# Cooperación en Ciberseguridad y Ciberdefensa Hemisférica

# Estructuras de los Países de las Américas


Resumo

Estudio de Área Estratégica, en el Sector Cibernético (EAE - CIBER) involucrando aspectos de Ciberseguridad y Ciberdefensa de 26 (veintiséis) países del continente americano



**Autor**

**ALEXANDER EDUARDO VICENTE FERREIRA**

CORONEL DEL EJÉRCITO BRASILEÑO

Profesor de Ciberseguridad y Ciberdefensa

del Colegio Interamericano de Defensa (CID)

Y

OFICIALES DEL CURSO DE COMANDO Y ESTADO MAYOR CONJUNTO DE LA

ACADEMIA DE DEFENSA MILITAR CONJUNTA DE ECUADOR

# INTRODUCCIÓN

El alcance principal de este trabajo es presentar un Estudio de Área Estratégica, en el Sector Cibernético (EAE - CIBER) involucrando aspectos de Ciberseguridad y Defensa Cibernética de 26 (veintiséis) países del continente americano.

## Antecedentes

El 26 de enero de 2023, la Junta Interamericana de Defensa (JID), con sede en Washington, Distrito de Columbia (DC), en los Estados Unidos de América (EE. UU.), remitió al Colegio Interamericano de Defensa (CID) Oficio No. 6291/ SSA/DST/JID con la solicitud de que se realice una investigación académica, que abarque algunos países del continente americano, sobre la Estructura de Cooperación en Ciberdefensa Hemisférica.

Entre los aspectos a observar se sugirieron dos áreas focales, a saber:

a. El. Estudio comparativo de las capacidades de Ciberdefensa de los países de las Américas; y

b. los aspectos relevantes de la cooperación existente entre las estructuras hemisféricas de Ciberdefensa.

El trabajo fue planificado, coordinado y guiado por el Coronel ALEXANDER EDUARDO VICENTE FERREIRA (alexander.ferreira@iadc.edu), del Ejército de Brasil, Profesor de Seguridad Cibernética del CID y contó con la participación y colaboración, en investigaciones de campo y en fuentes abiertas, por los Oficiales cursantes del Curso de Comando y Estado Mayor Conjunto de la Academia Militar Conjunta de Defensa (ADEMIC), de las Fuerzas Armadas del Ecuador.

Se trata, por tanto, de una investigación académica inicial, utilizando fuentes abiertas, sitios de internet, en literatura accesible, disponible y con Clasificación OSTENSIVA, con el objetivo de contribuir con el conocimiento de los datos sobre el tema, su intercambio a todos los Organismos/Estructuras/ Países interesados, y que seguramente se actualizarán constantemente.

## Estructura de trabajo

Este trabajo estudió 26 (veintiséis) países de las Américas y se dividió en 03 (tres) partes, siguiendo el orden alfabético de los países:

1) **América del Norte**, con 03 (tres) países: **Canadá, Estados Unidos y México**;

2) **Centroamérica y el Caribe**: con 09 (nueve) países: **Barbados, Costa Rica, Cuba, El Salvador, Guatemala, Haití, Honduras, Panamá, República Dominicana**; y

3) **América del Sur**: con 14 (catorce) países: **Argentina, Estado Plurinacional de Bolivia, Brasil, Chile, Colombia, Ecuador, Guyana, Guayana Francesa, Paraguay, Perú, Surinam, Trinidad y Tobago, Uruguay y Venezuela.**

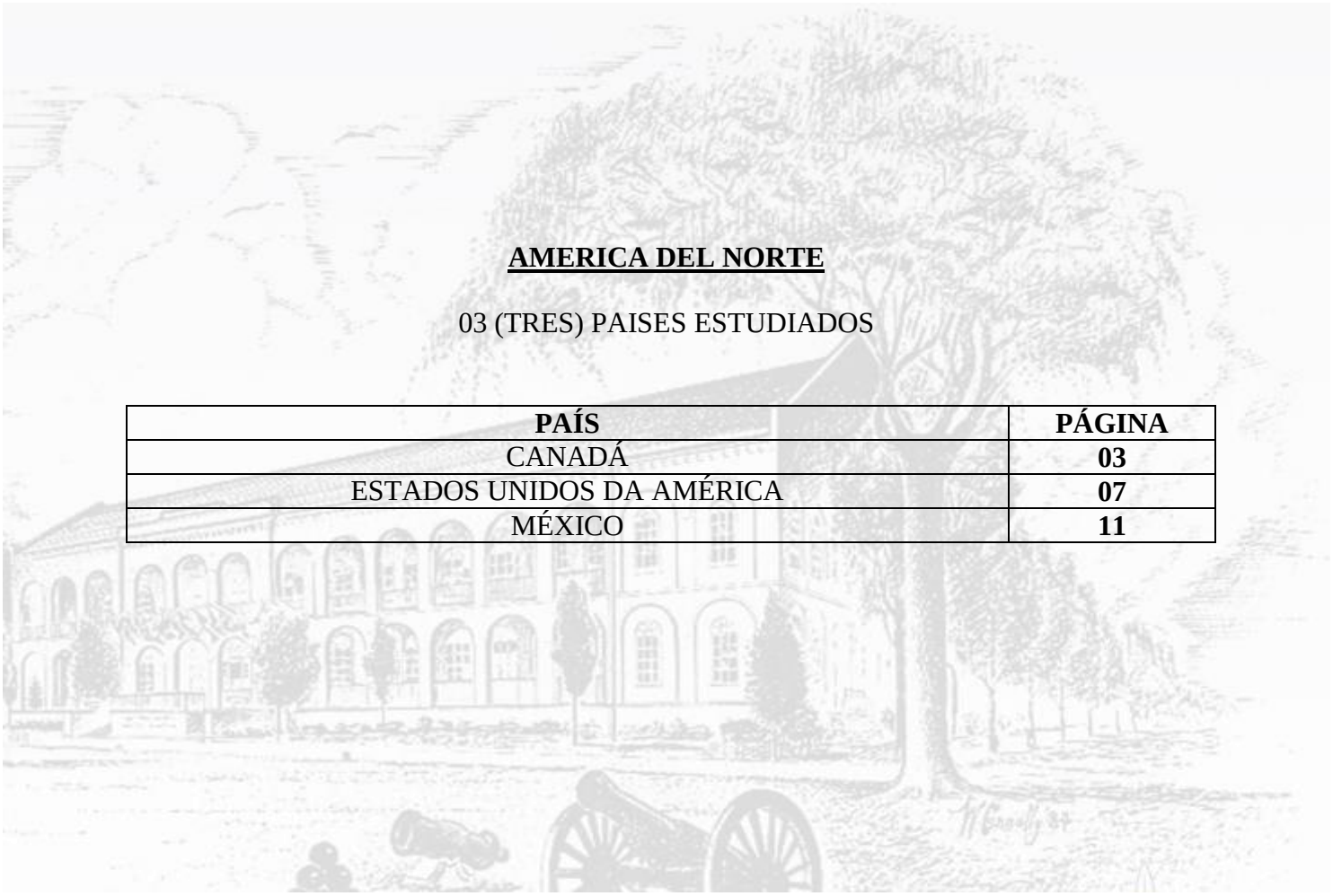
Para cada País se abordan las Generalidades, los datos de las Fuerzas Armadas, su estructura de Ciberseguridad, su Estructura de Ciberdefensa y una breve Conclusión Parcial.

Las Referencias Bibliográficas, al ser extensas, permanecerán disponibles, enumeradas por separado, en un enlace proporcionado al final del documento.

Todo el contenido de la obra, escrito originalmente en español, ha sido traducido y está disponible en ESPAÑOL, INGLÉS y PORTUGUÉS. Cualquier comentario, sugerencia, corrección, actualización o aporte podrá ser remitido al correo electrónico indicado anteriormente, o a la JID a través de los canales correspondientes.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu



## AMERICA DEL NORTE

03 (TRES) PAISES ESTUDIADOS





Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# CANADÁ

## Generalidades

Canadá un país desarrollado, es el segundo país más grande del mundo por área total de aproximadamente 9,98 millones de kilómetros cuadrados, ubicado en América del Norte, limitando al norte con el océano Ártico, al este con el océano Atlántico, al oeste con el océano Pacífico y al sur con Estados Unidos. El país es conocido por su apertura, su enfoque en los valores democráticos y su compromiso con el bienestar social y económico de sus ciudadanos. Su capital es Ottawa y su población está alrededor de 38 millones de habitantes, que habitan 10 provincias y tres territorios (Canadá travel, 2023).

Sus idiomas oficiales son el inglés y francés, su forma de gobierno es una Monarquía Parlamentaria federal, su rey es Carlos III, su Gobernadora general es Mary Simon y como primer ministro esta Justin Trudeau. Canadá es uno de los países más desarrollados siendo la octava economía más grande del mundo, entre sus principales recursos naturales están el petróleo, gas natural, minerales, madera y agua dulce, su producto interno bruto al 2022 fue de 2,14 billones USD, el mismo que crece en un 3,4 % anual y Per cápita de 54.966,5, su moneda el dólar canadiense, teniendo un índice de desarrollo humano (IDH) de 0,936 punto al 2021 (Banco Mundial, 2023).

## Datos de las Fuerzas Armadas

Las Fuerzas Armadas canadienses son una institución unificada consta de elementos marinos, terrestres y aéreos denominados como la Royal Canadian Navy (RCN), el Canadian Army y la Royal Canadian Air Force (RCAF) con un aproximado de 72.000 efectivos, de lo que podemos inferir que, son pequeñas por su tamaño en extensión, con una cantidad de hombres de pocos efectivos con relación a otras potencias y a los países en desarrollo como el Ecuador (Banco Mundial, 2023).

El Ejército de Canadá constituye la mayor parte de las Fuerzas Armadas canadienses, con 35 000 soldados. Las unidades de las fuerzas regulares tienen 19 500 soldados a tiempo completo, la Reserva del Ejército cuenta con unos 16 000 a tiempo parcial, existiendo además 4 100 empleados civiles (Banco Mundial, 2023).

Las Fuerzas Armadas canadienses han participado en varios conflictos fuera de su territorio, así: en la Primera Guerra Mundial (1914-1918) participó como parte del Imperio Británico y contribuyó con un gran número de tropas y recursos. La Batalla de Vimy Ridge en 1917 es especialmente notable por la destacada actuación de las fuerzas canadienses (Gavasa, 2020). En la Segunda Guerra Mundial (1939-1945), Canadá jugó un papel importante como parte de los Aliados, y sus fuerzas participaron en varias campañas cruciales, incluyendo la Batalla del Atlántico y el Día D en Normandía (Bertram, 2008); en la Guerra de Corea (1950-1953), envió tropas y apoyo militar para luchar contra la invasión comunista de Corea del Sur durante la Guerra de Corea, como parte de las fuerzas de la ONU; en la Guerra de Afganistán (2001-2014), desplegó tropas en Afganistán después de los ataques del 11 de septiembre de 2001 para apoyar la Operación Libertad Duradera y luchar contra el terrorismo (Libro Blanco de la Defensa de Canadá de 1994, 2023). Así mismo, participa en misiones de paz de la ONU y otras misiones humanitarias y de estabilización en todo el mundo, incluidos lugares como



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Bosnia, Kosovo, Somalia, Ruanda y Haití (Libro Blanco de la Defensa de Canadá de 1994, 2023)

Las Fuerzas Armadas de Canadá tienen una mayor capacidad tecnológica y financiera en comparación con las de Ecuador. Canadá opera una variedad de equipos modernos y tiene un enfoque más internacional en términos de participación en operaciones de paz y seguridad. Ecuador, por su parte, tiene una fuerza militar más modesta con un enfoque primordial en la defensa nacional y la soberanía territorial.

## Estructura de ciberseguridad

La estrategia establecida por Canadá para la Seguridad Cibernética es vista desde una visión de intervenir en la era digital de la mejor forma, es así que es establecida desde el más alto nivel, desarrollando políticas y marcos de gobernanza para coordinar los esfuerzos de ciberseguridad en todo el país. Esto implica la colaboración entre el gobierno federal, provincial y territorial, así como con el sector privado y otras partes interesadas (UNIDIR, 2023).

Canadá se ha centrado en identificar y proteger infraestructuras críticas, como sistemas de energía, comunicaciones y transporte, contra amenazas cibernéticas. Esto implica la implementación de medidas de seguridad robustas y la promoción de mejores prácticas en el sector privado (UNIDIR, 2023).

El país norteamericano reconoce la naturaleza global de las amenazas cibernéticas y ha estado cooperando con otros países y organizaciones internacionales para abordar los desafíos en el ciberespacio. Esto incluye la participación en foros internacionales y el intercambio de información y mejores prácticas (UNIDIR, 2023).

Las principales estructuras que se encargan de ciberseguridad son las siguientes:

Centro Canadiense de Seguridad Cibernética (CCSC), es una organización gubernamental de Canadá que se encarga de coordinar y promover la ciberseguridad en el país. Sus actividades abarcan una serie de áreas clave para proteger las infraestructuras críticas, los sistemas gubernamentales y el público en general en el ciberespacio; entre otras: Monitoreo, alerta temprana y asesoramiento a las organizaciones gubernamentales y al sector privado sobre posibles amenazas y vulnerabilidades; facilita el intercambio de información sobre amenazas y vulnerabilidades cibernéticas entre el gobierno y el sector privado; recomendar para mejorar las prácticas de seguridad, implementar medidas de protección y responder a incidentes; ayuda a mitigar los efectos de los incidentes y a restaurar la normalidad lo más rápido posible; contribuye al desarrollo de políticas y estándares en ciberseguridad; formación de profesionales en ciberseguridad y la difusión de información para el público en general; colabora con otros países y organizaciones internacionales en cuestiones de ciberseguridad; realiza investigación y desarrollo de nuevas tecnologías y enfoques para mejorar la ciberseguridad (UNIDIR, 2023).

Ministerio de Seguridad Pública y Preparación para Emergencias de Canadá (Public Safety Canadá), desempeña un papel fundamental en la gestión de la ciberseguridad y la preparación para emergencias cibernéticas en el país. Sus actividades en asuntos de ciberseguridad abarcan una variedad de áreas para proteger las infraestructuras críticas, responder a incidentes y promover la resiliencia cibernética. A continuación, se describen algunas de las actividades que el Ministerio de Seguridad Pública y Preparación para Emergencias lleva a cabo en relación con la ciberseguridad: formulación de políticas y estrategias nacionales de ciberseguridad; coordina la respuesta a incidentes cibernéticos a nivel nacional; mejorar la resiliencia de las infraestructuras críticas y sistemas en el ciberespacio; aumentar la concienciación pública sobre la importancia de la ciberseguridad; intercambio de


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

información sobre amenazas cibernéticas y mejores prácticas entre el gobierno, el sector privado y otros socios; evaluación y análisis de riesgos cibernéticos para identificar posibles amenazas y vulnerabilidades; colaboración con otros países y organizaciones para abordar desafíos cibernéticos globales (UNIDIR, 2023).

Real Policía Montada de Canadá, tiene una unidad especializada en delitos cibernéticos que investiga y persigue a los delincuentes de actividades delictivas en línea. Trabajan en estrecha colaboración con otras agencias gubernamentales y el sector privado para abordar los delitos cibernéticos, para lo cual ejecuta las siguientes actividades: investiga delitos cibernéticos para identificar a los responsables y llevarlos ante la justicia; desempeña un papel en la prevención de delitos cibernéticos al proporcionar educación y recursos sobre seguridad cibernética a la comunidad en general y a empresas. lucha contra la pornografía infantil en línea; operaciones para combatir actividades delictivas en línea, incluido el seguimiento y la desarticulación de redes criminales que operan en el ciberespacio; además de su enfoque en la aplicación de la ley, trabaja para apoyar y proteger a la comunidad en línea, brindando asistencia y recursos cuando se trata de delitos cibernéticos y seguridad en línea (UNIDIR, 2023).

## Estructura de ciberdefensa

Ministerio de Defensa de Canadá, es la principal institución de ciberdefensa, para proteger sus sistemas de información y garantizar la seguridad de sus operaciones en el ciberespacio, es así que cumple las siguientes actividades: trabaja para proteger los sistemas de información y redes utilizados por las Fuerzas Armadas Canadienses contra amenazas cibernéticas; detección, prevención y respuesta a ataques cibernéticos dirigidos a infraestructuras y sistemas militares; proporcionar capacitación y desarrollo de capacidades en ciberdefensa para el personal militar; operaciones de inteligencia cibernética para recopilar información sobre amenazas y actores maliciosos en el ciberespacio; colabora con otras agencias gubernamentales, como el Centro Canadiense de Seguridad Cibernética y la Policía Montada de Canadá, para compartir información y coordinar esfuerzos en ciberdefensa; invertir en investigación y desarrollo de tecnologías y soluciones avanzadas de ciberdefensa para mantenerse al día con las amenazas y desafíos emergentes (UNIDIR, 2023).

Seguridad de las comunicaciones (CSE), es una agencia de inteligencia electrónica y señales que forma parte del Departamento de Defensa Nacional de Canadá. Además de sus funciones de inteligencia, el CSE también juega un papel importante en la ciberseguridad del país, colaborando con el sector privado y otras entidades gubernamentales para proteger las infraestructuras críticas y las redes de comunicaciones del gobierno (UNIDIR, 2023).

Centro de Evaluación de Amenazas Cibernéticas, tiene un papel coordinador en la respuesta a incidentes de ciberdefensa a nivel nacional, asegurando que todos los departamentos y agencias del gobierno trabajen juntos para abordar las amenazas cibernéticas (UNIDIR, 2023).

Agencias de Seguridad y Defensa Cibernética Militar, Las Fuerzas Armadas Canadienses pueden tener unidades especializadas en ciberseguridad y defensa cibernética para proteger sus sistemas y operaciones contra amenazas cibernéticas.

Finalmente se puede mencionar a la Industria de Seguridad e Inteligencia Cibernética de Canadá (Canadian Cybersecurity and Intelligence Industry Association - CCIIA), aunque no es una entidad gubernamental, el CCIIA es una asociación de la industria que trabaja en colaboración con el gobierno y otras organizaciones para promover la ciberseguridad y la inteligencia cibernética en Canadá.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Canadá es uno de los países que ha ratificado y es parte de la Convención sobre Ciberdelincuencia, también conocida como Convención de Budapest. La Convención de Budapest es un tratado internacional que tiene como objetivo combatir el ciberdelito a través de la cooperación internacional y la armonización de leyes y enfoques en cuestiones relacionadas con la ciberseguridad y la ciberdelincuencia.

## Conclusión parcial

Canadá como país desarrollado y ubicado en segundo lugar de América y octavo en el mundo en el índice de ciberseguridad global, ha adoptado un enfoque altamente estratégico y adaptativo hacia la ciberseguridad y la ciberdefensa, consciente de la necesidad de proteger tanto su infraestructura crítica como a sus ciudadanos en un entorno de constante cambio tecnológico. Comprender la necesidad de proteger su sociedad y economía en un mundo cada vez más digital y tecnológicamente avanzado. La combinación de enfoques preventivos, colaborativos e innovadores muestra su firme compromiso de mantener la seguridad y la resiliencia en el ciberespacio a medida que evoluciona con el tiempo.

Sus instituciones tanto de seguridad como defensa y actividades en este ámbito reflejan un compromiso sólido en garantizar la seguridad en el ciberespacio y enfrentar los desafíos emergentes. Algunos puntos clave a destacar son:

Canadá como uno de los países que ha ratificado y es parte de la Convención sobre Ciberdelincuencia, también conocida como Convención de Budapest, entiende que sus esfuerzos de ciberseguridad no son estáticos, sino que evolucionan para abordar nuevos riesgos y desafíos, lo que demuestra su capacidad de adaptación; considera la importancia vital de su infraestructura crítica, Canadá ha establecido medidas de seguridad sólidas para garantizar la continuidad de operaciones y la resiliencia en caso de ciberataques; colaboración entre instituciones gubernamentales, fuerzas de seguridad, sector privado y otros actores es fundamental para una estrategia de ciberseguridad efectiva. Canadá ha establecido mecanismos de coordinación sólidos para maximizar la eficacia en la protección de su infraestructura y ciudadanos; énfasis en la educación y sensibilización sobre la ciberseguridad destaca la importancia de empoderar a los ciudadanos y empresas para protegerse en línea. Esto contribuye a una sociedad más informada y capaz de prevenir amenazas cibernéticas; inversión en investigación y desarrollo en ciberseguridad refleja la aspiración de Canadá de estar a la vanguardia en tecnologías defensivas. La adopción de soluciones innovadoras y la adquisición de capacidades avanzadas son componentes clave de su estrategia; comprende la naturaleza global de las amenazas cibernéticas y participa en la colaboración internacional para compartir conocimientos, experiencias y mejores prácticas. Esto contribuye a la seguridad en un entorno digital interconectado.

En última instancia, las instituciones y actividades de ciberseguridad y ciberdefensa en Canadá reflejan una comprensión de la necesidad de proteger su sociedad y economía en un mundo digital y tecnológicamente avanzado. La combinación de enfoques preventivos a través del fomento de leyes nacionales, colaborativos entre instituciones nacionales e internacionales e innovadores con la capacitación permanente, con una calificación de 97,67 sobre 100 puntos, muestra su firme compromiso de mantener la seguridad y la resiliencia en el ciberespacio a medida que evoluciona con el tiempo.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# ESTADOS UNIDOS DE AMÉRICA

## Generalidades

Estados Unidos de Norte América nace como república federal democrática luego de la declaración de Independencia el 4 de julio de 1776. Su moneda oficial es el dólar estadounidense, tiene una superficie de 9'837.306 Km cuadrados y una población de 339'996.567 personas, es considerada la primera economía mundial de acuerdo con su PIB de 6'181.215 millones de euros y un PIB per cápita de 72.710 euros, pero también es el país más endeudado, con una deuda pública de 24'905.559 millones de euros, por lo tanto, su deuda per cápita es de 74.946 euros por habitante. (Datosmacro.com, 2023).

## Datos de las Fuerzas Armadas

Sus Fuerzas Armadas está compuestas por 1'400.000 activos y 1'458.500 de personal de reserva distribuidos en el Ejército, Cuerpo de Marines, Armada, Fuerza Aérea, Fuerza Espacial, y la Guardia Costera. El Departamento de Defensa es el departamento ejecutivo del gobierno, encargado de coordinar y supervisar todas las agencias y funciones del gobierno directamente relacionadas con la seguridad nacional y las Fuerzas Armadas de Estados Unidos, tiene como objetivo garantizar las fuerzas militares para disuadir los conflictos bélicos y garantizar la seguridad de la nación.

