigadores especializados en estos temas, y mucho menos juzgados especializados en ciberdelitos. Las leyes de ciberdelincuencia no alcanzan los estándares mínimos y la gran mayoría no cuenta con legislación que proteja los datos personales de sus habitantes.

Por último, nos llamó de manera positiva la atención que muchos gobiernos a traves de sus agencias o autoridades han demostrado intenciones de mejorar y aprender de buenas practicas, lo que nos muestra que la región obtendrá notables mejorías en un futuro cercano.

ESTUDIO CENTROAMÉRICA CIBERSEGURA

	GUATEMALA	EL SALVADOR	HONDURAS	NICARAGUA	COSTA RICA	PANAMÁ	DOMINICANA
Equipo de respuesta a ataques cibernéticos	✗	✓	✗	✗	✓	✓	✓
Estrategia de ciberseguridad	✓	✗	✗	✗	✓	✓	✓
Ley de protección de datos	✗	✗	✗	✓	✓	✓	✗
Agencia o Ministerio TIC	✓	✓	✓	✓	✓	✓	✓
Participación en foros regionales multisectoriales de ciberseguridad	✓	✓	✓	✓	✓	✓	✓
Legislación conexa de ciberseguridad	✓	✓	✓	✓	✓	✓	✓
Participación en grupos de trabajo multisectorial de ciberseguridad	✗	✓	✓	✓	✓	✓	✓
Convenios o tratados de ciberseguridad	✗	✗	✗	✗	✗	✓	✓
Delitos cibernéticos	✗	✗	✗	✗	✗	✗	✓
Tribunales/agencias de investigación informática	✓	✓	✓	✗	✓	✓	✓

GUATEMALA EL SALVADOR HONDURAS NICARAGUA COSTA RICA PANAMÁ DOMINICANA

REFERENCIAS

- **[1] Unión Internacional de Telecomunicaciones.** (2018). Global Cyber Security Index 2018,- de la Unión Internacional de Telecomunicaciones. Sitio web: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- **[2] Treaty Office of Council of Europe.** Details of Treaty No. 185, de Council of Europe Sitio web: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- **[3]Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).** 2012. Decreto Ejecutivo N°37052-MICIT. -, de Sistema Costarricense de Información Jurídica. Sitio web:http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC
- **[4] Organization of American States. (2015).** OAS Supports Costa Rica in Development of a National Cyber Security Strategy. -, de Organization of American States. Sitio web: https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/15
- **[5]Asamblea Legislativa de Costa Rica. (2011)**. Ley de Protección de la persona frente al Tratamiento de sus Datos Personales. -, de Tribunal Supremo de Elecciones Sitio web: http://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf
- **[6] Portal oficial del Ministerio de Ciencia, Tecnología y Telecomunicaciones.** Sitio web: Asamblea Legislativa de Costa Rica. (2011). Ley de Protección de la persona frente al Tratamiento de sus Datos Personales. -, de Tribunal Supremo de Elecciones Sitio web: https://www.micit.go.cr/
- **[7]Autoridad Nacional para la Innovación Gubernamental. (2012).** Panamá sede internacional de Curso Especializado sobre Manejo de Incidentes de Seguridad Informática. -, de Sala de Prensa, Autoridad Nacional para la Innovación Gubernamental. Sitio web: http://www.innovacion.gob.pa/noticia/1064
- **[8]Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe. (2019).** Misión consultiva y taller sobre legislación sobre delitos cibernéticos y prueba electrónica y el Convenio de Budapest. -, de FOPREL Sitio web: http://foprel.org.ni/mision-consultiva-y-taller-sobre-legislacion-sobre-delitos-ciberneticos-y-prueba-electronica-y-el-convenio-de-budapest-2/
- **[9] Departamento de Cooperación Jurídica de la Organización de los Estados Unidos. (-)**. Legislación por país: Costa Rica. -, de Departamento de Cooperación Jurídica. Sitio web: http://www.oas.org/juridico/spanish/cyb_cos.htm
- **[10]Presidencia de la República de Costa Rica. (2017).** Costa Rica se adhiere a Convenio contra Ciberdelincuencia. -, de Presidencia de la República de Costa Rica. Sitio web: https://presidencia.go.cr/comunicados/2017/05/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/
- **[11]** https://pariscall.international/fr/supporters
- **[12]Organismo de Investigación Judicial. (-).** Sección Delitos Informáticos. -, de Organismo de Investigación Judicial Sitio web: https://sitiooij.poder-judicial.go.cr/index.php/oficinas/departamento-de-investigaciones-criminales/delitos-informaticos
- **[13]Laura Flores & Gabriel Campos Madrid. (2019).** Proponen una ley de datos y habeas data. -, de La Prensa Gráfica. Sitio web: https://www.laprensagrafica.com/elsalvador/Proponen-una-ley-de-datos-y-habeas-data-20190624-0452.html