La ciberdefensa y la ciberseguridad están estrechamente relacionadas ambas se centran en proteger las infraestructuras críticas y los sistemas de información del país frente a ciberataques y amenazas cibernéticas, se basa en una colaboración entre el gobierno federal, gobiernos estatales y locales, sector privado y sociedad civil. las principales entidades de ciberseguridad son; Departamento de Seguridad Nacional (DHS) responsable de la protección de las infraestructuras críticas, la coordinación de la respuesta a incidentes cibernéticos y desarrollo de políticas y estrategias de ciberseguridad a nivel nacional, la Oficina del Director Nacional Cibernético (ONCD) creada por el Congreso en 2021, trabaja bajo la Casa Blanca, Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) es una rama de la DHS encargada de proteger y fortalecer la infraestructura cibernética del país, trabaja con gobiernos estatales y locales además con el sector privado, Departamento de Defensa (DoD) tiene responsabilidades significativas en materia de ciberseguridad, incluye la defensa de redes y sistemas de gobierno y la realización de operaciones cibernéticas ofensivas cuando sea necesario y el Buró Federal de Investigaciones (FBI) responsable en la lucha contra el cibercrimen, investigando incidentes cibernéticos y colaborando con otras agencias nacionales como internacionales.

El presidente Biden expresó que uno de sus principales propósitos era proteger la nación de posibles amenazas cibernéticas, emitió una orden ejecutiva para aumentar el gasto en este ámbito y modernizar toda la tecnología a su alcance, además se reunió con los principales líderes de 26 compañías estratégicas, entre ellas, Apple, Google, IBM y Microsoft para transmitirles un mensaje: "Tenéis el poder, la capacidad y la responsabilidad de elevar el listón en ciberseguridad".



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Estructura de ciberseguridad

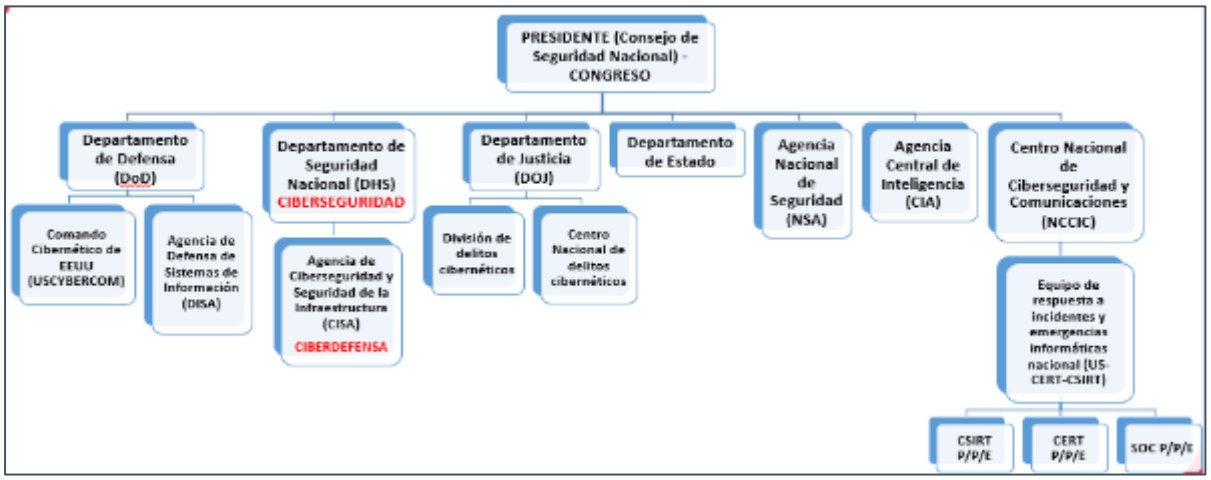
La administración norteamericana ha anunciado su nueva estrategia de ciberseguridad con la que busca hacer frente al incremento de los ciberataques. Para ello, su estrategia busca adecuar la regulación existente al nuevo escenario, potenciar la colaboración público-privada y poner la mira en los proveedores de software y servicios como defensores del ciberespacio desde cinco pilares; defender la infraestructura crítica, interrumpir y desmantelar a los actores de amenazas, dar forma a las fuerzas del mercado para impulsar la seguridad y la resiliencia, invertir en un futuro resiliente y forjar alianzas internacionales para perseguir objetivos compartidos.

El gobierno americano busca trasladar las responsabilidades de seguridad cibernética de los consumidores a la industria y tratar los ataques de ransomware como amenazas a la seguridad nacional, el plan es parte de la Estrategia Cibernética Nacional cuyo objetivo a largo plazo es involucrar a las personas, el gobierno y las empresas a operar el mundo digital con seguridad colocando la carga sobre la industria de la informática y el software para desarrollar productos seguros reduciendo significativamente la cantidad de fallas explotables antes de que se introduzcan en el mercado. Se busca mantenerse al día con la evolución del panorama de riesgos cibernéticos al reducir vulnerabilidades y construir resiliencia; contrarrestar a los actores malintencionados en el ciberespacio; responder a incidentes; y hacer que el ecosistema cibernético sea más seguro y resistente.

Existen numerosos centros de red de ciberseguridad a nivel federal, estatal y local, centros de investigación y empresas privadas, entre los principales está el Centro Nacional de Ciberseguridad y Comunicaciones (NCCIC) principal centro operativo del gobierno nacional para la respuesta a incidentes cibernéticos y la coordinación de la seguridad de la infraestructura crítica; el Centro Nacional de Seguridad Cibernética (NCSC) de ciberseguridad del Departamento de Seguridad Nacional de los EEUU que coordina la defensa cibernética del gobierno federal; el Instituto Nacional de Estándares y Tecnología (NIST) desarrolla estándares y guías para la seguridad de la información y la ciberseguridad, Centro de Análisis e Intercambio de Información (MS-ISAC) es un centro de ciberseguridad colaborativo que ayuda a los gobiernos estatales y locales a proteger su infraestructura y responder a incidentes cibernéticos; Centro de Operaciones Cibernéticas del Departamento de Defensa (DCO) es el centro de operaciones cibernéticas del Departamento de Defensa de los Estados Unidos, que supervisa y coordina las actividades de ciberseguridad en el ámbito militar. La ciberseguridad se encuentra en el nivel gubernamental el presidente de los Estados Unidos y el Congreso tienen un papel importante en la formulación de políticas y legislación relacionada con la ciberseguridad en el siguiente cuadro se puede observar su jerarquía



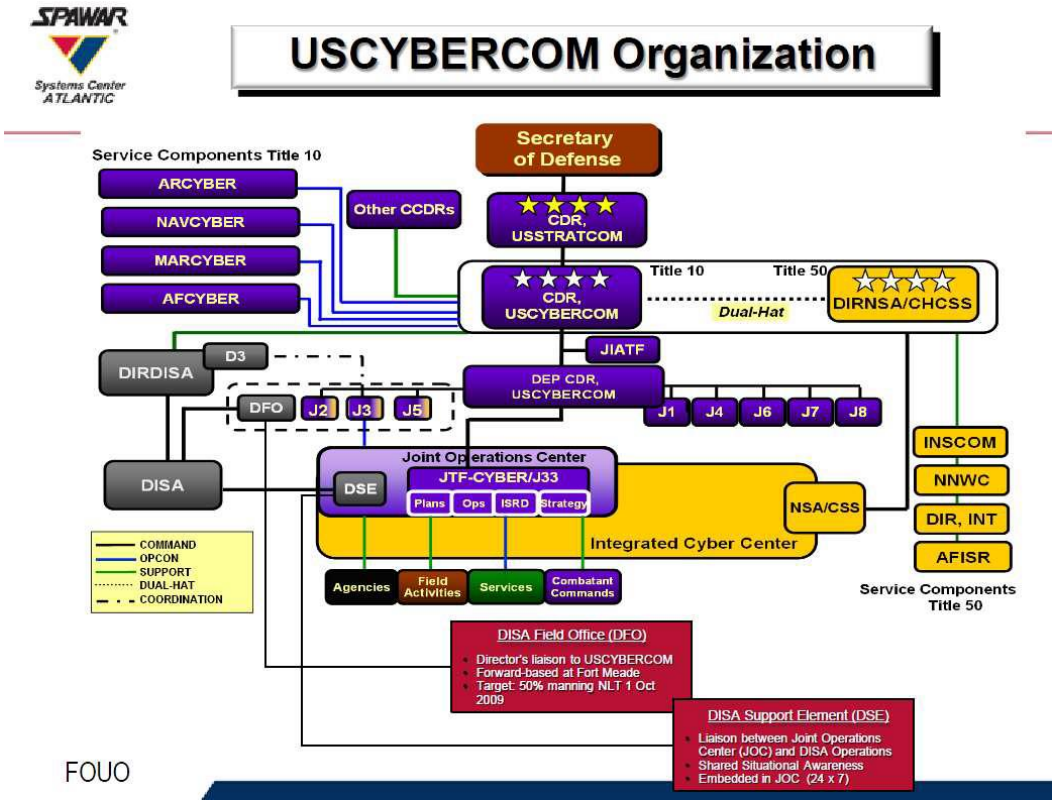
Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu



Fuente: ADEMIC

## Estructura de ciberdefensa

Las Fuerzas Armadas cuentan con el USCYBERCOM, unidad altamente especializada encargada de las operaciones de defensa de las redes de información sensibles, incluye entre sus competencias ejecutar operaciones de ataque cibernético para defender al país su estrategia busca que el ciberespacio debe equipararse a la tierra, el mar y el aire en lo que respecta a la guerra y que las ciber-defensas no se deben limitar al ámbito informático, sino que necesitan extenderse a las redes comerciales, controladas por el departamento de seguridad del territorio nacional.(Nathaniel Fick and Jami Miscik, Chairs Adam Segal, 2022).






Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Conclusión parcial

Se puede concluir que la ciberdefensa y la ciberseguridad están estrechamente relacionadas, ambas se centran en proteger las infraestructuras críticas y los sistemas de información del país frente a ciberataques y amenazas cibernéticas. La estructura de ciberseguridad en EE. UU está bastante desarrollada sin embargo continúa en evolución y adaptación a medida en base a las nuevas amenazas y el avance de nuevas tecnologías. Se basa en una colaboración entre el gobierno federal, gobiernos estatales y locales, sector privado y sociedad civil.

De igual forma que uno de sus principales propósitos del gobierno es proteger la nación de posibles amenazas cibernéticas para lo cual aumentó el gasto, dispuso modernizar toda la tecnología y emitió la estrategia de ciberseguridad que busca proporcionar seguridad nacional en la gestión de riesgos de ciberseguridad; aumentar la seguridad y la resiliencia en todo el gobierno redes e infraestructura crítica; disminuir la actividad cibernética ilícita; mejorar las respuestas a incidentes cibernéticos; y fomentar un ecosistema cibernético más seguro y confiable a través de un enfoque departamental, fuerte liderazgo y estrecha colaboración con otros organismos federales y entidades no federales.

Los Estados Unidos consideran que, así como se completa las capacidades al ámbito terrestre, naval y aéreo, se debe considerar este escenario como uno más dentro del desarrollo de políticas, capacidades que permita al país estar en condiciones de enfrentar a cualquier amenaza que atente contra su seguridad nacional


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# MÉXICO

## Generalidades

*México* es un País que se encuentra en América del Norte, limitando al norte con Estados Unidos, al sur y oeste con el océano Pacífico, al este con el golfo de México y el mar Caribe, y al sureste con Belice y Guatemala.

La capital de México es la Ciudad de México, también conocida como CDMX o simplemente México, el idioma oficial es el español, la población de México superaba los 126 millones de habitantes, lo que lo convertía en uno de los países más poblados del mundo.

México es una república federal con un sistema presidencial. El presidente es el jefe de Estado y de gobierno, y el poder legislativo está a cargo de una cámara de diputados y una cámara de senadores. Su presidente es Andrés Manuel López Obrador.

México tiene una economía mixta con un sector industrial desarrollado y una amplia base agrícola. Es uno de los mayores exportadores de productos manufacturados y es conocido por sus exportaciones de automóviles, electrónicos y productos agrícolas.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de las Fuerzas Armadas

*Las Fuerzas Armadas de México* están compuestas por tres componentes principales: el Ejército Mexicano, la Armada de México (Marina) y la Fuerza Aérea Mexicana. Las Fuerzas Armadas de México tienen como misión principal defender la soberanía del país, mantener el orden interno en casos de emergencia y desastres naturales, y contribuir a la seguridad nacional.

El Ejército Mexicano es el componente terrestre y se encarga de la defensa y seguridad interna. La Armada de México es responsable de las operaciones navales y marítimas, así como de la vigilancia de los océanos y costas. La Fuerza Aérea Mexicana se encarga de las operaciones aéreas y de defensa aérea.

El presidente de México es el comandante supremo de las Fuerzas Armadas y es responsable de tomar decisiones sobre asuntos militares. El Secretario de la Defensa Nacional y el Secretario de Marina son los líderes de los respectivos componentes y asesoran al presidente en cuestiones militares. En las últimas décadas, las Fuerzas Armadas de México han estado involucradas en operaciones para combatir el narcotráfico y mantener la seguridad interna en algunas regiones del país. Esto ha generado debates y discusiones sobre el papel de las fuerzas militares en tareas de seguridad pública.

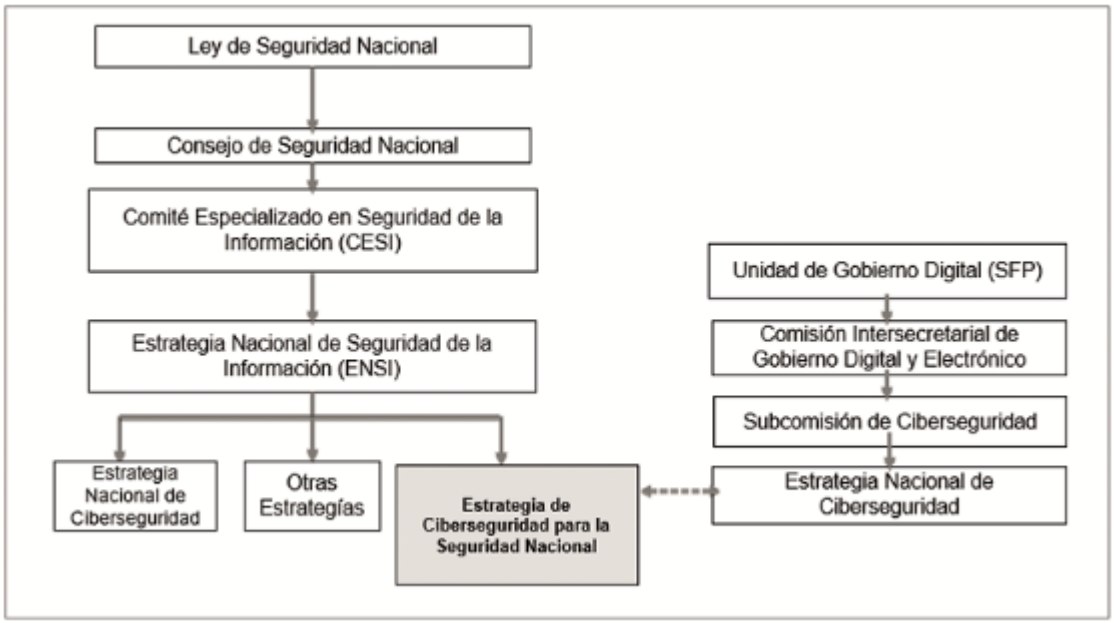
## Estructura de ciberseguridad

En lo que corresponde a la *estructura de ciberseguridad*, el aumento de riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos. (Gobierno México, 2017)

En México, el Gobierno de la República, en su rol de facilitador, promovió espacios de diálogo, discusión y aprendizaje mediante foros y talleres en un proceso de colaboración denominado “Hacia una Estrategia Nacional de Ciberseguridad” de marzo a octubre de 2017.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

En esta estrategia, diversas instituciones están involucradas, incluyendo la Secretaría de Seguridad y Protección Ciudadana (SSPC), la Secretaría de la Defensa Nacional (SEDENA), la Secretaría de Marina (SEMAR) y el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX). (Romero, 2019)




## Estructura de ciberdefensa

En México, la *ciberdefensa* se refiere a las estrategias, políticas y medidas tomadas para proteger los sistemas de información, redes y activos digitales del país contra amenazas cibernéticas.

México es el segundo país de Latinoamérica que más ataques cibernéticos recibe, sólo precedido por Brasil. A nivel global ocupa el cuarto lugar entre las naciones con mayor posibilidad de sufrir un ataque. Así, la calidad de la ciberseguridad en dependencias gubernamentales de México es un punto primordial para atender, después del hackeo y filtración de millones de documentos de la Secretaría de la Defensa Nacional. Pero no ha sido el único: en 2019 Pemex sufrió un ataque a más de 180,000 archivos de la empresa. A ella se suman la Lotería Nacional y la Plataforma Nacional de Transparencia.

## Conclusión parcial

Se puede *concluir* que México a nivel mundial se ubica en puesto cuatro en recibir amenazas cibernéticas, dispone de una estrategia nacional de ciberseguridad, en donde se incluye al Ciberdefensa, al momento se encuentra estableciendo y ejecutando una estrategia robusta y transversal de ciberseguridad en la que descanse toda la interacción de los entes oficiales, privados y sociales. (Romero, 2019)


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## AMERICA CENTRAL Y CARIBE

09 (NUEVE) PAISES ESTUDIADOS





Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# BARBADOS

## Generalidades

Barbados es una isla relativamente pequeña ubicada en el Océano Atlántico, en el sector más oriental de las Islas del Caribe, tiene 34 km de largo y 23 km de ancho, destacándose que al interior de la isla el terreno tiene poco relieve con suaves laderas hacia la región central.

Está localizada en un punto un poco alejado del eje de las demás islas, ya en el Océano Atlántico a 460 km al norte de Venezuela. La superficie de este país comprende un espacio territorial con un área de 430 $Km^2$, por lo que se lo considera como una de las naciones más pequeñas del mundo. Tiene una población de 281.200 habitantes (dato en el año 2021), pero debido a la pequeñez de su territorio está calificado como un país con alta densidad de población, por tener 654 habitantes por $Km^2$ (Datosmacro.com, 2023).

En cuanto al sistema de gobierno, su presidenta actual es Sandra Mason desde el 30 de noviembre de 2021. Barbados es una democracia parlamentaria, que se ampara en la Constitución de 1966, cuya última modificación se realizó en el año 2007. Políticamente su territorio comprende la capital que es Bridgetown y está dividido en 11 parroquias que son: Iglesia de Cristo, San Andrés, Saint George Bulkeley, Santiago, San Juan, San José, Santa Lucía, San Miguel, Saint Peter, San Felipe y Santo Tomás (Caribean Ilands, 2023).

Este país a lo largo de su historia fue parte de las colonias británicas en el Caribe, ya que por casi siglos se mantuvo como parte de la monarquía. Fue dominado desde el año 1627, a partir de la llegada de los primeros colonos del Reino Unido. Pero se independizó en el año 1966, sin dejar de estar bajo el control de la corona, hasta el 30 de noviembre de 2021 en que declaró su independencia definitiva, pero con la intención de mantenerse como parte de la Commonwealth (González, 2021).

El PIB per cápita de Barbados para el año 2022 fue de $19.040 euros, por lo está considerado en el puesto 53, es decir que tiene un bajo nivel de vida para sus habitantes, en un ranking de 196 países. Además, tiene un limitado desarrollo económico que lo sitúa en el puesto número 158 por el volumen de deuda que equivale al 120,78% del PIB, con una deuda per cápita de 24 245 euros para cada persona.

En cuanto al Índice de Desarrollo Humano (IDH) registrado por las Naciones Unidas, Barbados se ubica en el puesto 70, factor que también denota el limitado nivel en calidad de vida que tienen los habitantes de este país caribeño (Datosmacro.com, 2023).

El idioma oficial en Barbados es el "inglés", pero también se utiliza el dialecto "bajan" que es una lengua de origen anglo africano. La moneda oficial es el dólar de Barbados.

## Datos de las Fuerzas Armadas

Tiene un comando militar de tamaño moderado, denominado Fuerza de Defensa de Barbados, conformado por el Regimiento de Barbados, la Guardia Costera de Barbados y el Ala Aérea de Barbados.

De acuerdo con el sitio web Atlas Caribe, la república de Barbados tiene una cantidad de sólo 610 soldados efectivos en sus Fuerzas de Defensa, por lo que, para su formación, entrenamiento, compra de equipo y mantenimiento anualmente realiza un gasto de 33 millones del PIB. (2015)

Al momento la Fuerza de Defensa de Barbados no se encuentra inmersa en ningún conflicto internacional, sin embargo, emplea sus medios para la vigilancia del sin número de



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

islas e islotes en el norte y del litoral de Barbados, lugares en dónde se han visto en la obligación de vigilar y controlar el accionar negativo de los tráficos ilícitos que se multiplican en el Caribe (Atlas Caribe, 2015).

## Estructura de Ciberseguridad y de Ciberdefensa

Barbados es una nación pequeña que se encuentra en proceso de estructuración tanto en las políticas, como en las estrategias para su gobernanza, tras su reciente separación de la influencia británica, teniendo poca estructura de cibernética. Sin embargo, como parte de los países caribeños participa en los procesos mancomunados de apoyo para su desarrollo en todos los campos.

En este contexto los países del Caribe están tomando acciones conjuntas para dar los primeros pasos y fortalecer sus capacidades en el campo de la Ciberseguridad. Para ello y con la ayuda de la Organización de las Naciones Unidas (ONU) han determinado:

Considerar las siguientes iniciativas para su implementación temprana, las cuales tienen por objeto fortalecer la capacidad de los pequeños Estados insulares del Caribe en materia de seguridad:

- Establecer una red privada virtual que facilite el intercambio, en el ámbito regional, de inteligencia e información sobre delincuencia y otras bases de datos pertinentes en la lucha contra el terrorismo.
- El intercambio de información crítica entre las autoridades de control fronterizo para fortalecer la capacidad de control fronterizo en la lucha contra el narcotráfico y el terrorismo;
- Programas conjuntos de capacitación para permitir a las entidades existentes enfrentar los nuevos desafíos;
- Planificación estratégica conjunta y cooperación en la lucha contra estas amenazas comunes (OEA, 2023).

Además, Barbados es signatario de la Red de los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los estados miembros de la OEA, para ello ha conformado la Unidad de Telecomunicaciones establecida como entidad dependiente del Ministerio de Innovación, Ciencia y Tecnologías Inteligentes. Con la misión de generar un sector de telecomunicaciones competitivo y liberalizado que permita convertir alcanzar la excelencia en la tecnología de la información y las telecomunicaciones en el Caribe.

Entre otros tiene los siguientes objetivos:

- Promover la liberalización, la competencia y la transparencia en las operaciones de telecomunicaciones nacionales, regionales e internacionales.
- Desarrollar e implementar políticas regulatorias y de seguimiento destinadas a fomentar el crecimiento de un sector de telecomunicaciones competitivo y sostenible.
- Promover la protección de la privacidad personal de los usuarios y la seguridad de la información transmitida.
- Asegurar políticas para el funcionamiento eficiente y eficaz del sector de las telecomunicaciones.
- Para administrar de manera efectiva el espectro, la numeración, los nombres de dominio y las direcciones IP. (CSIRTAmericas network, 2023)

## Conclusión Parcial

Barbados es un país con un régimen republicano nuevo que de manera permanente ha sido dependiente de las capacidades tecnológicas que le ha ofrecido el Reino Unido en todos



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

los campos, por lo tanto, es una economía aún pequeña y en constante crecimiento que depende del accionar de sus gobernantes para establecer políticas firmes de desarrollo.

En el campo de la Ciberseguridad y la Ciberdefensa deberán buscar aliados estratégicos para en conjunto desarrollar su sector cibernético y alcanzar niveles adecuados de seguridad informática, con miras a no permitir que esta pequeña nación sea víctima de las ciberamenazas que pueden afectar su crecimiento económico y social.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# COSTA RICA

## Generalidades

Población: 5.180.000 personas y tiene una densidad de población de 101 habitantes por Km2, su área es de 51,100 km². El PIB: 64.28 miles de millones USD. Su gobierno es presidencialista y el Poder Legislativo es unicameral (Asamblea Legislativa). El idioma principal de Costa Rica es el español (castellano).

El artículo 12 de la Constitución de Costa Rica abolió el Ejército como institución permanente, aunque sí que continúa permitiendo organizar fuerzas militares para defensa militar o por convenio internacional.

## Estructura de Ciberseguridad y de Ciberdefensa

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

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

Desde la última década, la ciberseguridad se ha convertido en una de las prioridades globales en el mundo de la tecnología. Costa Rica no ha sido la excepción, y ha tenido que reforzar su estructura de ciberdefensa para enfrentar las amenazas que provienen del mundo virtual.

En Costa Rica, la estructura de ciberdefensa se encuentra liderada por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y cuenta con el apoyo del Ministerio de Seguridad Pública (MSP), el Organismo de Investigación Judicial (OIJ) y el Instituto Costarricense de Electricidad (ICE).

El MICITT, además, tiene a su cargo el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT), que es responsable de coordinar, preparar y responder a los incidentes relacionados con la seguridad informática en el país, en coordinación con varias entidades gubernamentales y privadas.

Asimismo, el CSIRT también se encarga de concientizar a la población sobre la importancia de la seguridad informática y cómo enfrentar posibles incidentes. De igual forma,



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

se ocupan de realizar investigaciones sobre nuevas amenazas para estar preparados para enfrentarlas en caso de ser necesario.

Por otro lado, el MSP y el OIJ se encargan de investigar y perseguir a los delincuentes virtuales y de colaborar con el CSIRT para identificar posibles puntos débiles en la seguridad informática del país.

Finalmente, el Instituto Costarricense de Electricidad (ICE) se encarga de proteger la infraestructura crítica del país, como los sistemas eléctricos y de telecomunicaciones.

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

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

- Estrategia de Transformación Digital
- Estrategia Nacional de Bioeconomía Costa Rica 2020-2030
- Plan Nacional de Desarrollo de Telecomunicaciones (PNDT)
- Política Nacional de Sociedad y Economía basada en el Conocimiento (PNSyEC)
- Estrategia de Prevención y Atención del Abuso y Explotación Sexual de Niños, Niñas
- Adolescentes en Línea (2021-2027)

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

Para ello, es necesario establecer modelos de actuación que afronten de manera coordinada una respuesta eficaz que garantice la confianza en los servicios que ofrecen las organizaciones a la sociedad, especialmente cuando los servicios que ofrecen son de carácter esencial. Los modelos estándares de ciberseguridad y ciberresiliencia son instrumentos vitales para ayudar a las organizaciones a evaluar, desarrollar y mejorar sus estrategias, metodologías y procedimientos de protección frente a las ciber amenazas.

La coordinación política y técnica que permiten implementar las líneas de acción de este plan está a cargo de una estructura que posibilita la acción conjunta entre los distintos actores. MICITT, será el punto focal a nivel nacional e internacional para cualquier tema relacionado con la seguridad cibernética del país.

El Comité Consultivo encargado de velar junto con MICITT para el cumplimiento de la estrategia está formado por:

- Dos representantes del MICITT
- Un representante del Poder Judicial
- Un representante de la SUTEL
- Dos representantes de la sociedad civil



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

- Dos representantes de la academia
- Dos representantes del Sector Privado
- Un representante de la PRODHAB
- Dos representantes del Sector Financiero

El Comité Consultivo, presidido por el MICITT, reforzará relaciones de coordinación, colaboración y cooperación entre los distintos sectores y partes interesadas en la ciberseguridad, incluyendo al Estado, el sector privado, la academia y la sociedad civil.

Además, tendrá la autoridad para monitorear y evaluar la implementación de los objetivos y de las líneas de acción de este Plan Nacional por parte de los distintos actores gubernamentales.

## Conclusión Parcial

Se puede concluir que la estructura de ciberdefensa de Costa Rica es un conjunto de entidades gubernamentales y privadas que trabajan juntas para proteger los intereses y la seguridad de los ciudadanos, empresas y organizaciones del país. A pesar de que aún falta camino por recorrer en materia de ciberseguridad, Costa Rica ha avanzado significativamente en la adopción de tecnologías y en la implementación de medidas de protección para garantizar la estabilidad y el bienestar del país.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# CUBA

## Generalidades

Límites: Cuba limita al norte con el estrecho de Florida y los Estados Unidos, al este con el Paso de los Vientos y el Atlántico, al sur con el mar Caribe y al oeste con el Golfo de México y México.

Capital: La Habana.

Población: Aproximadamente 11.3 millones de habitantes.

Área: Alrededor de 109,884 kilómetros cuadrados.

Tipo de gobierno: República socialista de partido único.

PIB: El Producto Interno Bruto (PIB) en 2021, era aproximadamente 97 mil millones de dólares estadounidenses.

IDH (Índice de Desarrollo Humano): hasta 2021, con un valor de alrededor de 0.783, lo que lo ubicaba en el puesto 73 a nivel mundial.

Idioma: El idioma oficial es el español.

Historia de Cuba: Cuba fue colonizada por España en el siglo XV y se convirtió en un importante centro de la producción de azúcar y tabaco. En 1898, tras la Guerra Hispanoamericana, Cuba pasó de ser una colonia española a un territorio bajo la influencia de los Estados Unidos. En 1902, Cuba obtuvo la independencia formal.

El país atravesó una serie de cambios políticos y económicos en las décadas posteriores, incluida la Revolución Cubana en 1959, liderada por Fidel Castro. Esta revolución condujo a la instauración de un gobierno socialista y a la implementación de políticas de nacionalización y reforma agraria.

Cuba mantuvo estrechos lazos con la Unión Soviética durante la Guerra Fría, lo que tuvo un impacto significativo en su economía. Después del colapso de la Unión Soviética, Cuba enfrentó dificultades económicas y un período conocido como el "Período Especial" (Fernández, 2018).

## Datos de Fuerzas Armadas

Fuerzas Armadas Revolucionarias (FAR): Las FAR son el principal componente de las fuerzas armadas cubanas y se encargan de la defensa del país. Incluyen el Ejército, la Armada y la Fuerza Aérea. Las FAR fueron creadas poco después del triunfo de la Revolución Cubana en 1959 (Ministerio de las Fuerzas Armadas Revolucionarias, 2023).

Tropas Guarda fronteras: Responsables de la seguridad y vigilancia de las fronteras marítimas y terrestres de Cuba.

Milicias: Las Milicias de Tropas Territoriales son una fuerza de reserva que puede ser movilizada en caso de amenaza o conflicto. Juegan un papel importante en la defensa del país.

Efectivos: La cantidad exacta de efectivos de las Fuerzas Armadas de Cuba no es siempre transparente y puede variar. Se estima alrededor de 39,000-50,000 efectivos activos en las FAR.

Equipamiento militar: Cuba ha mantenido históricamente relaciones militares con Rusia y otros países. Su equipamiento incluye una variedad de vehículos, armas ligeras y sistemas de defensa aérea.

Presupuesto militar: El presupuesto exacto destinado a las fuerzas armadas de Cuba no



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

es siempre de dominio público. Sin embargo, las limitaciones económicas del país pueden afectar el gasto en defensa.

Ideología política: Las Fuerzas Armadas de Cuba históricamente han estado fuertemente influenciadas por la ideología política del gobierno socialista y la Revolución Cubana.

## Estructura de Ciberseguridad

Ministerio de las Comunicaciones (MINCOM): El MINCOM es el organismo principal encargado de supervisar las políticas y estrategias de telecomunicaciones, informática y ciberseguridad en Cuba (Ministerio de Comunicaciones de Cuba, 2023).

Grupo Empresarial de Informática y las Comunicaciones (GEIC): El GEIC es una entidad que forma parte del MINCOM y se dedica a la gestión y el desarrollo de proyectos relacionados con las tecnologías de la información y las comunicaciones, incluida la ciberseguridad.

Empresa de Informática y Medios Audiovisuales (CINESoft): CINESoft es una entidad que se enfoca en el desarrollo de software y soluciones informáticas, y también juega un papel en la seguridad cibernética.

Centro de Seguridad y Ciberseguridad Informática (CESECI): Este centro es responsable de monitorear y proteger los sistemas informáticos críticos del país. Trabaja en la detección y respuesta a incidentes cibernéticos, así como en la investigación y el desarrollo de capacidades de ciberseguridad.

Academia de Ciencias de Cuba: A través de sus instituciones y centros de investigación, la academia puede estar involucrada en investigaciones y desarrollo en el campo de la ciberseguridad y las tecnologías de la información.

## Estructura de Ciberdefensa

La empresa cubana “Segurmática”, constituida en febrero de 1995 y única de su tipo en Cuba, desarrolla productos y soluciones de seguridad informática avanzados, así como, brinda servicios y consultoría especializada a entidades nacionales y extranjeras, de la tal manera de contribuir a fortalecer la ciberseguridad de Cuba. Esta empresa se le conoce en lo fundamental por sus programas antivirus; pero los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes y neutralización de ataques (Ministerio de Comunicaciones de Cuba, 2023).

## Conclusión parcial

A medida que la sociedad cubana se conecta cada vez más a Internet y a las redes globales, la ciberseguridad se vuelve crucial para salvaguardar los activos digitales, proteger la privacidad de los ciudadanos y garantizar la seguridad nacional. Por consiguiente, la ciberseguridad desempeña un papel fundamental en la protección de los intereses nacionales y ciudadanos de Cuba en un mundo digital cada vez más interconectado. Garantizar un ciberespacio seguro y confiable contribuye a la estabilidad, el desarrollo y el bienestar del país y sus habitantes.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# EL SALVADOR

## Generalidades

El Salvador está ubicado en Centroamérica. Tiene una población aproximada de 6,5 millones de habitantes. Su extensión territorial es de 21.041 km. cuadrados. Su sistema de Gobierno es Democrático, siendo el Presidente el Jefe de Estado. Su producto interno bruto (PIB) al año 2022 es de 72.318 millones. El Índice de Desarrollo Humano (IDH) se considera "Medio", según informes del Programa de las Naciones Unidas para el Desarrollo (PNUD). Su idioma oficial es el español, aunque dispone de dos lenguas nativas, la Náhuat y Lenca salvadoreño.

Históricamente ha atravesado períodos de inestabilidad política y conflicto armado, como la guerra civil de 1980-1992, luego de la cual pasó a la fase de paz y desarrollo. Es reconocido por su gastronomía, ricas tradiciones artesanales, celebraciones religiosas y folclóricas, entre otras cosas.

## Datos de las Fuerzas Armadas

El Salvador dispone de Fuerzas Armadas legalmente constituidas, con aproximadamente 30.000 efectivos en servicio activo que conforman el Ejército, Fuerza Aérea y la Fuerza Naval. A lo largo de su historia ha enfrentado varios conflictos, siendo el más significativo la Guerra Civil Salvadoreña (1980-1992), donde se enfrentaron el gobierno (Fuerzas Armadas de El Salvador FAES) y grupos guerrilleros del frente “Farabundo Martí para la Liberación Nacional” (FMLN), lo que provocó un gran número de víctimas y personas desplazadas y desaparecidas. La guerra terminó con la firma del Tratado de Paz de Chapultepec realizada en México en 1992.

## Estructura de Ciberseguridad

El Salvador dispone de una Política de Ciberseguridad publicada el 13 de mayo de 2022 según Decreto Ejecutivo N.º 163, cuyo objetivo es “regular las actividades de prevención, gestión y respuesta a las amenazas de incidentes de ciberseguridad” y cualquier otro aspecto relacionado con el manejo de las infraestructuras críticas del país, así como fortalecer los mecanismos de respuesta y desarrollar las habilidades técnicas y administrativas. La política también incluye objetivos específicos, como son: la creación de una entidad para coordinar los esfuerzos de seguridad cibernética; la promoción de campañas educativas de sensibilización; la adopción de buenas prácticas y la creación de centros de protección especializados; el análisis de leyes vigentes para promover la creación de un marco legal amplio y la capacitación necesaria dentro del sector judicial para investigar y perseguir los delitos cibernéticos; asimismo, fomenta la evaluación de riesgos como método para reducir los incidentes cibernéticos y promueve la cooperación internacional a través de la asistencia técnica y la colaboración con organismos internacionales y países amigos.

Dispone de la Oficina Salvadoreña de Ciberseguridad, dependiente de la Agencia Nacional de Innovación, Ciencia y Tecnología, así como un Comité de Ciberseguridad, que fungirá como ente consultivo y de asesoría técnica.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

El proyecto define los conceptos de amenaza, ciberseguridad, evento informático, incidente, indicadores de compromiso, infraestructuras críticas, operador, resiliencia, riesgo cibernético, servicio esencial, sistema informático y vulnerabilidad.

Por otro lado, la Policía Nacional de El Salvador fortalece sus capacidades para la investigación de delitos cibernéticos con La Unidad de Delitos Cibernéticos, de la División de Investigación, permitiendo mejorar la profesionalización de los funcionarios de la justicia penal en lo referente a prevención y lucha contra el ciberdelito.

De igual manera, el Consejo Nacional de Ciencia y Tecnología realiza un constante análisis y recopilación de información sobre las ciberamenazas o sus actores (CTI), el mismo que proporciona incentivos a la comunidad científica y tecnológica, cuyas áreas son Innovación Científica y Transferencia Tecnológica; además, dispone de un Observatorio Nacional de Ciencia y Tecnología.

La asamblea Legislativa de la República de El Salvador, mediante decreto Nro. 260 estableció la Ley Especial Contra los delitos informáticos y conexos, su objetivo es proteger los bienes jurídicos de aquellas conductas delictivas cometidas a través de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.

## Estructura de Ciberdefensa

El Salvador mantiene una organización en torno a diversas instituciones y organismos gubernamentales que se encargan de proteger y gestionar la ciberseguridad del país.

Los principales actores en la estructura de ciberseguridad de El Salvador son:

• Consejo Nacional de Seguridad Cibernética (CNSC): Órgano rector de la seguridad cibernética en El Salvador. Su tarea principal es coordinar y orientar las políticas y estrategias relacionadas con la seguridad nacional.

• Centro de Respuesta a Incidentes de Seguridad Cibernética (CSIRT): Encargado de identificar, analizar y responder a incidentes de seguridad cibernética en el país. También se pueden dar consejos y recomendaciones a varias partes sobre cómo protegerse de las ciberamenazas.

• Ministerio de Defensa y Fuerzas Armadas de El Salvador (FAES): Desempeña un papel importante en la seguridad cibernética nacional, especialmente en la protección de la infraestructura crítica y la defensa contra las amenazas cibernéticas que afectan la seguridad nacional.

• Ministerio de Justicia y Seguridad Pública: Es el responsable de formular e implementar la política de seguridad cibernética, particularmente en relación con la aplicación de la ley y la lucha contra el delito cibernético.

## Conclusión parcial

El Salvador, al decretar la Política de Ciberseguridad en el año 2022, ha logrado establecer las normas y directrices que permiten mantener el control ante el aparecimiento de amenazas cibernéticas, en todo su sistema informático especialmente para el control en el manejo de sus infraestructuras críticas, permitiendo que se mantenga la ciberseguridad del



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

país. Ha materializado una Política de Estado, orientada a la protección de uno de sus intereses nacionales.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# GUATEMALA

## Generalidades

El país de Guatemala tiene una población de 17.703.190 habitantes para el año 2023. Cuenta con una superficie de 108.899 Km2, lo que le convierte en el país más grande de la América Central.

Tienen fronteras terrestres con México, Belice, Honduras y El Salvador, asimismo limita con el Océano Pacífico al sur y el Mar Caribe al noreste; es un gobierno presidencialista constitucional, su presidente es el médico Alejandro Giammattei. En lo que corresponde al PIB registrará un crecimiento de 3.4% para 2023 y 3.7% para 2024 y el IDH es de 0.633, es el más bajo de Latinoamérica. Su idioma oficial es el español, pero también se hablan una serie de idiomas indígenas, como el k'iche', el mam, el q'eqchi' y el kaqchikel. Posee una rica historia, fue fundado por los mayas en el siglo III A.C y fue conquistado por los españoles en el siglo XVI, se independizó de España en 1821 y se unió a la República Federal de Centroamérica; en 1839, se separó de la República Federal de Centroamérica y se convirtió en una nación independiente. Además, es un Estado con una serie de desafíos, como la pobreza, la desigualdad y la violencia. El país también tiene una serie de fortalezas, como una economía en crecimiento, una población joven, una rica herencia cultural y sus paisajes naturales impresionantes, como los volcanes, selvas y ruinas mayas.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

En lo relacionado a las Fuerzas Armadas de Guatemala (FAG), están compuestas por tres ramas: el Ejército, la Marina y la Fuerza Aérea. El personal que conforman las FAG es de aproximadamente 21.500 efectivos (ejército 15.500, Marina 2.500 y Fuerza Aérea 3.500). Las FAG han estado involucradas en una serie de conflictos, incluyendo la guerra civil de Guatemala (1960-1996), la intervención en Honduras (1969) y la intervención en El Salvador (1979-1989). También han sido acusadas de violaciones de derechos humanos, incluyendo tortura y asesinatos extrajudiciales. Las FAG están reformándose para convertirse en unas fuerzas más profesionales y respetuosas de los derechos humanos. Adicional están trabajando para mejorar su capacidad para responder a desastres naturales, brindar asistencia humanitaria y proteger el medio ambiente.

## Estructura de Ciberseguridad

La Constitución Política de la República de Guatemala y la Ley Marco del Sistema Nacional de Seguridad, establecen el Sistema Nacional de Seguridad, cuyas directrices son determinados por el Presidente de la República desde el Consejo Nacional de Seguridad como órgano de máxima autoridad, el cual ha desarrollado distintos instrumentos de carácter funcional como son: La Política Nacional de Seguridad, la Agenda Nacional de Riesgos y Amenazas, la Agenda Estratégica de Seguridad de la Nación y el Plan Estratégico de Seguridad de la Nación.

En el documento publicado por el gobierno de la República de Guatemala, cuyo título es La Estrategia Nacional de Seguridad Cibernética, indica que “esta estrategia constituye el primer paso para establecer directrices y objetivos basados en el Eje de Transformación



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

tecnológico planteado en la Política Nacional de Seguridad, adicional es una de las dimensiones interrelacionadas y complementarias que conforman y propician el ambiente de Seguridad de la Nación".

La Estrategia Nacional de Seguridad Cibernética, está compuesta por 4 ejes estratégicos (legal, educación, cultura y sociedad, tecnologías de la información), 10 objetivos y 37 acciones que deben ser asumidas e implementadas por todos los actores y sectores involucrados directa o indirectamente.

Esta Estrategia es de gran importancia para Guatemala, dado que las amenazas y ataques cibernéticos surgen y evolucionan derivado de las diversas actividades que se desarrollan por la interconexión de medios digitales, lo cual representa una complejidad de condiciones que requieren la participación de todos los sectores del país, para poder desarrollar los marcos técnicos y jurídicos que fortalezcan la seguridad cibernética tanto a nivel nacional como global. Y mitigar las amenazas y ataques provenientes del ciberespacio, sin perder todas las ventajas que suponen las tecnologías de la información; y en caso de un incidente, contar con la resiliencia necesaria para reestablecer los servicios en el menor tiempo posible, evitando pérdida de información crítica y daños mayores.

Es así, que se ha considerado que la infraestructura critica del país tiene un origen tanto público como privado, para lo cual se ha establecido tomar acciones para proteger esta infraestructura: red eléctrica, rede de telecomunicaciones y transporte, sistema financiero, que son indispensables para la convivencia de población.

Es por ello, que la Estrategia Nacional de Seguridad Cibernética pretende abordar este tema en el marco del Sistema Nacional de Seguridad con el trabajo y monitoreo conjunto de sus componentes, como el Ministerio de Gobernación y el Ministerio de la Defensa Nacional; así también otros actores institucionales como el Ministerio de Comunicaciones Infraestructura Vivienda, para atender asuntos relacionados con la seguridad cibernética y defensa cibernética en los ámbitos de seguridad interior, exterior y gestión de riesgos respectivamente.