- **[14] Asamblea Legislativa de la República de El Salvador.** Ley de Acceso a la Información Pública, Decreto Legislativo Nº. 534. Disponible en: http://www.redipd.org/legislacion/common/legislacion/elsalvador/Decreto_N534.pdf
- **[15]FOPREL. (2019).** Misión consultiva y taller sobre legislación sobre delitos cibernéticos y prueba electrónica y el Convenio de Budapest. -, de Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe Sitio web: http://foprel.org.ni/mision-consultiva-y-taller-sobre-legislacion-sobre-delitos-ciberneticos-y-prueba-electronica-y-el-convenio-de-budapest-2/
- **[16] Departamento de Cooperación Jurídica de la Organización de los Estados Americanos. (-).** Legislación por país: El Salvador. -, de Departamento de Cooperación Jurídica Sitio web: http://www.oas.org/juridico/spanish/cyb_slv.htm
- **[17]Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe. (2019).** Misión consultiva y taller sobre legislación sobre delitos cibernéticos y prueba electrónica y el Convenio de Budapest. -, de FOPREL Sitio web: http://foprel.org.ni/mision-consultiva-y-taller-sobre-legislacion-sobre-delitos-ciberneticos-y-prueba-electronica-y-el-convenio-de-budapest-2/
- **[18]** https://pariscall.international/fr/supporters
- **[19]Oficina de las Naciones Unidas contra la Droga y el Delito. (-).** La Fiscalía General de la República de El Salvador Capacitada en Investigación de Cibercrimen Gracias al Apoyo de UNODC. -, de Oficina de las Naciones Unidas contra la Droga y el Delito Sitio web: https://www.unodc.org/ropan/es/IndexArticles/Cybercrime/la-fiscalia-general-de-la-republica-de-el-salvador-capacitada-en-investigacion-del-cibercrimen-gracias-al-apoyo-de-unodc.html
- **[20]Beatriz Calderón. (2018).** "Si hay acoso por cualquier red social, no borre el contenido, denuncie": FGR. -, de La Prensa Gráfica Sitio web: https://www.laprensagrafica.com/elsalvador/Si-hay-acoso-por-cualquier-red-social-no-borre-el-contenido-denuncie-FGR-20180424-0036.html
- **[21] Ministerio de Justicia y Seguridad Pública. (-).** Policía captura a sujeto acusado de pornografía. -, de Ministerio de Justicia y Seguridad Pública Sitio web: http://www.pnc.gob.sv/portal/page/portal/informativo/novedades/noticias/Polic%EDa%20captura%20a%20sujeto%20acusado%20de%20pornograf%EDa#.XYpXcSgzbIV
- **[22]Ministerio de Gobierno. (2018).** Estrategia Nacional de Seguridad Cibernética. -, de Ministerio de Gobierno. Sitio web:http://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf
- **[23] Congreso de la República de Guatemala.** Iniciativa 4090, Ley de Protección de DatosPersonales. Disponible en: https://www.congreso.gob.gt/wp-content/plugins/paso-estadoincidencias/includes/uploads/docs/988.pdf
- **[24]Congreso de la República de Guatemala.** Decreto Número 57-2008, Ley de Acceso a la
- Información Pública. Disponible en: https://www.oas.org/juridico/pdfs/mesicic4_gtm_acceso.pdf
- **[25]Sara Fratti. (2019).** Estudio Centroamericano de Protección de Datos, Guatemala. -, de IPANDETEC Sitio web: https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Guatemala.pdf
- **[26]Council of Europe. (2019).** GLACY+: Advisory Mission on Cybercrime Legislation in FOPREL countries. -, de Council of Europe. Sitio web: https://www.coe.int/en/web/cybercrime/-/glacy-advisory-mission-on-cybercrime-legislation-in-foprel-countries
- **[27]** https://pariscall.international/fr/supporters
- **[28]Eduardo Tomé. (2019).** Estudio Centroamericano de Protección de Datos, Honduras. -, de IPANDETEC Sitio web:https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Honduras.pdf
- **[29] Instituto Hondureño de Ciencia, Tecnología y la Innovación. (-).** Sobre nosotros. -, de Instituto Hondureño de Ciencia, Tecnología y la Innovación. Sitio web:https://senacit.gob.hn/static/sobre-nosotros.html