En cuanto a los mecanismos coordinados de respuesta a incidentes cibernéticos, han existido esfuerzos e iniciativas como el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-gt), un equipo ad hoc que operó bajo la gestión del Ministerio de la Defensa; que por falta de un marco jurídico y regulatorio que lo soportara dejó de funcionar.
Al momento se encuentra conformado un Comando de Informática y Tecnología del Ejército de Guatemala, entidad responsable de la ciberdefensa del Estado "Este Comando posee la responsabilidad de planificar, instalar y administrar los sistemas electrónicos de información, telecomunicaciones y ciberdefensa".

Además, existe una unidad en la Policía Nacional Civil (PNC) encargada de la investigación de delitos cibernéticos que es necesario reforzar e impulsar al igual que la Unidad Científica de Peritaje Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF). Sin embargo, el Ministerio Público aún no cuenta con una Unidad de Delitos Cibernéticos, la cual deberá ser creada y reforzada para trabajar en conjunto con las demás unidades relacionadas al tema.

En el país, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales, en tal razón se determinó la importancia de que el país se adhiera al Convenio de Budapest, para generar y fortalecer esos vínculos de coordinación y cooperación internacionales facilitados por un marco jurídico armonizado con los países adscritos a dicho Convenio. Cabe señalar que el Gobierno de Guatemala ya expresó el interés de adherirse al mismo, y está siendo gestionado por el Ministerio de Relaciones Exteriores.

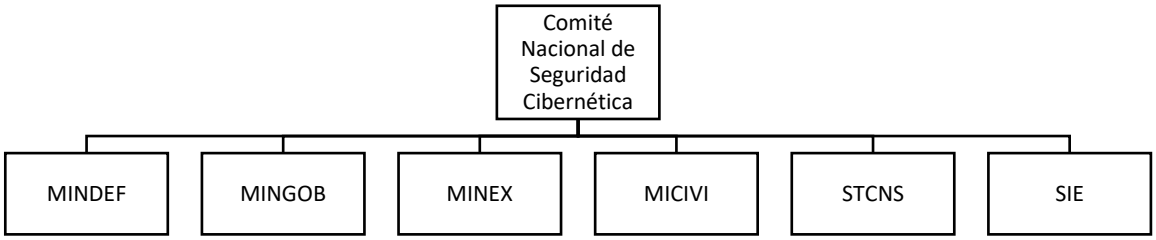
La gobernanza de la seguridad cibernética en Guatemala se entiende entonces como las políticas, instrumentos estratégicos, procesos e instituciones necesarias para administrar,



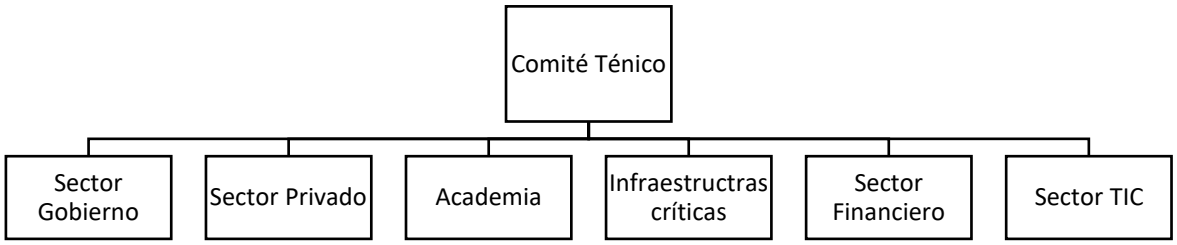
Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

gestionar y coordinar lo relacionado con la seguridad del ciberespacio a nivel nacional. En este sentido, la Estrategia Nacional de Seguridad Cibernética, propone varias líneas de acción que instan a crear la institucionalidad y la coordinación de la seguridad cibernética en el país, como la conformación de Comités de Seguridad Cibernética tanto a nivel estratégico como técnico que permitirá generar los canales y espacios de intercambio de información necesarios entre el sector público y privado para actuar bajo un marco común de normas y lineamientos.

El Comité Nacional de Seguridad Cibernética se propone como ente asesor del Consejo Nacional de Seguridad y requerirá la formulación normativa apropiada para su creación. El Comité incentiva y favorece los espacios de coordinación de las políticas interinstitucionales e intersectoriales, así como la canalización de los esfuerzos en la vinculación de los distintos planes estratégicos con una visión compartida que permita alcanzar los objetivos de la Estrategia Nacional de Seguridad Cibernética.




El Comité Técnico estará presidido por un delegado del Comité Nacional de Seguridad Cibernética y reforzará las relaciones de colaboración, cooperación y coordinación entre los distintos sectores y partes interesadas en la seguridad cibernética. Desde este espacio, se promoverán análisis, estudios y propuestas de iniciativas tanto en el ámbito nacional como internacional, que favorezcan el ecosistema de la seguridad cibernética en el país.




Las acciones realizadas por la República de Guatemala en lo referente a ciberseguridad se consideran las siguientes:

- La gestión para ingresar al convenio de Budapest
- La creación de un Comando de Informática y Tecnología del Ejército
- Fortalecimiento de la Policía Nacional Civil (PNC) encargada de la investigación de delitos cibernéticos.
- Fortalecimiento de la Unidad Científica de Peritaje Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF).


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Conclusión parcial

Se puede concluir que en la República de Guatemala se ha elevado como política pública el incrementar la seguridad y protección contra ataques cibernéticos, es así como la Estrategia Nacional de Ciberseguridad, que se encuentra plasmada en un documento, establece los ejes y objetivos a ser alcanzados, con la finalidad de proteger la infraestructura critica, las instituciones públicas y privadas y sobre todo a la población de los ciberataques. Es importante señalar que las instituciones tanto públicas y privadas tienen las disposiciones claras a fin de colaborar para el cumplimiento de esta estrategia.

Asimismo, que las Fuerzas Armadas de Guatemala, trabajan en coordinación con otras agencias estatales, para tomar acciones de seguridad contra ataques cibernéticos. En tal razón es importante señalar que las Fuerzas Armadas tomaran todas las medidas necesarias para proteger la información militar contra amenazas cibernéticas y las ciberamenazas.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# HAITI

## Generalidades

La República de Haití está ubicada en el Océano Atlántico, es parte de una gran isla denominada "La Española", que forma parte de las Antillas del Caribe.

Está localizada aproximadamente a 850 km al Norte de Colombia y Venezuela, y limita al Este con República Dominicana, que ocupa la parte oriental de la isla. Tiene una extensión territorial de 27750 km² y un litoral marítimo total de 1.771 km, es decir, es un país relativamente pequeño.

Su población es de 11 447 569 habitantes, y está considerado con una alta densidad poblacional en su territorio ya que tiene 413 habitantes por $Km^2$(Datosmacro.com, 2023).

La capital de Haití es la ciudad de Puerto Príncipe, que tiene una población de 2 870 000 habitantes, y cuenta con otras ciudades importantes como Cabo Haitiano, Gonaives, St. Marc, Les Cayes y Jacmel. El país se encuentra dividido en diez departamentos que son: Noroeste, Norte, Noreste, Artibonite, Central, Oeste, Grand´Anse, Nipes, Sur y Sudeste.

El idioma oficial de Haití es el kreol o criollo haitiano, pero se habla también el francés como segunda lengua. Su moneda es la GURDA, pero esta moneda ha pasado a un segundo plano, en vista que la economía haitiana está dolarizada.

El PIB per cápita para el año 2022, es de $1 680 euros, lo que lo ubica como una de las naciones más pobres, en el puesto número 153, ya que sus habitantes tienen un bajísimo nivel de vida con relación a los 196 países.

De igual manera el índice de desarrollo Humano (IDH) de la ONU para medir el progreso del país muestra que sus habitantes tienen un bajísimo nivel de vida con relación al resto de países en el mundo.

El sistema de gobierno es Haití es semipresidencialista, y se lo elige mediante votación popular para un periodo de cinco años, el mismo que no puede ejercer más de dos mandatos y estos no pueden ser consecutivos. El presidente electo es el encargado de nombrar al primer ministro de entre los parlamentarios que tienen mayoría en la cámara de representantes. Actualmente ejerce el cargo de primer ministro Ariel Henry, quien asumió el cargo el 20 de julio de 2021, poco tiempo después del asesinato del presidente Jovenel Moïse (Centro de Estudios Internacionales, 2020).

Históricamente, la Revolución Francesa tuvo gran influencia en la independencia de Haití, con la declaración de los Derechos del Hombre en el año 1789, con la cual se proclama la igualdad entre las personas, provocando el inicio del conflicto, por los reclamos de los esclavos que provocaron diferentes enfrentamientos violentos que se extendieron hasta el año 1804 en el que se declara la independencia por parte del general Jacques Dessalines, el mismo que se autoproclama como emperador de Haití. El nuevo emperador ejerce un poder tiránico por lo que es asesinado en el año 1806. La ocupación de la parte española de la isla por parte de los franceses termina a finales del año 1808, iniciando las dos repúblicas, Haití que ocupa el sector oeste y República Dominicana que ocupa el sector este de la isla "Española" (Ministerio de Cultura y Deporte, 2023).

## Datos de las Fuerzas Armadas

La república de Haití ha sufrido diferentes conflictos internos que han sido encabezados por los miembros de las fuerzas armadas y policía, causando por repetidas ocasiones graves



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

consecuencias como la caída del gobierno y toma del poder por parte de los militares. Pero posterior a ello estas acciones también han generado la disolución de las fuerzas del orden, ya que han provocado que el país sea considerado como estado fallido, y se ha dado la intervención internacional para ejecutar procesos para la reestructuración del Estado, de las fuerzas armadas y policía.

De acuerdo con los datos proporcionados por el Banco Mundial se han producido variaciones importantes en las fuerzas armadas de Haití desde el año 1989, en el que existían 9 000 miembros, para el año 1995 esta cantidad bajó a 7 000. En el año 2 000 la cantidad de miembros de fuerzas armadas era de 5 300, lo que dura hasta el año 2006, en el que se disuelven las fuerzas del orden por un periodo de cuatro años.

Con la ayuda internacional se empieza a reestructurar las fuerzas armadas en Haití a partir del año 2010, para contar con 50 efectivos en el 2011. Este proceso ha evolucionado hasta el año 2019 en el que se cuentan 1 000 miembros de fuerzas armadas (Banco Mundial, 2023).

El gasto militar del porcentaje presupuestario del gobierno de Haití para el año 2019 es del 0,9% y del 0,1% del PIB para el mismo año, es decir que en este proceso de reestructuración el aporte internacional es muy importante (Banco Mundial, 2023).

De esta manera se evidencia la capacidad casi nula que actualmente tienen las fuerzas armadas y policía, como órganos de seguridad de Haití para cumplir misiones en defensa de la población civil tanto en el ámbito externo, y sobre todo en el ámbito interno en el cual la conflictividad social alcanza niveles de conflictividad insostenibles para el Estado.

El gobierno del primer ministro Ariel Henry ha manifestado su intención de pedir ayuda a las fuerzas armadas extranjeras (E.U.A.), por no contar con las capacidades suficientes tanto en fuerzas armadas como en la policía, para mantener el orden frente a las pandillas que son cada vez más poderosas y siembran el caos permanente al interior del país (América Latina, 2022).

## Estructura de Ciberseguridad y Ciberdefensa

Actualmente la República de Haití sufre de grandes falencias en sus capacidades de conectividad a internet, debido a que solo un 40% de la población tiene acceso a la energía eléctrica, lo que genera una gran limitación para poder contar con el servicio de internet ya que solo el 12.19% de habitantes del país pueden acceder a dicho servicio (Banco Interamericano de Desarrollo, 2020), lo que muestra que sus estructuras destinadas a Ciberseguridad y Ciberdefensa prácticamente son inexistentes.

Como miembro de la OEA, Haití es beneficiario del Programa de Ciberseguridad del CICTE, que proporciona ayuda a los Estados miembros en el desarrollo de capacidades, nivel técnico y de políticas públicas para contar con un ciberespacio abierto, seguro y resistente, aspecto que podrá desarrollarse en la medida que la infraestructura y los medios disponibles en el país permitan la implementación de un sistema de interconexión informática permanente (OEA, 2023).

## Conclusiones parciales

La república de Haití es un país que ha sido afectado de manera permanente por conflictos internos que le han convertido en una nación relegada en el aspecto político, social y económico con características de Estado Fallido. Se requiere de la ayuda internacional permanente en un proceso de reestructuración para alcanzar el orden y la gobernabilidad, por ello Haití se enfrenta a graves problemas para poder establecer servicios básicos para su población, entre ellos y con


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

grandes dificultades el servicio de internet, dependiente de la energía eléctrica que llega solo a un 40% de su población y en consecuencia permite que solo el 12,19% de habitantes puedan tener acceso a la conectividad de internet.

Es por ello por lo que este país deberá aliarse a socios estratégicos, en condiciones de entregar el apoyo en tecnologías y medios para alcanzar las capacidades que permitan el acceso a internet, aspecto que deberá establecerse con sistemas de Ciberseguridad adecuados.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# HONDURAS

## Generalidades

La República de Honduras está ubicada en el Corazón de Centro América y posee Costas tanto en el Océano Atlántico como en el Pacífico; limita al oeste con Guatemala y al sur con Nicaragua y El Salvador.

| | | |
|---|---|---|
| 1 | Extensión | 112.491 km² |
| 2 | Población aproximada | 10.117.000 habitantes |
| 3 | Densidad poblacional | 90 hab. / km² |
| 4 | Idioma oficial | Español y más 8 dialectos nativos |
| 5 | Forma de gobierno | República constitucional democrática |
| 6 | División política | 18 departamentos, 298 Municipios, 3,731 Aldeas y 30,591 caseríos |
| 7 | Capital | Tegucigalpa |
| 8 | índice de Desarrollo Humano (IDH) (2021) | 0.621ocupa el puesto 137 de 191 uno de los más bajos de América Latina y el Caribe (Banco Mundial, 2023) . |
| 9 | El PIB per cápita (2022) | 3.135 dólares US |
| 10 | Economía número | 102 por volumen de PIB |
| 11 | Deuda pública (2021) | 14.234 millones de dólares, con una deuda del 50,31% del PIB. |
| 12 | Deuda per cápita | 1.407 $ dólares por habitante. |
| 13 | Índice de Percepción de la Corrupción del sector público (Datos macro.com, 2023) | 23 puntos percepción de corrupción es muy alta) percepción de la población) |
| 14 | Nivel de pobreza | 49,5 % vivía con menos de 6,85 dólares al día (US$6,85 por persona por día en Paridad del Poder Adquisitivo, PPA, de 2017) |

## Datos de las Fuerzas Armadas

*Las Fuerzas Armadas de Honduras* son una Institución Nacional de carácter permanente, esencialmente profesional, apolítico, obediente y no deliberante. Su función es defender la integridad territorial y la soberanía de la República, mantener la paz, el orden público y el imperio de la Constitución, los principios de libre sufragio y la alternabilidad en el ejercicio de la Presidencia de la República.

Las Fuerzas Armadas estarán constituidas por el Alto Mando, el Ejército, la Fuerza Aérea, la Fuerza Naval, la Fuerza de Seguridad Pública y los organismos que determine su Ley Constitutiva. Sus efectivos se indican en el siguiente cuadro:


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

| Honduras - Personal de defensa | | | | | | |
|---|---|---|---|---|---|---|
| Fecha | Armada | Ejercito de tierra | Fuerza área | Otro personal miitar | Personal militar total | Militares por 100.000 habitantes |
| 2021 | 1.500 | 7.500 | 2.000 | 5.000 | 16.000 | 158,15 |
| 2019 | 1.500 | 7.500 | 2.500 | 4.000 | 15.500 | 158,65 |

Fuente: https://datosmacro.expansion.com/estado/defensa-ejercitos/honduras

El último conflicto interestatal que Honduras enfrentó fue la conocida como la Guerra del Fútbol con su vecino El Salvador, que tiene como antecedente la tierra disponible, demasiada gente en un lugar demasiado pequeño, El Salvador, que degeneró en los problemas por la migración masiva de campesinos, agricultores desposeídos, salvadoreños a Honduras en busca de tierra y su posterior persecución por la ley hondureña crea para limitar el éxodo.

El 27 de junio, mientras los jugadores de los dos países se preparaban para el partido decisivo que definía quien clasificaba al mundial de México 1970, El Salvador rompió relaciones diplomáticas con Honduras.

El 14 de julio, El Salvador ordenó a sus fuerzas militares invadir Honduras y se lanzó una ofensiva aérea. En ese tiempo, la Organización de Estados Americanos, logró que ambos países llegaran a un cese al fuego el 18 de julio, después de que 3.000 personas murieran, la mayoría de ellos civiles hondureños.

## Estructura de Ciberseguridad y Ciberdefensa

Honduras, aunque no tiene un equipo nacional dedicado solamente a la *ciberseguridad,* cuenta con un órgano regulador como la Comisión Nacional de Telecomunicaciones (CONATEL), que supervisa el sector de las telecomunicaciones (Ipandetec centroamérica, 2020). En el 2018, se anunció una nueva ley que estableció una comisión encargada de crear una estrategia de ciberseguridad nacional pero no tiene un equipo dedicado solamente a ciberseguridad.

En el sector Público solo algunas instituciones que abordan temas financieros manejan temas relacionados con ciberseguridad. En lo Privado, la mayoría de los bancos y empresas de telecomunicaciones muy avanzado.

Ataques permanentes a la empresa privada, mayormente bancos. Pero tienen el equipo para evitar daños. No obstante, la mayor debilidad es la estafa que se incrementó después de la pandemia (phishing).

Honduras cuenta con variada legislación conexa que regula la materia de ciberseguridad, varias disposiciones específicas se pueden encontrar en el Código Penal, en el Procedimiento Penal Hondureño. Actualmente se elaboró un proyecto de Ley sobre la Ciberseguridad, sin embargo, aún está pendiente su aprobación en el Congreso Nacional, como también los procesos de socialización de esta.

La ley existente para proteger la ciberseguridad se aplica solamente a las redes sociales (Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en Redes Sociales)[1]. También, Honduras no cuenta con una ley de datos personales. En 2006 se aprobó la Ley de Transparencia y Acceso a la Información Pública

[1] . Ley de Estrategia de Ciberseguridad Nacional, El Pais (2018), https://www.elpais.hn/tag/ley-de-estrategia-de-ciberseguridad-nacional/.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

(Decreto 170-2006)[2], que estableció el Instituto de Acceso a la Información Pública (IAIP) (Ipandetec centroamérica, 2020). También se aprobó la Ley Especial para la Intervención de las Comunicaciones Privadas, que permite el acceso y la búsqueda de comunicaciones privadas (particularmente grabadas, electrónicas) sin consentimiento[3].

El nuevo código penal de Honduras sí codifica varios delitos cibernéticos, incluyendo piratería, phishing, robo de identidad, pornografía y provocación sexual[4], pero varios gremios están en contra del código penal promulgado en 2019, que penaliza una pena mayor por conducta criminal en línea. La legislatura ha intentado, aprobar una ley de ciberseguridad que obligaría a las empresas a bloquear o eliminar el "contenido ilegal" publicado en las plataformas (Ipandetec centroamérica, 2020).

De acuerdo con el Índice de Ciberseguridad Global (ICG) que es una iniciativa de la Unión Internacional de Telecomunicaciones (UIT), el organismo especializado de las Naciones Unidas para las TIC, Honduras se encuentra ubicado en el puesto 178 de 195 vis, como se observa en el cuadro siguiente:

Ranking global de los países (ITU, 2020)

Table 3: GCI results: Global score and rank

| Country Name | Score | Rank |
|---|---|---|
| United States of America** | 100 | 1 |
| United Kingdom | 99.54 | 2 |
| Saudi Arabia | 99.54 | 2 |
| Estonia | 99.48 | 3 |
| Papua New Guinea** | 26.33 | 118 |
| Ecuador | 26.3 | 119 |
| Mongolia | 26.2 | 120 |
| Sierra Leone | 25.31 | 121 |
| Maldives** | 2.95 | 177 |
| Honduras** | 2.2 | 178 |
| Djibouti | 1.73 | 179 |
| Burundi | 1.73 | 179 |

* no data collected

** no response to the questionnaire

En el reporte también se presentan los perfiles de cada país, al respecto Honduras presenta el siguiente diagrama:

**Honduras (República de)****


**Development Level:**
Developing Country

**Area(s) of Relative Strength**
Legal Measure
**Area(s) of Potential Growth**
Technical, Organizational, Cooperative, Capacity Development Measures

| Overall Score | Legal Measures | Technical Measures | Organizational Measures | Capacity Development | Cooperative Measures |
|---|---|---|---|---|---|
| 2.20 | 2.20 | 0.00 | 0.00 | 0.00 | 0.00 |

[2] Ley de Transparencia a Acceso a la Información Pública (2006), https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transpare

[3] Ley Especial sobre Intervención de las Comunicaciones Privadas (2011), https://www.tsc.gob.hn/web/leyes/Ley%20Especial%20sobre%20Intervenci%C3%B3n%20de%20las%20Comunicaciones%20Privadas.pdf.

[4] El Código Penal (Decreto No. 130-2017), https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

La formulación de la Agenda Digital de Honduras 2014-2018 forma parte de los esfuerzos de la Secretaría Técnica de Planificación y Cooperación Externa dirigidos a promover la competitividad y la innovación a través del uso efectivo, masivo y de calidad de las Tecnologías de Información y Comunicaciones (TIC). Los objetivos de la Agenda procuran ser consistentes con las necesidades existentes en el país en el campo de las TIC y con las restricciones actuales a nivel macroeconómico y principalmente a nivel de las finanzas públicas.

Existen algunas iniciativas orientadas a mejorar la adopción de TIC's, pero aún sigue concentrado en los factores básicos de la competitividad, dejando casi de lado los factores que impulsan la eficiencia de los mercados y la innovación productiva. Debido a esto, los datos referentes al Índice de Desarrollo de las Tecnologías de la Información y la Comunicación (IDI) evaluado por la Unidad Internacional de Telecomunicaciones (UIT), indican que Honduras ocupa una posición muy relegada desde 2011. Esto implica la existencia de una considerable brecha digital, no solo con relación a los países más desarrollados, sino también con América Latina e incluso con los demás países de la región Centroamericana (Ipandetec centroamérica, 2020).

Honduras todavía no tiene un CSIRT nacional, pero existen entidades privadas que prestan servicios de respuesta a incidentes. Aunque hay mucho que avanzar en materia de proveedores de servicios de ciberseguridad, las principales firmas del sector privado han comenzado a priorizar la seguridad cibernética y tomar precauciones al respecto, (BID, 2020).

En Honduras no existe ninguna estructura relacionada con *ciberdefensa* pero ha suscrito varios acuerdos con otras naciones en materia de seguridad cibernética con la preparación militar contra las amenazas de seguridad cibernética mediante un entendimiento con México en materia de la defensa nacional (Ipandetec centroamérica, 2020). (Ipandetec centroamérica, 2020).

## Conclusiones parciales

Para finalizar se puede *concluir* que la ciberseguridad se ha convertido en una cuestión cada vez más importante en la sociedad de la información sin embargo Honduras a pesar de los esfuerzos para tener una legislación adecuada en ciberseguridad no logra concretar todas las iniciativas, tampoco tiene una estructura de ciberseguridad o ciberdefensa, ni tiene un CSIRT nacional, por lo que por lo que Honduras tiene una capacidad limitad de acción ante amenazas cibernética y un alto riesgo de exposición y vulnerabilidad para ataques cibernéticos potencialmente devastadores tanto para el gobierno, su infraestructura crítica, así como para las empresas con graves consecuencias para el país.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# PANAMÁ

## Generalidades

Panamá es un país ubicado en el extremo sureste de América Central. Panamá conecta América Central con América del Sur y es conocido por su ubicación estratégica entre los océanos Atlántico y Pacífico. El Canal de Panamá es una importante vía de navegación que une estos dos océanos. La extensión territorial de Panamá es de aproximadamente 75,517 kilómetros cuadrados.

Capital y ciudades principales: La capital de Panamá es la Ciudad de Panamá. Otras ciudades importantes incluyen Colón, David, Santiago y Chitré.

Idioma: El idioma oficial es el español.

Moneda: La moneda oficial es el balboa, pero el dólar estadounidense también se utiliza ampliamente en la economía panameña.

Economía: Panamá tiene una economía basada en el comercio, servicios financieros y el tránsito por el Canal de Panamá. Es considerado un centro financiero y de negocios en la región. el Producto Interno Bruto (PIB) de Panamá era de alrededor de 70.8 mil millones de dólares estadounidenses, según datos del Banco Mundial a 2021.

La economía de Panamá se basa principalmente en un sector de Servicios que representa casi el 80 % de su PIB. Según el último informe de la OCDE, Panamá cuenta con un sólido marco de gobernanza para desarrollar un gobierno digital, aunque sus instituciones de ciberseguridad aún se encuentran en etapas de desarrollo. (Oficina Económica y Comercial de la Embajada de España en Panamá, 2022)

Cultura y etnias: La población panameña es diversa y está compuesta por diferentes grupos étnicos, incluyendo mestizos, afrodescendientes, indígenas y europeos. Esto ha influido en una rica mezcla de culturas y tradiciones. La población de Panamá era de aproximadamente 4 millones de personas a 2021, el Índice de Desarrollo Humano (IDH) de Panamá era de aproximadamente 0.814, lo que lo ubicaba en la categoría de "Alto Desarrollo Humano".

Panamá es una república presidencialista. Esto significa que tiene un sistema de gobierno en el que el Presidente es el jefe del estado y del gobierno, y ejerce un considerable poder ejecutivo. El Presidente es elegido por voto popular y encabeza el Poder Ejecutivo, mientras que el Poder Legislativo está representado por la Asamblea Nacional de Diputados.

Clima: Panamá tiene un clima tropical, con una estación lluviosa de mayo a noviembre y una estación seca de diciembre a abril.

## Datos de Fuerzas Armadas

Las Fuerzas Armadas de Panamá consistían en las Fuerzas de Defensa de Panamá (FDP), que incluían al Ejército de Panamá, la Fuerza Aérea de Panamá y la Marina de Panamá. Sin embargo, en 1990, el país pasó por una importante transformación militar bajo los términos del Tratado Torrijos-Carter, y las Fuerzas de Defensa de Panamá fueron desmanteladas en 1994.

Desde entonces, Panamá no tiene un ejército convencional y su seguridad está a cargo de organismos como la Policía Nacional y otras fuerzas de seguridad. La Policía Nacional de Panamá es la principal fuerza encargada de mantener la seguridad interna y el orden público en el país. Según datos históricos, en los últimos años la fuerza policial ha tenido alrededor de 25,000 a 30,000 efectivos.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Panamá ha experimentado varios conflictos bélicos a lo largo de su historia. Algunos de los conflictos más significativos en los que Panamá ha estado involucrado son:

Guerra de Independencia de Colombia (1899-1903): Panamá formaba parte de Colombia en ese momento, y durante este período hubo tensiones y descontento en Panamá debido a desacuerdos políticos y económicos con el gobierno central de Bogotá. Esta situación eventualmente condujo a la proclamación de la independencia de Panamá el 3 de noviembre de 1903.

Invasión estadounidense de Panamá (1989): Conocida como la "Operación Causa Justa", esta invasión fue llevada a cabo por Estados Unidos con el objetivo de derrocar al dictador Manuel Noriega, quien estaba involucrado en actividades ilícitas y había sido acusado de tráfico de drogas. La operación causó una cantidad significativa de daños y víctimas civiles.

Conflicto de la Zona del Canal (1964): Este fue un enfrentamiento entre Estados Unidos y Panamá sobre la soberanía de la Zona del Canal de Panamá. El conflicto resultó en la muerte de civiles panameños y condujo a negociaciones que finalmente llevaron a acuerdos para la devolución gradual de la Zona del Canal a Panamá.

Es importante mencionar que, además de estos conflictos destacados, ha habido momentos de inestabilidad política y social en Panamá a lo largo de su historia. Sin embargo, en tiempos recientes, el país ha estado enfocado en el desarrollo económico, el comercio internacional y el mantenimiento de relaciones diplomáticas y pacíficas con otras naciones.

## Estructura de Ciberseguridad

Panamá tiene una tasa de penetración de Internet relativamente alta de 2,9 millones, el 67 % de la población 2. Cerca de 2,5 millones de panameños obtienen acceso a internet a través de sus teléfonos inteligentes. Panamá cuenta con las mejores conexiones de fibra óptica submarina de América Latina, con conectividad a ocho cables submarinos. El país está cableado en las costas del Pacífico y del Atlántico, y está conectado directamente con muchos países del hemisferio occidental: América del Norte, América del Sur, América Central y el Caribe.

La estructura de ciberseguridad en Panamá mantiene varios organismos gubernamentales, regulaciones y entidades dedicadas a abordar temas relacionados con la seguridad cibernética y la protección de la infraestructura digital en la que se puede identificar los siguientes.

Ley de Delitos Informáticos: Panamá tiene leyes y regulaciones específicas para abordar los delitos cibernéticos y la seguridad de la información. La Ley de Delitos Informáticos establece las bases legales para perseguir y sancionar actividades ilícitas en línea.

Autoridad Nacional para la Innovación Gubernamental (AIG): La AIG es una entidad gubernamental encargada de liderar la transformación digital del Estado y promover la innovación tecnológica en Panamá. También tiene un papel en la promoción de la ciberseguridad y la protección de datos en la administración pública.

Ministerio de Seguridad Pública: Este ministerio juega un papel importante en la seguridad en línea y la lucha contra los delitos cibernéticos. Trabaja en coordinación con otras agencias y fuerzas de seguridad para abordar los aspectos de ciberseguridad que afectan la seguridad nacional.

Agencia Nacional de Seguridad de Panamá (ANSP): Esta agencia es responsable de proteger los sistemas de información y comunicación del Estado, así como de garantizar la seguridad en línea en sectores estratégicos.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Equipo de Respuesta a Incidentes Cibernéticos (CSIRT): El CSIRT de Panamá es un grupo encargado de responder a incidentes de seguridad cibernética y proporcionar asesoramiento técnico a entidades gubernamentales y privadas en cuestiones de ciberseguridad.

Colaboración Internacional: Panamá colabora con organizaciones internacionales y otros países para fortalecer su capacidad en ciberseguridad el gobierno tiene acuerdos con el BID a través del "Programa Panamá en Línea" aprobado en el 2016. El CSIRT de este país es miembro del CSIRT Américas por lo que participa en iniciativas regionales y globales para abordar los desafíos cibernéticos.

## Estructura de ciberdefensa

Panamá comenzó a implementar su estrategia de ciberseguridad en marzo de 2013 con la aprobación de la Resolución N.º 21; se trata de la Estrategia Nacional de Ciberseguridad y Protección de Infraestructuras Criticas, puesta en marcha con el lema "Panamá confiable en el ciberespacio, una labor de todos".

Los pilares de la misma son: proteger la privacidad; prevenir e interrumpir los delitos en el ciberespacio; fortalecer la infraestructura crítica; fomentar el desarrollo del sector privado; impulsar una cultura en materia de ciberseguridad, y en cuanto a la formación, innovación y adopción de estándares; y mejorar la capacidad de los organismos públicos para dar respuesta a incidentes. (Oficina Económica y Comercial de la Embajada de España en Panamá, 2022)

Uno de los aspectos de la ciberseguridad que se destaca en la estrategia es la protección de la infraestructura crítica, ya que esta es "vital para el bienestar de la población, los servicios básicos, el funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas", y de la que requiere "una protección integral".

CSIRT Panamá se estableció como el equipo nacional de respuesta a incidentes de seguridad informática en 2011 a través del Decreto Ejecutivo N° 709 en el marco de la Autoridad Nacional para la Innovación Gubernamental. Además de prevenir, tratar, identificar y resolver incidentes de seguridad cibernética, CSIRT Panamá también tiene como tarea aumentar el conocimiento general del país sobre seguridad cibernética.

Es importante que cada país identifique las Infraestructuras Críticas. En Panamá está el Canal, cuyo funcionamiento es vital para la sociedad y el ecosistema económico mundial. Cualquier amenaza a su operatividad puede tener consecuencias perjudiciales para el comercio global.

Uno de los pilares que implementa el país en su estrategia de ciberseguridad se centra en el fortalecimiento de la infraestructura crítica, ya que es vital para el bienestar de la población, los servicios básicos, el funcionamiento del gobierno y las organizaciones privadas.

## Conclusión parcial

Panamá trabaja en el fortalecimiento de su sistema de ciberdefensa y ciberseguridad para abordar los desafíos y amenazas en el ciberespacio, mediante la implementación de políticas del país, sin embargo, hay aspectos generales que se deben considerar:

Desarrollo en progreso: La ciberseguridad y la ciberdefensa son áreas en constante evolución en muchos países, incluido Panamá. La importancia de proteger los sistemas digitales y la infraestructura crítica se ha vuelto cada vez más evidente debido a las crecientes amenazas cibernéticas.

Colaboración interinstitucional: La ciberdefensa suele requerir la colaboración entre varios organismos gubernamentales y agencias. Esto podría involucrar al Ministerio de


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Seguridad Pública, la Autoridad Nacional para la Innovación Gubernamental (AIG), la Agencia Nacional de Seguridad de Panamá (ANSP) y otras entidades relevantes que todavía se encuentran en un proceso de desarrollo e integración.

Normativas y leyes: Un sistema de ciberdefensa efectivo se basa en leyes y regulaciones adecuadas para abordar los delitos cibernéticos y establecer normas de seguridad. Panamá tiene leyes como la Ley de Delitos Informáticos que contribuyen a este marco legal y ha implementado otras leyes con visión regional que tienen el objetivo de proteger su infraestructura crítica.

Equipos de Respuesta a Incidentes Cibernéticos (CSIRT): Estos equipos son esenciales en la ciberdefensa. Panamá cuenta con su propio CSIRT que trabaja en la detección y respuesta a incidentes cibernéticos.

Concientización y educación: La educación en ciberseguridad es crucial para tener una ciberdefensa sólida. Esto involucra la formación de profesionales, la sensibilización del público y la promoción de buenas prácticas en línea que en el proyecto de crédito con el BID está considerado.

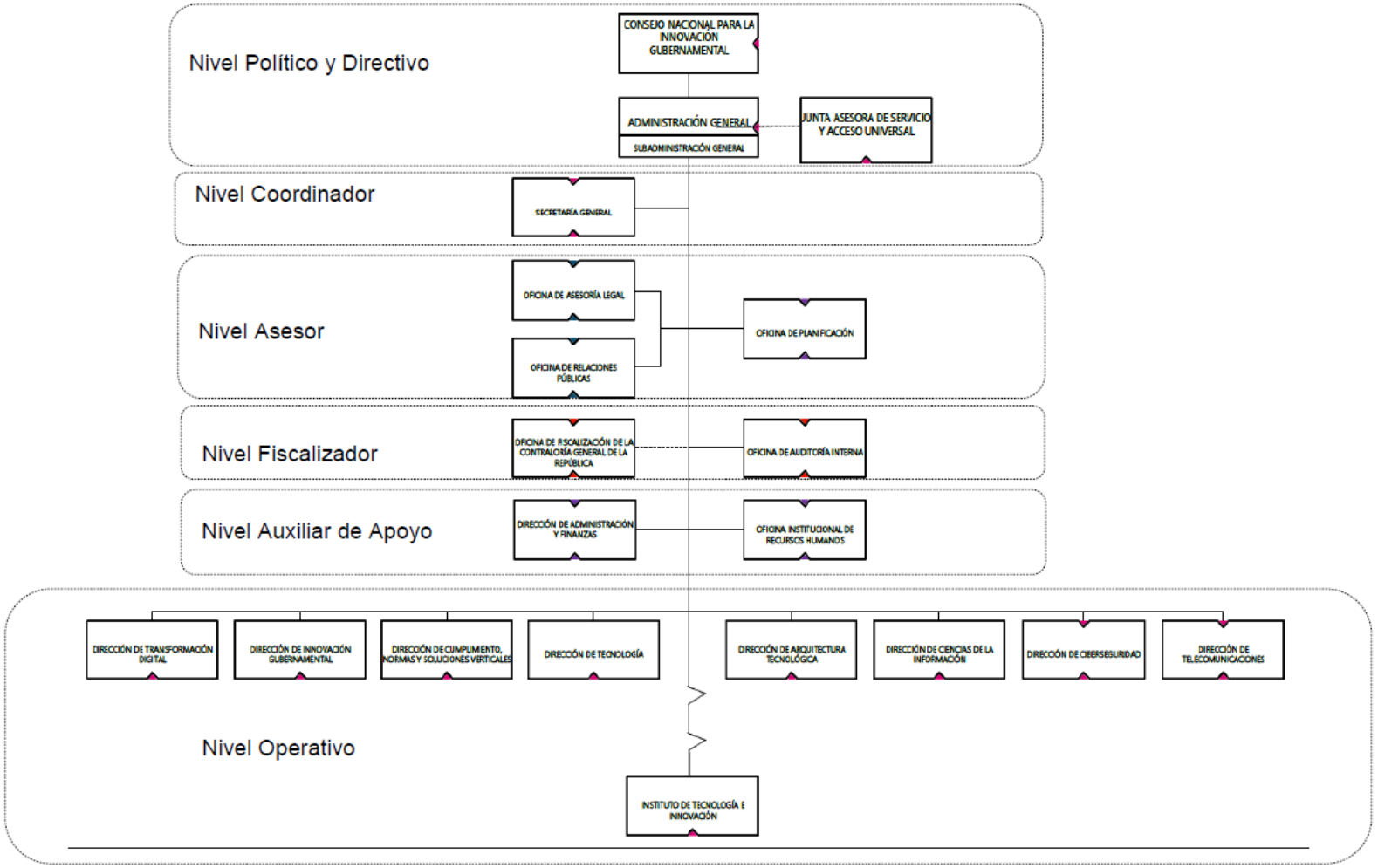
Colaboración internacional: La ciberdefensa no se limita a las fronteras nacionales. La cooperación internacional y la participación en iniciativas regionales y globales son componentes importantes para enfrentar amenazas cibernéticas transfronterizas que lo realiza a través del BID con el “Programa Panamá en Línea” desde el 2016 y el CSIRT Panamá que es miembro del CSIRT Américas.

Cabe destacar el papel que juega el Canal de Panamá como un negocio crítico para el país. Es una vía marítima y empresa autónoma del Estado panameño de 80 kilómetros de longitud que une los océanos Atlántico y Pacífico, y que se ha convertido en una de las principales rutas de comercio mundial y motor de la economía panameña que de afectar a través de ataques cibernéticos afectaría no solo a la economía del país sino interrumpiendo el comercio marítimo a nivel mundial. desafíos referentes a la seguridad en la era digital.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

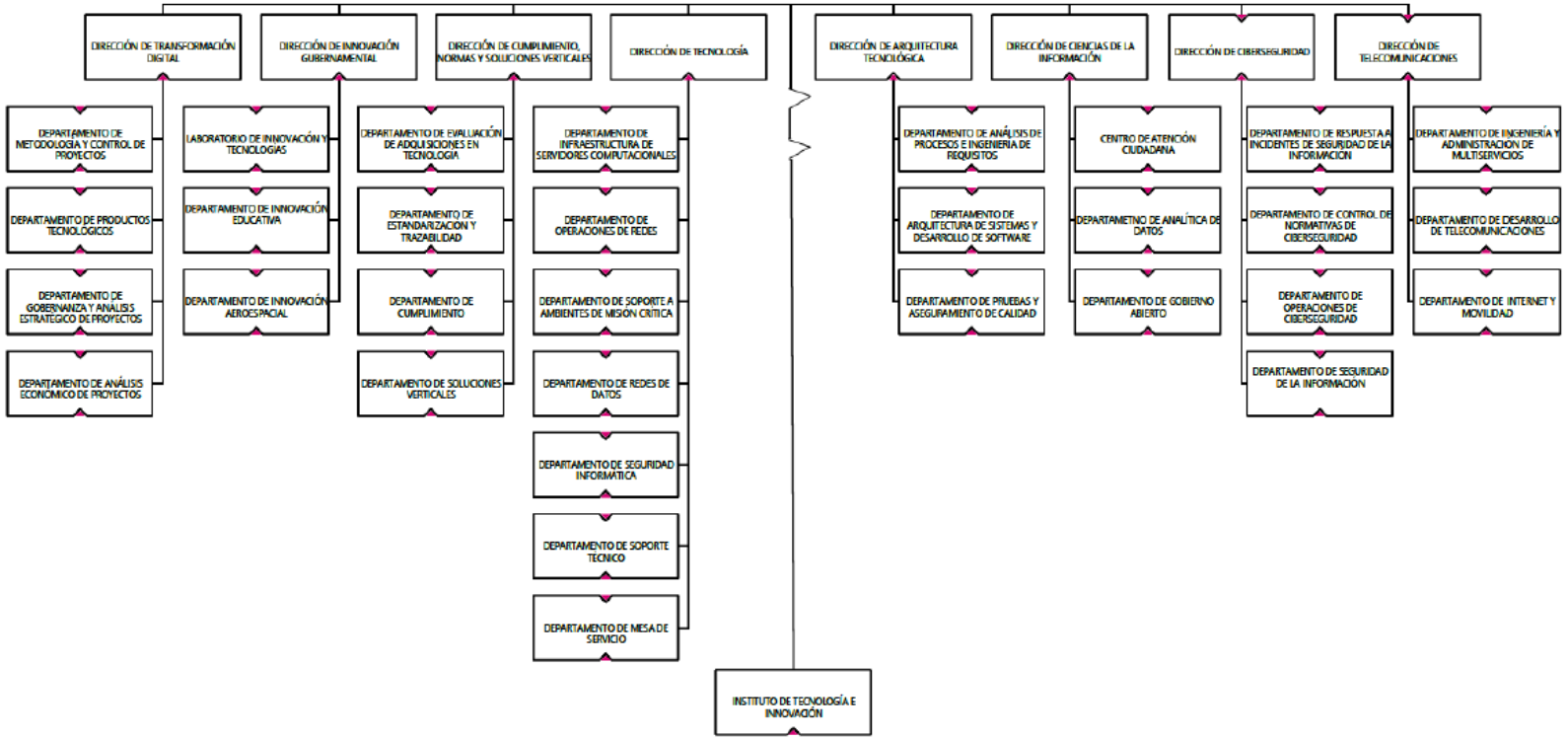
ANEXO A

Panamá: Estructura de Ciberdefensa






Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu




(Panamá, 2023)



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# REPÚBLICA DOMINICANA

## Generalidades

*República Dominicana* tiene una población aproximada de 10 millones de habitantes y su extensión territorial es de 48,442 km². El tipo de gobierno es una democracia representativa presidencialista.

El Producto Interno Bruto (PIB) per cápita de República Dominicana es de alrededor de $8,300 USD y el Índice de desarrollo Humano (IDH) se sitúa en la posición 98 a nivel mundial. El idioma oficial es el español.

La historia de este país se remonta a la época precolombina, siendo posteriormente colonizada por los españoles. El año 1821 se independizó de España y en 1844 se proclamó como República Dominicana.

La cultura dominicana es muy rica y diversa, presentando influencias africanas, taínas y españolas. La música, el baile, la gastronomía y el deporte se constituyen en algunas de las manifestaciones culturales más destacadas del país. Es un destino turístico popular en el Caribe.

El ingreso de Internet a República Dominicana se produjo a mediados de la década de 1990, con la instalación de los primeros proveedores de servicios de Internet (ISP). Desde entonces, ha habido un crecimiento significativo en el acceso a Internet en el país, con una mayor disponibilidad y velocidad. En República Dominicana, según datos actualizados hasta 2021, se estima que alrededor del 70% de la población tiene acceso a Internet. En República Dominicana, actualmente existen varios proveedores de servicios de Internet, entre los más conocidos incluyen Claro, Altice, Tricom, Wind Telecom y Viva.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

El número aproximado de las *Fuerzas Armadas de República Dominicana* incluye alrededor de 47312 miembros en total, distribuidos entre el Ejército, la Marina y la Aviación. La fuerza del ejército regular es de 22712 miembros, de ellos 19,217 eran hombres y 3,495 mujeres. En la Marina existe un numérico de 12200 efectivos. Por su parte la Fuerza Aérea tiene 12400 miembros.

En cuanto a conflictos externos e internos, actualmente República Dominicana no se encuentra involucrada en conflictos militares significativos. Sin embargo, en el pasado ha enfrentado conflictos internos, como la Guerra de la Restauración en el siglo XIX y la Revolución Dominicana en el siglo XX. En cuanto a la Policía Nacional, es responsable de mantener la seguridad y el orden público en el país.