- **[30] Departamento de Cooperación Jurídica de la Organización de los Estados Americanos. (-).** Legislación por país: Honduras. -, de Departamento de Cooperación Sitio web: http://www.oas.org/juridico/spanish/cyb_hnd.htm
- **[31]Redacción. (-).** Ley de Ciberseguridad se adheriría a Convenio de Budapest sobre ciberdelincuencia. -, de Cholusat Sur Sitio web: http://cholusatsur.com/noticias/ley-de-ciberseguridad-se-adheriria-convenio-de-budapest-sobre-ciberdelincuencia/
- **[32]Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe. (2019).** Misión consultiva y taller sobre legislación sobre delitos cibernéticos y prueba electrónica y el Convenio de Budapest. -, de FOPREL. Sitio web: http://foprel.org.ni/mision-consultiva-y-taller-sobre-legislacion-sobre-delitos-ciberneticos-y-prueba-electronica-y-el-convenio-de-budapest-2/
- **[33]** https://pariscall.international/fr/supporters
- **[34]OBSERVACOM. (2019).** Organizaciones sociales rechazan proyecto de Ley de ciberseguridad y contra el odio en Internet en Honduras. -, de Observatorio Latinoamericano de Regulación Medios y Convergencia. Sitio web: https://www.observacom.org/organizaciones-sociales-rechazan-proyecto-de-ley-de-ciberseguridad-y-contra-el-odio-en-internet-en-honduras/
- **[35] Robert Martín García. (2018).** Edison Lanza "un régimen de censura privada establece ley que regulará Internet.".Honduras, de El Heraldo. Sitio web: https://www.elheraldo.hn/pais/1150315-466/edison-lanza-un-r%C3%A9gimen-de-censura-privada-establece-ley-que-regular%C3%A1-internet
- **[36] IPANDETEC. (2018).** Amenazas a la libertad de expresión en línea en Honduras. -, de Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC). Sitio web: https://www.ipandetec.org/2018/02/15/amenazas-la-libertad-de-expresion-en-linea-en-honduras/
- **[37] Asamblea Nacional de la República de Nicaragua.** La Ley 787, Ley de Protección de Datos Personales. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d
- **[38] Roger Cajina. (2019).** Estudio Centroamericano de Protección de Datos, Nicaragua. -, de IPANDETEC Sitio web: https://www.ipandetec.org/wp-content/uploads/2019/03/EDP_Nicaragua-2.pdf
- **[39] Asamblea Nacional de la República de Nicaragua.** Ley número 621, Ley de Acceso a la Información Pública. Disponible en:http://deviunn.asamblea.gob.ni/iunp/docspdf/gacetas/2012/3/g61.pdf
- **[40] Asamblea Nacional de la República de Nicaragua.** La Ley No. 787, Ley de Protección de Datos Personales. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d
- **[41] Asamblea Nacional de la República de Nicaragua.** Ley 561, Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros. Disponible en: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/1A3ECC04110514C9062570F300755895?OpenDocument
- **[42] Asamblea Nacional de Nicaragua. (-).** Marco legal. -, de TELCOR Sitio web: https://www.telcor.gob.ni/MarcoLegal.asp?Accion=VerRecurso&REC_ID=177
- **[43]Cristina Morales. (2019).** Derechos Digitales en Nicaragua 2018. -, de IPANDETEC Sitio web: https://www.ipandetec.org/2019/01/11/derechos-digitales-en-nicaragua-2018/
- **[44]Departamento de Cooperación Jurídica. (-).** Legislación por país: Nicaragua. -, de Organización de los Estados Americanos Sitio web: http://www.oas.org/juridico/spanish/cyb_nic.htm