## Estructura de Ciberseguridad

República Dominicana ha desarrollado una serie de *estructuras de ciberseguridad* para protegerse contra las amenazas en el ámbito digital. Algunas de estas estructuras incluyen:

a. Estrategia Nacional de Ciberseguridad: Es un plan integral que establece las políticas y acciones para fortalecer la seguridad cibernética en el país.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

b. Equipo de Respuesta a Incidentes Cibernéticos (CTIR): Es el organismo encargado de coordinar y responder a incidentes cibernéticos en el país, brindando asistencia técnica y coordinación en la gestión de incidentes.

c. Organismos Civiles: Entre los organismos civiles destacados se encuentra el Instituto Dominicano de las Telecomunicaciones (INDOTEL), que es el responsable de regular y supervisar el sector de las telecomunicaciones, incluyendo aspectos relacionados con la ciberseguridad.

d. Organismos Militares: Las Fuerzas Armadas de República Dominicana también desempeñan un papel importante en la ciberseguridad. A través del Centro Cibernético del Ministerio de Defensa (CECIM) y del Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i) de las FF. AA, se llevan a cabo actividades de monitoreo, defensa y respuesta ante amenazas cibernéticas.

## Estructura de ciberdefensa

En base al Plan Estratégico Institucional (PEI-MIDE) 2017-2020 y previa aprobación de Fuerzas Armadas, mediante Orden General N.º. 35 del Ministro de Defensa se crea el Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia de Fuerzas Armadas (C5i) como componente del Estado Mayor Conjunto de las Fuerzas Armadas, con el objeto de ser el Puesto de Mando Principal de Fuerzas Armadas para la conducción de las operaciones conjuntas, combinadas e Inter agenciales.

En cuanto a la jerarquía de estas estructuras, la organización y funcionamiento de los organismos encargados de la ciberseguridad en República Dominicana, de acuerdo con el siguiente organigrama podemos describir la siguiente:


En el año 2021 las Fuerzas Armadas de la República Dominicana afrontaron significativos desafíos en el ciberespacio, así como también alcanzaron logros que representan un antes y un después para el sector militar. A partir de la promulgación de la Estrategia Nacional de Ciberseguridad (2018-2021), el Ministerio de Defensa creó el *Centro de Comando, Control,*


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

*Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i), e incluyó bajo el mando de esta dependencia a la Dirección de Ciberseguridad y Ciberdefensa,* dentro de la cual opera el CSIRT-Defensa. En cuanto a la ciberseguridad y ciberataques, República Dominicana también ha experimentado un aumento en las amenazas cibernéticas. Los ciberataques pueden incluir ataques de malware, phishing, robo de datos y otros delitos cibernéticos. Es importante tomar medidas para protegerse en línea, como utilizar contraseñas seguras, mantener el software actualizado y ser consciente de las prácticas de seguridad en línea.

En los últimos años, ha habido avances significativos en ciberseguridad y ciberdefensa en República Dominicana. Algunos de estos avances incluyen:

a. Legislación y regulación: Se han implementado leyes y regulaciones específicas para abordar los delitos cibernéticos y promover la seguridad en línea.

b. Creación de organismos especializados: Se han establecido entidades como el Centro Nacional de Ciberseguridad (CNC) para coordinar y fortalecer los esfuerzos de ciberseguridad a nivel nacional.

c. Mayor conciencia y educación: Se han llevado a cabo campañas de concientización y programas educativos para informar a la población sobre las amenazas cibernéticas y promover buenas prácticas de seguridad en línea.

d. Colaboración internacional: República Dominicana ha participado en iniciativas internacionales de ciberseguridad, colaborando con otros países y organizaciones para compartir información y mejores prácticas.

Estos avances son parte de los esfuerzos continuos para fortalecer la ciberseguridad y la ciberdefensa en el país, aunque siempre es importante estar al tanto de las últimas amenazas y seguir adoptando medidas proactivas para protegerse en línea.


En AGO22, el Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i) de las Fuerzas Armadas, a través de la Dirección de Ciberseguridad y Ciberdefensa de esa unidad, llevó a cabo la "Operación ojo de Halcón 2022 CTF", en la cual se brindaron herramientas para la detección y caza de amenazas cibernéticos que pudieran presentarse en el ciberespacio.

Podemos concluir que la ciberdefensa y ciberseguridad ha ganado una mayor atención y conciencia en República Dominicana, con un reconocimiento cada vez mayor de los riesgos y amenazas cibernéticas, a través de la creación de unidades especializadas en FF. AA como el Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i).

Se han realizado grandes esfuerzos para desarrollar y fortalecer las capacidades de ciberdefensa y ciberseguridad en ese país, incluyendo la formación de expertos, la adopción de tecnologías y la implementación de políticas y regulaciones.

En los últimos años República Dominicana ha tenido un aumento en las amenazas cibernéticas, estos pueden incluir ataques de malware, phishing, robo de datos y otros delitos cibernéticos, por lo que se han dado avances significativos en este campo referente a la legislación y regulación, la creación de organismos especializados, una mayor conciencia y educación en este campo, la colaboración internacional, la participación en iniciativas internacionales de ciberseguridad, colaborando con otros países y organizaciones para compartir información y mejores prácticas, lo que le ha permitido a este país el fortalecer la ciberseguridad y la ciberdefensa.

El Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i) de las Fuerzas Armadas Dominicanas en agosto 2022, a través de la Dirección de Ciberseguridad y Ciberdefensa de esa unidad, llevó a cabo la "Operación ojo de Halcón 2022 CTF", en la cual se brindaron herramientas para la detección y caza de amenazas cibernéticos que pudieran presentarse en el ciberespacio.

## Conclusión parcial

Para la *comparación del desarrollo de* ciberseguridad y ciberdefensa en los piases objeto de estudio podemos tomar como referencia el Índice de Ciberseguridad Global (ICG) que es una iniciativa de la Unión Internacional de Telecomunicaciones (UIT), el organismo de las Naciones Unidas especializado en las TIC. A continuación, se presenta unos cuadros comparativos de los países en análisis. El año de recopilación de la información es el 2020. (Unión Internacional de Telecomunicaciones, 2020)

| CLASIFICACIÓN EN ÁMERICA | PUNTUACIÓN GLOBAL ICG | CLASIFICACION REGIONAL |
|---|---|---|
| MÉXICO | 81,68 | 4 |
| URUGUAY | 75,15 | 5 |
| REP DOMINICANA | 75,07 | 6 |
| ECUADOR | 26,3 | 19 |
| HONDURAS | 2,2 | 35 |

Cuadro 1. Clasificación en América según el ICG. Un total de 35 países, con EEUU en la 1ra posición y con 100 puntos.

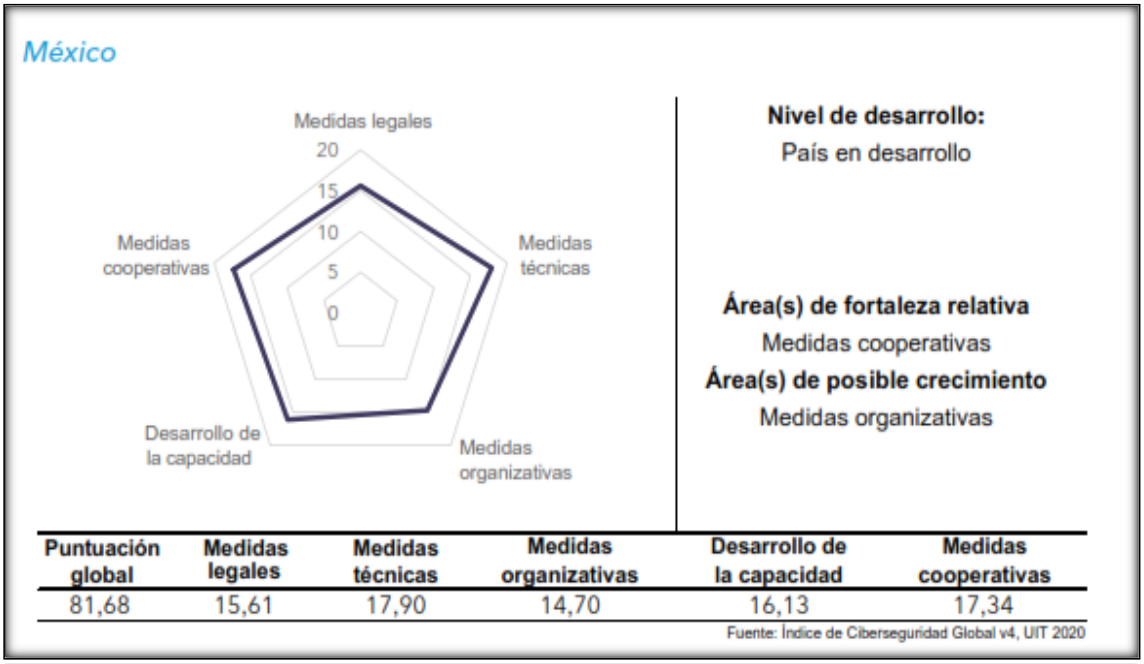
El presente cuadro muestra la comparación o relación entre los países en estudio tomando como referencia en relación con 5 pilares, 20 indicadores y 82 preguntas que conforman el ICG. Cada pilar está valorado en máximo 20 puntos y la sumatoria asigna los 100 puntos para la puntuación global.

| **PAÍS** | **JURÍDICO Medición de las leyes y reglamentos** | **TÉCNICO Medición de capacidades técnicas en organismos nacionales y sectoriales** | **ORGANIZACIÓN Medición de las estrategias nacionales** | **CAPACITACIÓN Medición de las campañas de sensibilización, formación, educación e incentivos** | **COOPERACIÓN Medición de asociaciones entre organismos, Empresas y países** |
|---|---|---|---|---|---|
| MÉXICO | 15,61 | 17,90 | 14,70 | 16,13 | 17,34 |
| URUGUAY | 13,90 | 18,27 | 12,13 | 19,04 | 11,81 |
| REP DOMINICANA | 16,38 | 18,42 | 18,52 | 9,94 | 11,81 |

| | | | | | |
|---|---|---|---|---|---|
| ECUADOR | 10,22 | 9,55 | 0,00 | 6,53 | 0,00 |
| HONDURAS | 2,20 | 2,20 | 0,00 | 0,00 | 0,00 |

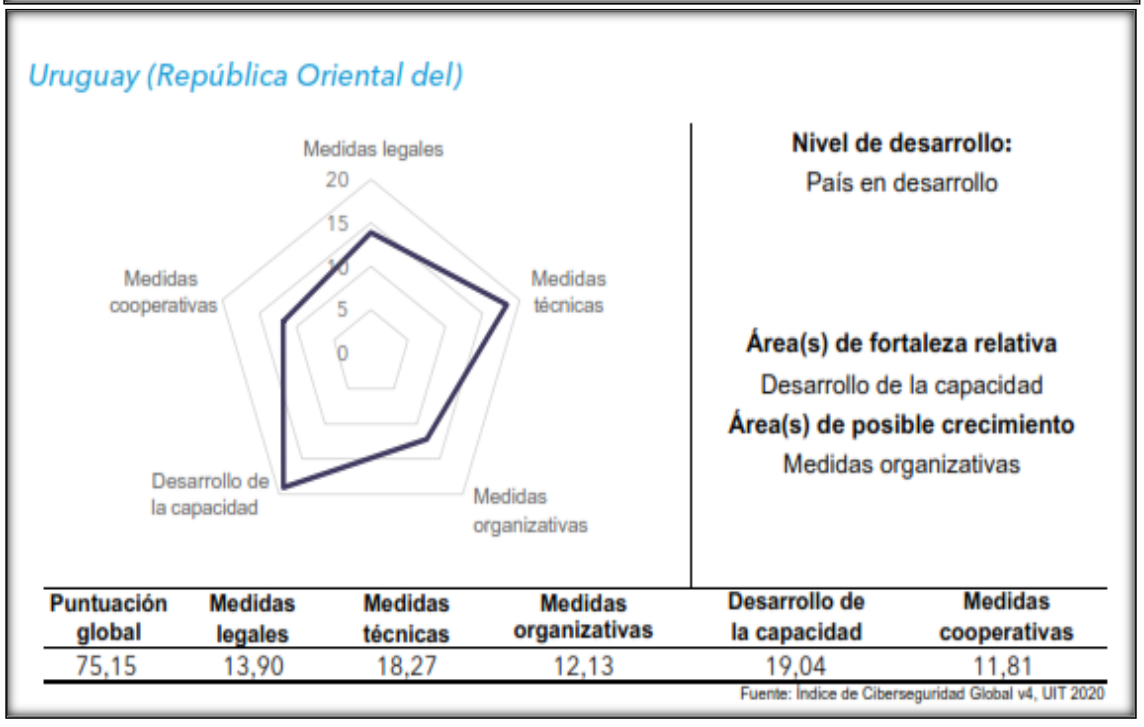
Cuadro 2. Puntaje alcanzado de cada país con relación a los 5 pilares de la ciberseguridad

A continuación, se muestra los gráficos de los índices ICG de cada país, en los cuales se puede apreciar las fortalezas, el desarrollo y avance en cada pilar de la ciberseguridad.




| Puntuación global | Medidas legales | Medidas técnicas | Medidas organizativas | Desarrollo de la capacidad | Medidas cooperativas |
|---|---|---|---|---|---|
| 81,68 | 15,61 | 17,90 | 14,70 | 16,13 | 17,34 |

Fuente: Índice de Ciberseguridad Global v4, UIT 2020



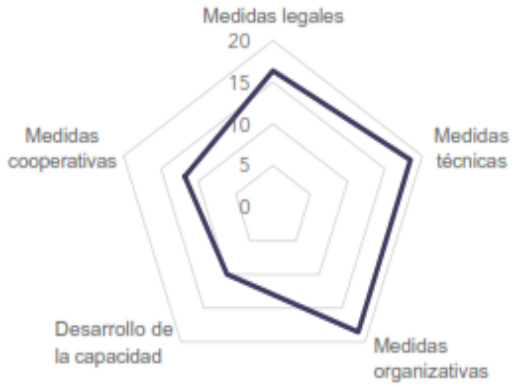

| Puntuación global | Medidas legales | Medidas técnicas | Medidas organizativas | Desarrollo de la capacidad | Medidas cooperativas |
|---|---|---|---|---|---|
| 75,15 | 13,90 | 18,27 | 12,13 | 19,04 | 11,81 |

Fuente: Índice de Ciberseguridad Global v4, UIT 2020



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## *República Dominicana*



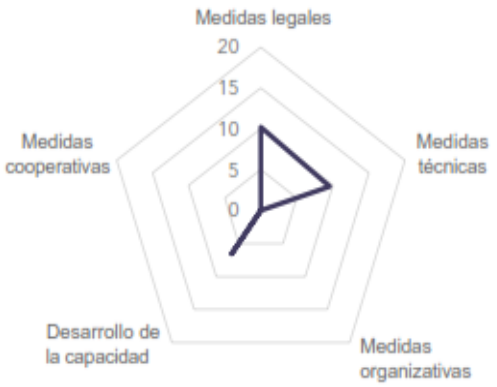

**Nivel de desarrollo:**
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

**Área(s) de fortaleza relativa**
Medidas organizativas
**Área(s) de posible crecimiento**
Medidas cooperativas

| Puntuación global | Medidas legales | Medidas técnicas | Medidas organizativas | Desarrollo de la capacidad | Medidas cooperativas |
|---|---|---|---|---|---|
| 75,07 | 16,38 | 18,42 | 18,52 | 9,94 | 11,81 |

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

## *Ecuador*




**Nivel de desarrollo:**
País en desarrollo

**Área(s) de fortaleza relativa**
Medidas legales
**Área(s) de posible crecimiento**
Medidas organizativas,
Medidas cooperativas

| Puntuación global | Medidas legales | Medidas técnicas | Medidas organizativas | Desarrollo de la capacidad | Medidas cooperativas |
|---|---|---|---|---|---|
| 26,30 | 10,22 | 9,55 | 0,00 | 6,53 | 0,00 |

Fuente: Índice de Ciberseguridad Global v4, UIT 2020



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

*Honduras (República de)***


**Nivel de desarrollo:**
País en desarrollo

**Área(s) de fortaleza relativa**
Medidas legales
**Área(s) de posible crecimiento**
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

| Puntuación global | Medidas legales | Medidas técnicas | Medidas organizativas | Desarrollo de la capacidad | Medidas cooperativas |
|---|---|---|---|---|---|
| 2,20 | 2,20 | 0,00 | 0,00 | 0,00 | 0,00 |

Fuente: Índice de Ciberseguridad Global v4, UIT 2020



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## AMERICA DEL SUR

14 (catorce) países estudiados





Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# ARGENTINA

## Generalidades

Argentina tiene una superficie de 2.780.400 km2, siendo el segundo país de mayor extensión en América del Sur, después de Brasil. Posee, además, 200 millas marinas.

El territorio argentino se divide en ocho regiones geográficas: “Llanura pampeana”, “Llanura Chaqueña”, “Mesopotamia”, “Sierras Pampeanas”, “Noroeste”, “Cuyo” (o la variante “Andes Áridos”) y “Meseta Patagónica” y “Andes Patagónicos”

Los idiomas que se hablan son: español (oficial), quechua y guaraní., Tiene como moneda el Peso argentino y una superficie de 2.780.400 km² con una población de 46.044.703. Su población tiene una composición étnica de blancos (90,97%), mestizos, amerindios y otros grupos (3%).

Con respecto a las religiones, tienen un 92% de religión católica romana, un 2% protestante, 2% judía y 4% otras. Tiene un PBI de US$ 632,77 billones, con una deuda externa total de US$ 154,28 billones y un índice de Desarrollo Humano IDH de 0,9.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de las Fuerzas Armadas

Estado Mayor Conjunto de las Fuerzas Armadas

Misión del Estado Mayor Conjunto de las Fuerzas Armadas

Asistir y Asesorar al Ministro de Defensa en materia de Estrategia Militar y realizar el Planeamiento Estratégico Militar, a fin de contribuir en forma coordinada con las otras Fuerzas de la Nación al Sistema de Defensa Nacional.

Misión de las Fuerzas Armadas

Contribuir a la Defensa Nacional actuando en forma disuasiva o empleando los medios en forma efectiva, a fin de proteger y garantizar de modo permanente la soberanía e independencia, la integridad territorial, la capacidad de autodeterminación, la vida y libertad de los habitantes y los recursos de la Nación frente a los riesgos y eventuales amenazas de origen externo.

Reseña Histórica

El Estado Mayor Conjunto de las Fuerzas Armadas tiene su origen en la Ley 13.234 suscrita por el Honorable Congreso de la Nación el 9 de septiembre de 1948. La misma establecía las pautas generales referidas a la Defensa Nacional, teniendo en cuenta los nuevos conceptos vigentes en el mundo a la luz de las experiencias recogidas al finalizar la Segunda Guerra Mundial. Dicha ley en su parte pertinente establece:

En el Artículo 11

"La conducción de la guerra compete directamente al Presidente de la Nación, quien adoptará las resoluciones pertinentes en acuerdo parcial de Gabinete, asistido por los Secretarios de Estado de Relaciones Exteriores, Guerra, Marina y Aeronáutica, constituidos al efecto en Gabinete de Seguridad Exterior (Gabinete de Guerra), con el asesoramiento directo del Estado Mayor de Coordinación".



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Total de Efectivos de Fuerzas Armadas 77.866


La guerra de las Malvinas o conflicto del Atlántico Sur fue una guerra no declarada oficialmente entre Argentina y Reino Unido de diez semanas de duración en el año 1982, por la cual se disputó la soberanía de las islas Malvinas, Georgias del Sur y Sandwich del Sur, ubicadas en el Atlántico Sur.

## Estructura de Ciberseguridad

El Sistema de ciberseguridad de la república Argentina

El ciberespacio, al igual que los espacios terrestres, marítimos, aéreo y espacial, es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. En los últimos años, y especialmente luego del ataque cibernético a Estonia en 2007, diversos países han incluido la problemática en sus agendas de estrategia nacional de seguridad; así como, han incorporado a sus estructuras institucionales, organismos especializados en ciberseguridad y ciberdefensa (Trama & de Vergara, 2017).

En el caso argentino, Gastaldi y Justribró delimitan 5 dimensiones referidas a la ciberdefensa: Ciberseguridad o Seguridad Informática, Ciberinteligencia, Ciberdefensa, Geopolítica del Ciberespacio y Derechos Humanos (2014, pág. 9).

Es conveniente empezar aclarando que, los ámbitos de actuación en el ciberespacio están divididos en Ciberseguridad y Ciberdefensa.

La República Argentina legalmente tiene diferenciados los ámbitos de la Defensa Nacional y la Seguridad Interior. Las Fuerzas Armadas no poseen atribución para involucrarse en aspectos que sucedan en el ámbito de la Seguridad Interior. Tal situación aplica a la protección cibernética.

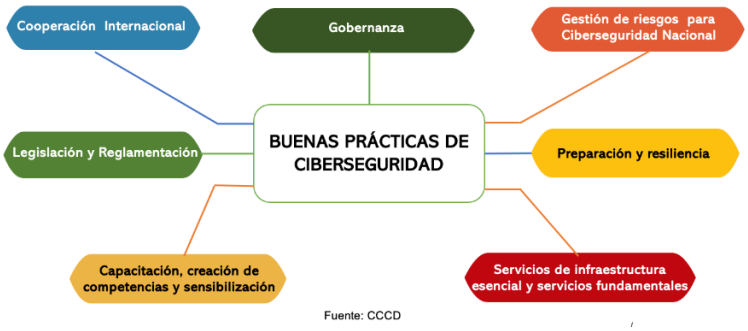
En este marco referencial. El Sistema Nacional de Ciberseguridad está materializado por el Comité de Ciberseguridad, creado como una respuesta a la necesidad de reunir a los representantes de las principales áreas de gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada esta, desarrollar el plan de acción necesario para la implementación de dicha Estrategia.

En el ámbito de la Ciberdefensa propiamente dicha, mediante Decreto del Presidente de la Nación N° 42/2016, se crea en el Ministerio de Defensa, la Subsecretaría de Ciberdefensa, con Control Funcional sobre el Comando Conjunto de Ciberdefensa (CCCD) (Taverna & Rutz, 2021).

En la dinámica del ciberespacio como nuevo ámbito de operaciones, se aprecia la multiplicidad de actores involucrados en la problemática de la Ciberseguridad y la Ciberdefensa,


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

siendo necesario la actualización constante de normas para desenvolverse en el Ciberespacio, el CCCD considera que adquiere particular relevancia en la materialización de las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad", convirtiéndose en una eficaz herramienta del Estado para hacer frente a este nuevo escenario del conflicto (GB Tomás Ramón Moyano, 2020).




Comité de Ciberseguridad

Funciones de la Unidad Ejecutiva del Comité de Ciberseguridad:

1. Convocar, organizar y realizar el seguimiento de las reuniones del Comité de Ciberseguridad.
2. Coordinar la labor de los Grupos de Trabajo que se creen, interactuando con los Entes Reguladores, de corresponder.
3. Elaborar los proyectos de actos administrativos y formular las propuestas de acciones, cuando así lo disponga el Secretario de Gobierno de Modernización de la Jefatura de Gabinete de Ministros, en virtud de lo dispuesto por el artículo 5° del Decreto N° 577/17.
4. Convocar a otros organismos cuya presencia resulte conveniente, en base a las decisiones que adopte el Comité de Ciberseguridad.
5. Documentar y comunicar a través de actas, las decisiones y cursos de acción que adopte el Comité de Ciberseguridad.
6. Poner a disposición de los integrantes del Comité de Ciberseguridad los documentos que sean necesarios para el desarrollo de su actividad.
7. Mantener un registro actualizado de todos los documentos que se elaboren.
8. Brindar asistencia administrativa al Comité de Ciberseguridad y llevar adelante todas las labores encomendadas por este.

Estrategia Nacional de Ciberseguridad de la República Argentina

La Estrategia Nacional de Ciberseguridad promueve una serie de objetivos centrales, sustentados por principios rectores, que conducirán al desarrollo de planes, políticas y acciones concretas para beneficio de la Nación (Secretaría de Gobierno de Modernización, 24/05/2019).

**Objetivos de la Estrategia Nacional de Ciberseguridad**:

Objetivo 1) Concientización del uso seguro del Ciberespacio. Es el proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ello la adopción de hábitos basados en las mejores prácticas.

Objetivo 2) Capacitación y educación en el uso seguro del Ciberespacio. Es el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio.

Objetivo 3) Desarrollo del marco normativo. Es adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.

Objetivo 4) Fortalecimiento de capacidades de prevención, detección y respuesta. Es fortalecer las capacidades de prevención, detección y respuesta frente al uso del Ciberespacio con fines ilegales.

Objetivo 5) Protección y recuperación de los sistemas de información del Sector Público. Garantizar que los sistemas de información que utiliza el Sector Público, incluyendo sus organismos descentralizados, posean un adecuado nivel de seguridad y recuperación.

Objetivo 6) Fomento de la industria de la ciberseguridad. Es promover el desarrollo de la industria nacional en los sectores vinculados a la ciberseguridad.

Objetivo 7) Cooperación Internacional. Es contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Objetivo 8) Protección de las Infraestructuras Críticas Nacionales de Información. Es fortalecer la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país.

## Conclusión parcial

Argentina establece 5 dimensiones para la ciberdefensa y ciberseguridad, donde accionar de las Fuerzas Armadas es limitada, porque su legislación dispone únicamente para la Defensa Nacional. Argentina dispone de una Estrategia Nacional de Ciberseguridad que mediante el cumplimiento de sus objetivos materializan la defensa en el ciberespacio.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# Estado Plurinacional de Bolivia

## Generalidades

Bolivia es un país situado en el centro-oeste de América del Sur. Limita con cinco países: Brasil al norte y al este, Paraguay y Argentina al sur, Chile al suroeste y Perú al oeste. Tiene una geografía diversa que incluye altas montañas, vastas llanuras, selvas tropicales y mesetas, no tiene salida al mar, la perdió luego de la denominada "Guerra del Pacífico", en la cual Chile tomó posesión de la costa boliviana por la fuerza.

Población: 12.186.079 habitantes, ocupa el puesto 79º a nivel mundial, con una Densidad (estimada) 11,09 hab./km². El Área/Superficie: 1.098.581 km², puesto 28º a nivel mundial. Agua (%): 1,4%, el PIB: USD$ 46 097 millones, el Índice Per cápita: Crecimiento USD$ 3.800 y los idiomas oficiales: Castellano con otras 36 lenguas indígenas.

Forma de Gobierno: Estado Plurinacional Presidencialista Democrático Unitario Descentralizado, de partido hegemónico:

- Presidente: Luis Arce
- Vicepresidente: David Choquehuanca

## Datos de las Fuerzas Armadas

Las Fuerzas Armadas del Estado Plurinacional de Bolivia, están conformadas por el Comando en Jefe, el Ejército de Bolivia, la Fuerza Aérea Boliviana y la Armada de Bolivia. Dichas instituciones dependen del Ministerio de Defensa de este país.

La Policía Nacional de Bolivia, aunque dependiente del Ministerio de Gobierno en tiempos de paz, forma parte de las Reservas de las Fuerzas Armadas según la Ley Orgánica de las Fuerzas Armadas de esta nación, junto con otros cuerpos de reserva como las unidades SAR-FAB de emergencia y salvamento.

El tamaño y la composición de las FF.AA. de Bolivia, entre las tres principales fuerzas (Ejército, Armada y Fuerza Aérea) suman un total de 70.000 efectivos, mientras que la Policía Boliviana ronda los 40.000 elementos. Mantienen en empleo un total de diez (10) Divisiones de Ejercito, que comportan 81 unidades tipo Batallón, Regimiento y Cuerpos Aéreos, organizados en Regiones militares, Distritos Navales y Regiones Aéreas de Bolivia.

Las Fuerzas Armadas tienen por misión fundamental, la de defender y conservar la independencia nacional, la seguridad y estabilidad del Estado Plurinacional de Bolivia, asegurar el imperio de la Constitución política del Estado, garantizar la estabilidad del gobierno legalmente constituido y asegurar la soberanía del país, tanto en el ámbito militar como en el político y económico.

## Estructura de Ciberseguridad y Ciberdefensa

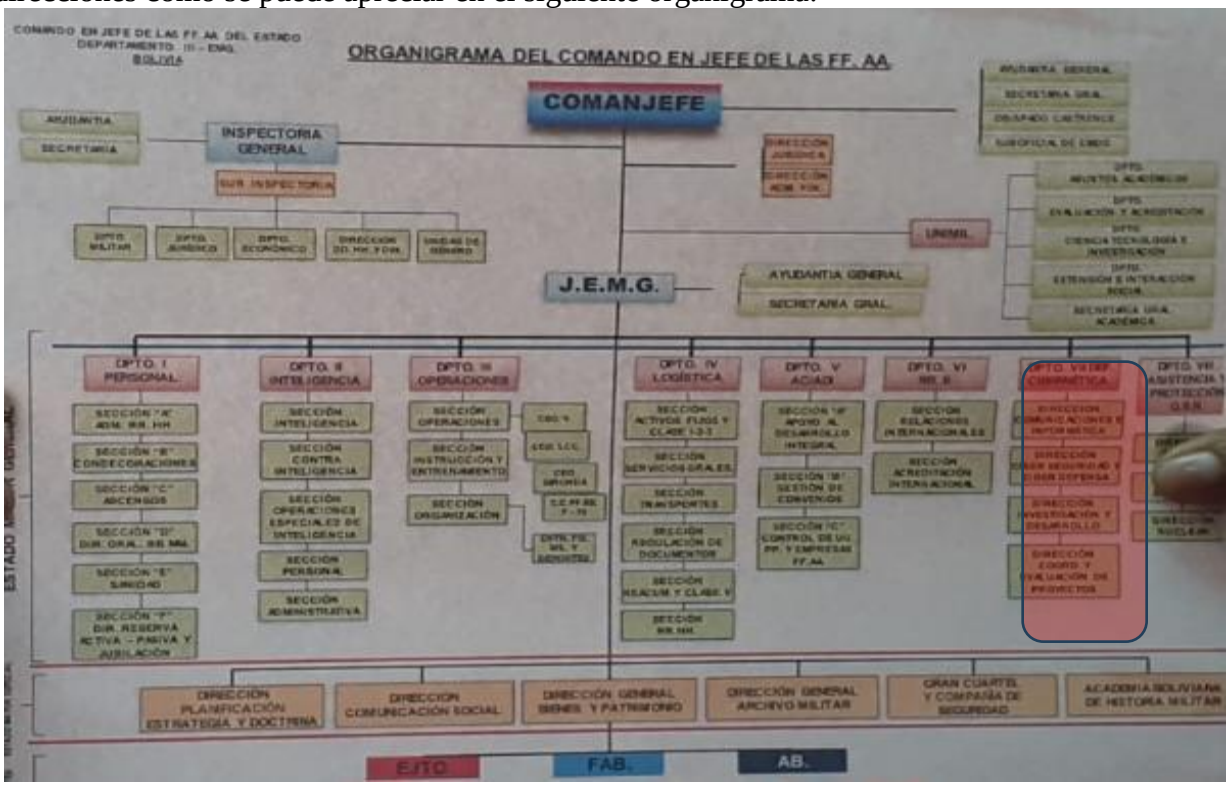
En diciembre de 2016, el Ejército boliviano, crea el "Centro de Ciberdefensa y Ciberseguridad", en respuesta a una serie de ciberataque que sufrió el sector defensa y el sector minero aparentemente por hackers chilenos. El presidente de ese entonces Evo Morales, dispuso al Ejército la creación de mencionado centro para el que inicialmente se dotó con vehículos y medios de radio.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

A partir de este incidente, donde los hackers chilenos bloquearon de la Policía y la Marina boliviana, el gobierno de Morales tuvo que acudir a los hackers bolivianos quienes iniciaron una batalla contra sus similares chilenos, retomando el control de las páginas atacadas. (Marques, 2021, pág. 134)

En la actualidad el Comando en Jefe de las Fuerzas Armadas del Estado, cuenta con el Departamento VII, Defensa Cibernética completamente estructurado, el mismo que tiene cuatro direcciones como se puede apreciar en el siguiente organigrama:




*Organigrama del Comando en Jefe de las FF. AA de Bolivia.*

En el gráfico anterior, se puede apreciar el Dpto. VII "Defensa Cibernética", con sus cuatro direcciones:

- Dirección de Comunicaciones e Informática
- Dirección de Ciberseguridad y Ciberdefensa
- Dirección de Investigación y Desarrollo
- Dirección de Coordinación y Evaluación de Proyectos

La ciberseguridad en Bolivia todavía es muy incipiente, no ha tenido el impulso que el Estado debería darle, las Fuerzas Armadas han tomado la iniciativa de la Ciberseguridad y la Ciberdefensa dentro del departamento de Seguridad Cibernética para la protección de la información militar y en servicio a otras instituciones del Estado, pero no se ha desarrollado este sistema como parte del aparato del Estado. (Fernández, 2019)


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Cuadro 5: Resultados del ICG: Región de las Américas (continuación)

| Nombre del país | Puntuación global | Clasificación regional |
|---|---|---|
| Venezuela | 27,06 | 18 |
| Ecuador | 26,3 | 19 |
| Trinidad y Tabago | 22,18 | 20 |
| Barbados | 16,89 | 21 |
| Bolivia (Estado Plurinacional de) | 16,14 | 22 |
| Antigua y Barbuda | 15,62 | 23 |
| Bahamas | 13,37 | 24 |
| El Salvador** | 13,3 | 25 |
| Guatemala | 13,13 | 26 |
| Saint Kitts y Nevis | 12,44 | 27 |
| San Vicente y las Granadinas** | 12,18 | 28 |
| Santa Lucía** | 10,96 | 29 |
| Belice | 10,29 | 30 |
| Granada | 9,41 | 31 |
| Nicaragua | 9 | 32 |
| Haití | 6,4 | 33 |
| Dominica | 4,2 | 34 |
| Honduras** | 2,2 | 35 |

*Índice Mundial de Ciberdefensa 2020.*

Con lo que muestra la tabla anterior del Índice Mundial de Ciberdefensa, Bolivia cumple con un 16,14% ubicándose en el puesto 22 de los países de América y en el puesto 140 a nivel mundial, lo que pone de manifiesto que este país sudamericano no ha desarrollado un sistema eficiente de Ciberdefensa poniéndolo en muy mala situación ante ciberataques desde el interior de Bolivia o desde algún otro país como ya ocurrió en 2015-2016. (ITU Publicaciones, 2020, págs. 28,30)

En lo que, si ha puesto énfasis, es en la comunicación a través de redes sociales, revistas y emisoras de radio por todo el país. Se utiliza en forma activa y permanente los mensajes por las redes sociales más importantes y visitadas por sus miembros. Estos mensajes están dirigidos hacia el personal militar y también para la población civil en general.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

*Mensaje de la Dirección de Comunicación Social del Ejército boliviano, revista el vocero.* (2023)


*Mensaje de la Dirección de Comunicación Social del Ejército boliviano, revista militar.* (2023)

## Conclusión parcial

Se puede concluir que, a partir de los ataques sufrido en 2016, aparentemente por hackers chilenos en contra de los sistemas de Seguridad y Minería, el Ejército boliviano creó el Comando de Ciberseguridad y Ciberdefensa el cual no ha podido desarrollarse en forma adecuada.

En la actualidad el Comando en Jefe de las Fuerzas Armadas del Estado, cuenta con el Departamento de Defensa Cibernética, el mismo que tiene cuatro direcciones.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# BRASIL

## Generalidades

Brasil es un país localizado en América del Sur cuy extensión es de poco más de 8,5 millones de km², lo que l confiere la quinta posición en extensión al nivel mundial. El idioma hablado oficialmente en Brasil es el portugués.

Según el Instituto Brasileiro de Geografía e Estatística (IBGE)[5] (2023), en el último censo realizado en 2022, viven en suelo brasileño cerca de 203 millones de personas, ocupando la séptima posición y por lo tanto uno de los países más poblados del mundo. Brasil es, conforme su Constitución Federal promulgada en 1988, una República Federativa presidencialista compuesta por la Unión indisoluble de 26 Estados, el Distrito Federal y 5.570 municipios. La capital de Brasil es Brasilia y la moneda es el Real (R$).

Considerando los datos publicados por Estadão (2023), y referentes al año de 2022, Brasil ocupa la novena posición del mundo cuando se habla en Producto Interno Bruto (PIB), con una monta de US$ 1,8 mil billones de dólares americanos. Ya con relación al Índice de Desarrollo Humano (IDH), el informe de la ONU referente al periodo de 2021/2022, Brasil posee un índice de 0,754, lo que lo hace ocupar la posición 87 del ranking entre los 191 países analizados. Tal aspecto lamentablemente revela ser el Estado brasileño una de las naciones con mayores índices de desigualdad del mundo.

Además, la Constitución de 1988 prevé que el Estado brasileño es compuesto por los poderes Ejecutivo, Legislativo y Judiciario, y asegura la observancia de los principios republicanos, sistema representativo y régimen democrático. Además, Brasil es un país que a lo largo de su historia ha adoptado una política exterior pacifista y de no intervención en otros Estados, aspecto que le asegura naturalmente gran habilidad para ser mediador de conflictos, exactamente como lo hizo a través de los años, en particular durante el periodo de independencias vivido en los siglos XIX y XX por los países sudamericanos.

Asimismo, es relevante destacar que Brasil ha adoptado hace décadas una política externa multilateral en general bastante proactiva, cooperativa, de defensa de la paz, participativa y con miras a alcanzar una mejor integración regional, como es el caso del Mercado Común del Sur (Mercosur). Cabe destacar su papel relevante en la Organización de los Estados Americanos (OEA) y en la Organización de las Naciones Unidas (ONU), siendo que en ésta última ha ejercido un rol fundamental al incremento de la paz mundial, con la contribución de grandes efectivos militares e inclusive de tropas desde su creación en 1945.

Es oportuno resaltar que Brasil tiene enormes desafíos a superar en cuestiones de seguridad, incluyendo lógicamente la cibernética, sobre todo en razón da necesidad de monitorear y proteger sus enormes riquezas minerales y naturales, a ejemplo de la enorme biodiversidad existente en la Amazonia brasileña, reservas de agua dulce estimadas en 12% de las existentes en el planeta (Acuíferos que posee, “Alter de Chão” y “Guarani”), reservas de petróleo estimadas en más de 13 mil millones de barriles, y de la gigantesca “Amazonia Azul” a preservar y defender en razón del mar territorial fruto de su inmensa costa atlántica (con 7.491 Km).

[5] Es el órgano gubernamental brasileño que tiene atribuciones relacionadas con las geociencias y las estadísticas sociales, demográficas y económicas, que incluyen la realización de censos y la organización de las informaciones para apoyar a los órganos públicos, a otras instituciones y al público en general.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Por fin, no se podría dejar de acrecentar que su gigantesca dimensión territorial (con fronteras terrestres de casi 17 mil km con 10 de los 12 países sudamericanos trae considerables desafíos a superar en consecuencia de la permeabilidad de sus fronteras con países como Colombia, Perú, Bolivia (éstos los tres mayores productores de cocaína del planeta) y con Paraguay, éste el mayor productor de marihuana, aspectos que demandan grandes inversiones en el área de seguridad y consecuentemente en Ciberseguridad y Ciberdefensa a fin de combatir los delitos y amenazas consecuentes.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de las Fuerzas Armadas

Las Fuerzas Armadas están compuestas por el Ejército Brasileño (EB), la Marina de Brasil (MB) y Fuerza Aérea Brasileña (FAB). El efectivo autorizado por la legislación del país es máximo de 444.814 militares, así distribuidos: 296.334 militares de la Fuerza Terrestre; 80.507 militares de la Fuerza Naval; y 80.937 militares de la Fuerza Aérea. Los efectivos disponibles para casos de necesidad de movilización nacional son alrededor de 1.340.000 reservistas (2023).

Con relación al presupuesto previsto para empleo por el Ministerio de la Defensa (MD) de Brasil y sus Fuerzas Armadas en 2023, según información obtenida de Caiafa (2023) disponible en el sitio Infodefensa.com, la monta llegó alrededor de R$ 124,4 mil millones de reales (moneda local), lo que equivale a cerca de 25,4 mil millones de dólares americanos[6].

Importante destacar aún conforme sostiene Caiafa (2023), que del total previamente citado cerca de 78,2% es destinado a pagos de personal, lo que corresponde a cifras alrededor de R$ 94,6 mil millones, es decir, cerca de U$ 19,3 mil millones de dólares americanos, y que solamente cerca de R$ 25,5 mil millones de reales o U$ 5,2 mil millones de dólares americanos fueron destinados para otros gastos e inversiones en programas y proyectos planteados por el Ministerio de la Defensa y respectivas Fuerzas Armadas.

Por fin, Caiafa (2023) cita que solamente alrededor de U$ 2,2 mil millones de dólares americanos del total previsto a la Defensa (lo que corresponde al 6,1% del total) fueron destinados a inversiones en proyectos estratégicos de las FF. AA brasileñas.

## Estructura de Ciberseguridad

De principio es importante señalar que actualmente la estructura de Ciberseguridad de Brasil está conformada básicamente por la estructura de Ciberdefensa desarrollada en el ámbito del Ministerio de la Defensa, eso porque desde el inicio que se observó la necesidad de desarrollar capacidades para proteger ciertos activos estratégicos y/o infraestructuras críticas del país, el MD y en particular el Ejército Brasileño fueron los principales responsables por la implementación de la defensa cibernética en territorio nacional, eso porque la Política Nacional de Defensa[7] (PND) y la Estrategia Nacional de Defensa (END) de 2008 atribuyeron la responsabilidad de coordinar la implantación de ese importante sector estratégico al Ejército Brasileño.

Es oportuno decir que solamente con la edición de la Estrategia Nacional de Ciberseguridad (e-Ciber), ocurrida en 2020, fue posible que estos asuntos empezasen a ser tratados con más amplitud a partir del nivel político, una vez que su gestión migró para el *Gabinete de Segurança*

[6] Considerando una taja de conversión de U$ 1 = R$ 4,9 - el 4 de agosto de 2023)

[7] La PND y la END son ttambién conocidas por el "Libro Verde" por los brasileños.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

*Institucional* (GSI) de la Presidencia de la República, el cual pasó a ser el principal órgano responsable por el tema en Brasil. De esa forma, con la publicación de la e-Ciber ya citada, la temática de ciberseguridad ascendió del nivel estratégico para el político, hecho que ha permitido desde entonces avances significativos en la consolidación del asunto al nivel nacional.

Tanto fue que el próximo paso hacia una unificación reglamentaria, conforme relata GSI (2023) en la documentación referenciada, es la aprobación de la Política Nacional de Ciberseguridad (PNCiber) que ya está lista para ser analizada por el Congreso Nacional aún este año de 2023. Con la aprobación de ese marco legal máximo relativo a la Política de Ciberseguridad en Brasil, expresa GSI (2023) que se unificará la legislación existente, se minimizará el creciente número de incidentes cibernéticos que afectan diversos sectores claves del país, se reducirá la deuda tecnológica nacional en el sector, y se ampliará la participación brasileña en la cooperación internacional en el tema.

Mismo delante las inúmeras limitaciones y desafíos en esta nueva área en Brasil (cuestiones presupuestarias, capacitación de personal, entre otras), no faltó voluntad y dedicación al personal asignado para cumplir esta misión tan relevante atribuida al Ejército, el cual de pronto puso en marcha estudios y acciones que acabaron por crear estructuras que hoy aseguran a Brasil la posición 18 (de 182 países) en el Índice Global de Ciberseguridad (ICG) según la Unión Internacional de Telecomunicaciones (2020). Tal aspecto revela la seriedad del trabajo realizado por el personal involucrado que resultó en una evolución continuada, sustancial y bastante sólida que fue conquistada gracias a una serie de marcos legales que fueron publicados a lo largo de los últimos años a partir de la edición de la PND y de la END de 2008.

En ese sentido cabe añadir que el objetivo mayor fue preparar con urgencia las capacidades necesarias para promover la protección adecuada contra las amenazas decurrentes del "ciberespacio" (o la "quinta dimensión"), éste totalmente transversal a las demás ya conocidas: terrestre, marítimo, aéreo y espacial. Delante estos nuevos desafíos, la prioridad fue proteger las infraestructuras críticas, siendo que la oportunidad surgida con la realización en Brasil de una serie de "Grandes Eventos[8]" ocurridos en la década pasada muchísimo contribuyeron (con inúmeras lecciones aprendidas) para que pasos consistentes fuesen dados en el sentido de perfeccionar tanto la legislación referente al asunto como la infraestructura que fue evolucionando año tras año. Importante destacar que la creciente interacción y participación de otros sectores gubernamentales, en todos los niveles, mucho contribuyeron para la evolución de la doctrina y mejoría alcanzada hasta hoy por el sector cibernético brasileño.