- **[45] Ministerio de la Presidencia. (2011).** Decreto Ejecutivo No. 709 de 26 de septiembre de 2011. Por el cual se crea el "CSIRT PANAMA" Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño. -, de Gaceta Oficial Sitio web:https://www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf
- **[46]Consejo Nacional para la Innovación Gubernamental. (2013).** Resolución No. 21. Por la cual se aprueba el documento titulado: Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. -, de Gaceta Oficial Sitio web:https://sherloc.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf
- **[47] Asamblea Nacional de Panamá,** Ley No. 6 del 22 de enero de 2002, Que dicta normas para la transparencia en la gestión pública establece la acción de Habeas Data y dicta otras disposiciones. Disponible en:http://www.mef.gob.pa/es/transparencia/Documents/Ley%20No%206%20de%2022%20enero%20de%202002.pdf
- **[48] Asamblea Nacional de Panamá,** Ley No. 24 del 22 de mayo de 2002, Que regula el servicio de información sobre el historial de crédito de los consumidores o clientes. Disponible en:http://www.legalinfopanama.com/legislacion/00297.pdf
- **[49] Asamblea Nacional,** Ley N. 51 de 18 de septiembre de 2009 que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones. Disponible en: https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf
- **[50] Asamblea Nacional,** Ley General No. 3 de 5 enero de 2000 sobre las infecciones de transmisión sexual, el virus de la inmunodeficiencia humana y el sida. Disponible en: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127734.pdf
- **[51] Autoridad Nacional para la Innovación Gubernamental. (2012).** Panamá sede internacional de Curso Especializado sobre Manejo de Incidentes de Seguridad Informática. -, de Autoridad Nacional para la Innovación Gubernamental. Sitio web: http://www.innovacion.gob.pa/noticia/1064
- **[52]Departamento de Cooperación Jurídica. (-).** Legislación por país: Panamá. -, de Organización de los Estados Americanos. Sitio web: http://www.oas.org/juridico/spanish/cyb_pan.htm
- **[53]Sara Fratti. (2018).** Panamá: Un país con la necesidad de una legislación sobre cibercrimen. -, de IPANDETEC Sitio web: https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf
- **[54]Appel de Paris.** Les soutiens. Sitio web: https://pariscall.international/fr/supporters
- **[55] Inicio - Centro Nacional de Ciberseguridad.** Sitio web: https: https://cncs.gob.do
- **[56] Decreto 230-18 del 19 de junio de 2018**. Sitio web: https://indotel.gob.do/media/10605/decreto-230-18.pdf
- **[57] Ley No. 172-13** que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Sitio web: https://indotel.gob.do/media/6200/ley_172_13.pdf
- **[58] República Digital.** ¿Por qué es importante defender nuestros datos personales? Sitio web: https://republicadigital.gob.do/blog/proteccion-datos-personales/
- **[59] Instituto Dominicano de las Telecomunicaciones.** Sitio web: https://www.indotel.gob.do/
- **[60] Oficina Presidencial de Tecnologías de la Información y Comunicación.** Sitio web: https://optic.gob.do/
- **[61] Policía Nacional de República Dominicana. (2019).** Ejercemos acciones contra la ciberdelincuencia para fortalecer el clima de tranquilidad ciudadana. Sitio web: http://www.policianacional.gob.do/noticias/ejercemos-acciones-contra-la-ciberdelincuencia-para-fortalecer-el-clima-de-tranquilidad-ciudadana/

- **[62]Departamento de Cooperación Jurídica de la Organización de los Estados Unidos. (-).** Legislación por país: República Dominicana. -, de Departamento de Cooperación Jurídica. Sitio web: http://www.oas.org/juridico/spanish/cyb_repdom.htm
- **[63]Centro Nacional de Ciberseguridad. (2019).** La República Dominicana se adhiere al Llamado de París para la confianza y la seguridad en el ciberespacio. Sitio web:https://cncs.gob.do/la-republica-dominicana-se-ha-adhiere-al-llamado-de-paris-para-la-confianza-y-la-seguridad-en-el-ciberespacio/
- **[64] Organización de Estados Americanos. (2007).** Ley No. 53-07 sobre crímenes y delitos de alta tecnología. Sitio web: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf
- **[65] Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología.** Sitio web: http://dicat.gob.do/

IPANDETEC
CENTROAMÉRICA