En relación con el marco legal, en particular con respecto a documentos y marcos de referencia básicos, Oliveira et al. (2017) cita en su obra referenciada "*Guía de Defesa Cibernética na América do Sul*" que Brasil posee una legislación considerable, compuesta por el Libro Blanco, por estrategias que abordan el tema y por instrumentos jurídicos, tales como: Constitución Federal, Código Civil, Marco Civil de la Internet (Ley nº 12.965, 23/4/2014) y su reglamentación (Decreto nº 8.771, de 11/5/2016), bien como la Ley nº 12.737, de 30/11/2012 (dispone sobre la tipificación criminal de delitos informáticos (pág. 72), los cuales ciertamente sirvieron de base a importantes avances posteriores en el área reglamentaria relacionada a cibernética en Brasil.

A continuación, en 2009, y luego después de la edición de la PND y de la END de 2008 (hoy el Libro Verde tiene última edición datada de 2020), la Directiva Ministerial nº 14 atribuyó

[8] Ejemplos de Grandes Eventos ocurridos en Brasil: la Conferencia de las Naciones Unidas Rio+20, en 2012; la Copa de las Confederaciones y la Jornada Mundial de la Juventud, ambas en 2013; la Copa del Mundo en 2014; y los Juegos Olímpicos en 2016.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

oficialmente al Ejército Brasileño (EB) la responsabilidad de coordinar el Sector Cibernético en el ámbito de la Defensa, conforme ya estaba previsto en Estrategia de Defensa Nacional (END), como ya explicado. En la más reciente END, el Congreso Nacional de Brasil (2020) cita en general los siguientes lineamientos/objetivos cuando habla del Sector Cibernético:

- Incluir, prioritariamente, tecnologías de COM entre las unidades de las FF. AA;
- Asegurar interoperabilidad y capacidad de actuar de manera integrada;
- Mejorar la Seguridad de la Información, las Comunicaciones y la Ciberseguridad, en todas las instancias del Estado, con énfasis en la protección de las Infraestructuras Críticas;
- Completar la infraestructura del Sistema de Ciberdefensa Militar, con su marco legal, sus normas conexas, así como desarrollar su preparación y empleo, en todos los niveles;
- Incentivar la investigación, desarrollo e innovación, con un enfoque en tecnologías que permiten planificar y ejecución de actividades Cibernéticas en el ámbito del Sector Defensa y que contribuyan a la Ciberseguridad a nivel nacional, involucrando a la comunidad académica nacional e internacional;
- Fortalecer la colaboración entre el Sector Defensa y la comunidad académica nacional, los sectores públicos y el sector privado y la Base Industrial de Defensa;
- Intensificar alianzas estratégicas e intercambios con Fuerzas Armadas de otros países. (pág. 61)

Aún en el cuerpo de la END más reciente se observa con claridad las siguientes Estrategias de Defensa (ED) y Acciones Estrategias de Defensa (AED), todas relacionadas al Sector Cibernético de Brasil:

- ED-1 Fortalecimiento del Poder Nacional

AED-1 Desarrollar los sectores estratégicos de defensa (nuclear, cibernético e espacial).

- ED-2 Fortalecimiento de la capacidad de disuasión

AED-10 Desarrollar capacidades para monitorear y controlar el espacio aéreo, el ciberespacio, territorio, aguas jurisdiccionales brasileñas y otras áreas de interés.

AED-11 Aumentar las capacidades de defensa y exploración del ciberespacio.

- ED-9 Fortalecimiento del área de ciencia y tecnología de defesa

AED-52 Promover el desarrollo de la tecnología cibernética.

En 2012, surgió la Política de Defensa Cibernética por medio de la publicación de la *Portaria Ministerial* Nº 3.389, de 21de diciembre de 2012. Dos años después, fue publicada la Doctrina Militar de Defensa Cibernética por medio de la *Portaria Ministerial* Nº 3.010, de 18 de noviembre de 2014, en la cual se creó las bases para la creación del Comando de Defensa Cibernética (ComDCiber), estructura clave y a partir del cual avances importantes fueron dados directamente en el área de Ciberdefensa e indirectamente en el área de Ciberseguridad. En 2018, nuevo paso importante fue dado con la publicación de la Política Nacional de Seguridad de la Información, hecha mediante el Decreto Presidencial Nº 9.637, de 26 de diciembre de 2018, por medio de la cual se regló la gobernanza de la seguridad de la información bien como la renuncia a la licitación en los casos en que puede comprometer la seguridad nacional.

Sin embargo, fue a partir de la Estrategia Nacional de Seguridad Cibernética (e-Ciber) publicada mediante Decreto Presidencial Nº 10.222, de 5 de febrero de 2020, que relevante paso fue dado en el sentido de pasar del nivel hasta entonces limitado a la Ciberdefensa para el nivel Ciberseguridad, la cual pasó a tener como gestor el Gabinete de Seguridad Institucional del Presidente de la República. A pesar de haber sido publicada sin una Política Nacional de Ciberseguridad anteriormente publicada, lo que le daría mucha más efectividad, tal paso permitió


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

que avances importantes fuesen realizados en dirección a la consolidación de una política de seguridad cibernética en Brasil más madura delante las lecciones aprendidas por otras naciones más evolucionadas en la temática.

El anteproyecto de la Política Nacional de Ciberseguridad (PNCiber) en Brasil, disponible en el sitio de Gobierno de Brasil y desarrollado por el Gabinete de Segurança Institucional *(GSI)* (2023) ya fue presentado y está disponible para consulta al público, y hay previsión de ser apreciado por el Congreso Nacional brasileño aún en este año de 2023. En ella se prevé la creación de un Sistema Nacional de Ciberseguridad, de una Agencia Nacional de Ciberseguridad (ANCiber), de una "entidad" supervisora llamada Comité Nacional de Ciberseguridad (CNCiber) y de una Oficina de Gestión de Seguridad (Cyber)Crises, cuyo acrónimo será GGCiber.

Otro paso importante dado en dirección la gestión de crisis en incidentes de naturaleza cibernética fue la creación, por la Presidência da República (2021), de la Red Federal de Manejo de Incidentes Cibernéticos (Regic) (Decreto Presidencial Nº 10.748, de 16 de julio de 2021), la cual tiene como objetivo mejorar y mantener la coordinación entre los órganos y entidades de la administración pública federal, directa, autárquica y base para la prevención, tratamiento y respuesta a incidentes cibernéticos, con el fin de elevar el nivel de resiliencia de seguridad cibernética de sus activos de información. Entre los objetivos previstos en el texto de la citada Red están: difundir medidas de prevención, tratamiento y respuesta a incidentes cibernéticos; compartir alertas sobre ciberamenazas y vulnerabilidades; divulgar información sobre ciberataques; promover la cooperación entre los participantes de la Red; y promover la rapidez en la respuesta a incidentes cibernéticos.

La Red Federal de Manejo de Incidentes Cibernéticos (Regic) tiene como órgano coordinador el Departamento de Seguridad de la Información de la Oficina de Seguridad Institucional de la Presidencia de la República (GSI/PR en Brasil). El órgano ejecutivo-operativo es el Centro de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos Gubernamentales, éste ubicado en el más alto nivel (político), y es el único *Computer Security Incident Response Team* (CSIRT) responsable en el ámbito de la administración pública federal brasileña por la coordinación de la Regic, conforme GSI (2022) citado en el Plan de Gestión de Incidentes Cibernéticos para la Administración Pública Federal (Plangic) aprobado mediante la *Portaria* Nº 120, de 21 de diciembre de 2022.

Por fin, una imagen abajo que compila todos los niveles con responsables del sector cibernético de Brasil, desde la Ciberseguridad hasta la Guerra Cibernética, con la Oficina de Seguridad Institucional de la Presidencia de la República (GSI/PR en Brasil) conduciendo el nivel político; el MD, EMCFA[9] y FF. AA el nivel estratégico; y el ComDCiber el nivel operacional.

[9] EMCFA, acrónimo que significa Estado Mayor Conjunto de las FF. AA.

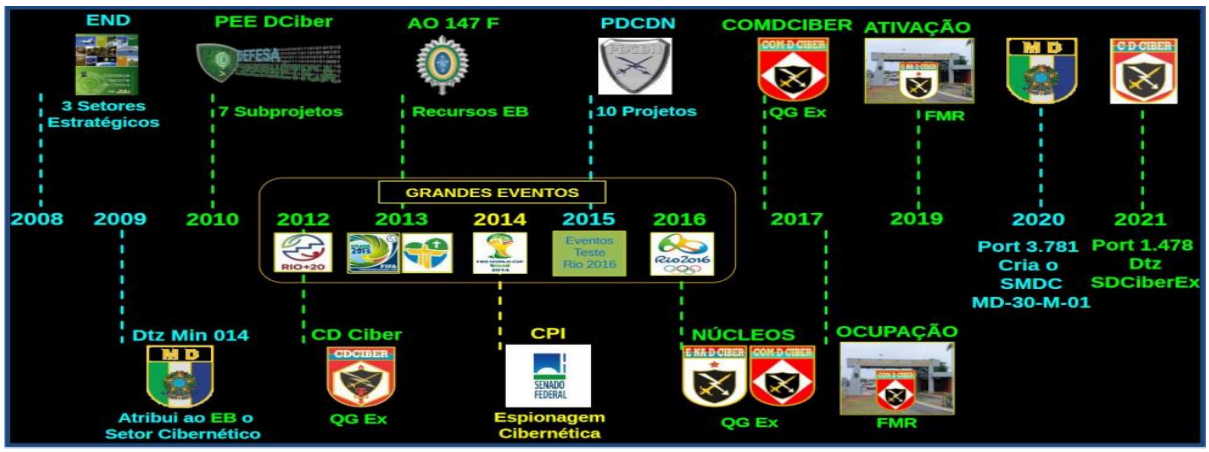


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu


Fuente: Imagen del Manual Doctrina de Operaciones Conjuntas del MD (2020)

## Estructura de Ciberdefensa

Con relación a la estructura de Ciberdefensa, Brasil ha evolucionado bastante desde que la Política Nacional de Defensa (PND) y la Estrategia Nacional de Defensa (END) fueron publicadas en 2008, momento a partir del cual empezaron una serie de medidas en el ámbito del Ministerio de Defensa (MD) para orientar las actividades de Ciberdefensa, en el nivel estratégico, y de Guerra Cibernética, en los niveles operativo y táctico, con miras al logro de los objetivos planteados. La figura abajo muestra como ocurrió la evolución del marco legal relacionado a la cibernética en Brasil, bien como cuando algunas estructuras surgieron en el MD para cumplir la misión de implementación de ese sector en Brasil:




Fuente: Imagen de Presentación del Estado Mayor del Ejercito (EME).

Teniendo en cuenta la línea del tiempo, luego después de la Directiva Ministerial nº 14 de 2009 que atribuyó oficialmente al Ejército Brasileño (EB) la responsabilidad de coordinar el Sector Cibernético en el ámbito de la Defensa se activó, en 2 de agosto de 2010, el Núcleo del Centro de


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Defensa Cibernética. Dos años más tarde, el 21 de diciembre de 2012, fue publicada la Política Cibernética de Defensa, por medio de la Portaria Ministerial Nº 3.389, cuya finalidad fue orientar, en el ámbito del Ministerio de la Defensa (MD), las actividades de Cibernética tanto en el nivel estratégico como en los niveles más bajos (operacional y táctico), además de desarrollar y mantener actualizada la doctrina de empleo del Sector Cibernético.

En fines de 2014, surgió la Doctrina Militar de Defensa Cibernética mediante publicación de la Portaria Ministerial Nº 3.010, creando las bases de la doctrina de Ciberdefensa en el ámbito del MD, y contribuyendo a la acción conjunta de las Fuerzas Armadas en la defensa del ciberespacio en Brasil. Cabe resaltar que fue a partir de esta publicación que se pasó a visualizar la necesidad de crearse un Comando de Defensa Cibernética (ComDCiber), algo que ocurriría un poco más tarde con la evolución doctrinaria y creación del Sistema Militar de Defensa Cibernética (SMDC) en 2020.

El Sistema Militar de Defensa Cibernética fue instituido por medio de la Portaria Ministerial N° 3.781, de 17 de noviembre de 2020, la cual definió el Comando de Defensa Cibernética (ComDCiber) como organismo central, conjunto, con la competencia para proponer y ejecutar acciones colaborativas con naciones amigas en el Sector Cibernético de Defensa, incluso a través de la interacción con organizaciones internacionales. Su definición conforme consta en la Portaria citada del Ministerio da Defesa (2020) es la siguiente:

*"un conjunto de instalaciones, equipos, doctrina, procedimientos, tecnologías, servicios y personal indispensables para llevar a cabo acciones encaminadas a asegurar el uso efectivo del ciberespacio por parte de la Defensa Nacional, así como prevenir o dificultar acciones hostiles contra sus intereses."*

Aún conforme Ministerio da Defesa (2020), el SMDC está compuesto por el Comando de Defensa Cibernética (ComDCiber), como órgano central; estructuras de Defensa Cibernética de cada una de las Fuerzas Armadas; estructuras de Guerra Cibernética de Comandos Operacionales activados; y otras estructuras incluidas en el Sistema, incluyendo los sectores de la administración central y los organismos vinculados al Ministerio de Defensa.

Importante señalar que concomitantemente a la creación del SMDC, toda la Doctrina de Operaciones Conjuntas de Brasil fue perfeccionada y adaptada a la nueva realidad decurrente del surgimiento de la quinta dimensión (el ciberespacio), éste enmarcado por "la transversalidad y la ausencia de fronteras físicas, siendo posible, en cualquier situación, la necesidad de una acción cibernética contra blancos ubicados fuera del TO/AOp[10]", conforme cita Ministerio de la Defensa (2020) en la última edición de la Doctrina de Operaciones Conjuntas publicada el 15 de septiembre de 2020 (pág. pág. 80/238).

Con respecto a la estructura del ComDCiber, la Doctrina de Operaciones Conjuntas publicada por Ministerio de la Defensa (2020), establece el siguiente organigrama de forma a permitir que ese Comando Operacional cumpla su misión:

[10] TO/AOp – Teatro de Operaciones/Área de Operaciones (en portugués).



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu


Fuente: Imagen del Manual Doctrina de Operaciones Conjuntas del MD (2020)

Conforme Ministério da Defesa (2020), son las siguientes las atribuciones de cada uno de los integrantes del ComDCiber:

- Centro de Defensa Cibernética - misión de ejecutar la parte operativa del ComDCiber ligadas a las actividades de Ciberdefensa (a cargo del Ejército Brasileño);

- Centro de Gestión Estratégica - misión de desarrollar capacidades cibernéticas, en las áreas de: relación institucional, gestión de talentos, gestión del conocimiento, así como coordinar actividades de investigación, desarrollo e innovación (a cargo de la FAE);

- Centro de Coordinación de Operaciones Cibernéticas - misión de aplicar las capacidades cibernéticas, en el ámbito del SMDC, realizando la planificación de operaciones y acciones conjuntas, combinadas e interinstitucionales para contribuir al uso efectivo del espacio cibernético, impidiendo o dificultando su uso en contra de los intereses de la Defensa Nacional (a cargo de la Marina de Brasil);

- Escuela Nacional de Defensa Cibernética - misión de promover la capacitación de recursos humanos (RH) del Sector Cibernético, promover y difundir las capacidades necesarias para la Defensa Cibernética en el ámbito de la Defensa Nacional, además de contribuir a las áreas de investigación, desarrollo, operación y gestión de la Ciberdefensa para la mejora de la cualificación de la mano de obra nacional para el sector (a cargo del Ejército Brasileño).

Es relevante citar que debido a su considerable conocimiento agregado, infraestructura y madurez obtenida a lo largo de los últimos años, el Comando de Defensa Cibernética (ComDCiber) colabora con el Departamento de Seguridad de la Información de la Oficina de Seguridad Institucional de la Presidencia de la República (GSI/PR, en Brasil), en un esfuerzo por aumentar la protección cibernética de las infraestructuras críticas, buscando reducir la posibilidad de amenazas que explotan vulnerabilidades en los activos informacionales que podrían comprometer la defensa nacional.

Cabe aún destacar la actuación cooperativa del MD y FF. AA en la mejoría de la capacitación de los RH involucrados en asuntos de Ciberseguridad/Ciberdefensa, la cual ha ocurrido anualmente por medio del ejercicio simulado llamado (en portugués) "*Ejercicio Guardião Cibernético* (*EGC*)", éste totalmente coordinado por el ComDCiber. Ya en su quinta edición prevista a ocurrir en 2023, la actividad cuenta con la participación de entidades públicas gubernamentales, Fuerzas Armadas, Universidades y Sector Privado vinculados a las siguientes áreas prioritarias: agua, comunicaciones, energía, finanzas, transporte y bioseguridad. Abajo una imagen que compila las entidades que participaron del EGC 3.0, realizado en 2021, el cual contó con la participación de 75 entidades, y un efectivo de 350 participantes y observadores.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu


Fuente: Imagen de Presentación del Estado Mayor del Ejercito (EME).

A seguir, la estructura del Sistema Nacional de Seguridad de la Información instituyo por medio de la Política Nacional de Seguridad de la Información, publicada en 2018, en la cual se incluye el Sistema Militar de Defensa Cibernética creado en 2020, permitiendo una visualización más clara y amplia de la estructura de Ciberdefensa brasileña por niveles (político, estratégico, operacional y táctico). Es importante recordar que con la creación de la Oficina de Seguridad Institucional de la Presidencia de la República (GSI/PR en Brasil), en 2001, cupo a este nuevo órgano, entre otras competencias, la coordinación de las actividades de Seguridad de la Información en el nivel político.


Fuente: Imagen de Presentación del Estado Mayor del Ejercito (EME).

## Conclusión parcial

Por fin, con relación a programas y proyectos del Sector Cibernético de Defensa, existe dos actualmente vigentes: uno ligado al Sistema Militar de Defensa Cibernética, llamado "Programa de la Defensa Cibernética en la Defensa Nacional (PDCDN)" y otro dentro del Sistema Defensa Cibernética del Ejército llamado "Defesa Cibernética" (Prg EE Def Ciber[11]), además de una acción estratégica dentro del Plano Estratégico del Ejército que promueve la participación en foros y actividades internacionales. Tal acción permite por ejemplo que militares participen de eventos de gran relevancia a nivel mundial como el ejercicio llamado "*Locked Shields*" coordinado por el

[11] Programa Estratégico do Exército Defesa Cibernética, en portugués.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

*Cooperative Cyber Defence Centre of Excellence* (CCDCOE) de la OTAN, permitiendo el incremento continuado de las capacidades cibernéticas de intereses de la Defensa y del País.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# CHILE

## Generalidades

Chile está ubicado en la costa occidental de América d Sur. Limita al Norte con Perú, al Este con Bolivia y Argentina, al Oeste con el Océano Pacífico. La población aproximada es d 19 millones de personas, su capital es Santiago, la moneda ofici es el peso chileno, su cotización en el mercado es un dólar americano por 844,57 pesos. El español es el idioma oficial. (Wikipedia , 2022)

El 18 de septiembre de 1810 es la fecha en la cual se proclamó la independencia de Chile, es una república democrática con un sistema presidencialista, su actual presidente es Gabriel Boric. Se caracteriza por ser un país largo y estrecho que se extiende desde el Desierto de Atacama en el norte hasta la región de la Patagonia en el sur.

Chile es considerado uno de los países más desarrollados de América Latina, los sectores más importantes para su economía y desarrollo son la minería con el cobre, carbón y nitrato; los productos manufacturados destacándose el procesamiento de alimentos, productos químicos, madera, y la agricultura, pesca, viticultura y fruta.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de las Fuerzas Armadas

Están compuestas por tres ramas principales: el Ejército de Chile, la Armada de Chile y la Fuerza Aérea de Chile, y posee un efectivo de 122.000 soldados. El Ejército tiene como misión la defensa y seguridad del territorio nacional, así como de la participación en ayuda humanitaria. La Armada de Chile es responsable de la defensa y seguridad marítima del país, protección de la Zona Económica Exclusiva, operaciones de búsqueda y rescate, y operaciones humanitarias. La Fuerza Aérea tiene como misión la defensa aérea y del espacio aéreo chileno, búsqueda y rescate, y en misiones de apoyo humanitario[12]. Militares de las tres ramas pueden participar en operaciones de paz tanto en misiones individuales como integrando tropas. (https.//es.wikipedia.org > wiki > Fuerzas_Armadas_de_Chile, 2022)

Dentro de los conflictos más importantes a lo largo de su historia, se destacan las guerras de independencia hispanoamericana (1810 – 1829), la Guerra del Pacífico (1879 – 1884) contra Perú y Bolivia. Actualmente, existe un conflicto entre el Estado de Chile y el pueblo Mapucheque, el cual tiene como base la disputa por territorios indígenas. Además, existe un reclamo por parte de Bolivia que exige su salida al mar luego de haberla perdido en la Guerra del Pacífico.

## Estructura de Ciberseguridad

Política Nacional de Ciberseguridad

En su política nacional se destaca como principales aspectos que son considerados para atender las amenazas presentes en esta nueva dimensión, resaltan las siguientes (www.ciberseguridad.gob.cl Política Nacional de CIberseguridad, 2017):

a. Se identifica las instituciones involucradas en ciberseguridad;

[12]https.//es.wikipedia.org > wiki >Fuerzas_Armadas_de_Chile



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

b. Proporciona una descripción general de riesgos y amenazas;

c. Identifica los objetivos de política a alcanzar para 2022;

d. Establece lineamientos para lograr una infraestructura de información robusta y resiliente, preparada para enfrentar y recuperarse de incidentes de ciberseguridad, bajo un enfoque de gestión de riesgos;

e. Los derechos de las personas a ser protegidos en el ciberespacio;

f. Desarrollo de una cultura de ciberseguridad basada en la educación, las buenas prácticas y la rendición de cuentas en el manejo de las tecnologías digitales;

g. Las acciones de cooperación con otras partes interesadas en el campo de la ciberseguridad y participación en foros y discusiones internacionales; y

h. Promover el desarrollo de una industria de ciberseguridad al servicio de sus objetivos estratégicos.

Es mes de mayo del 2023, se presentó al actual gobierno una nueva política de 2023-2028, entregada al presidente Gabriel Boric, que se estructura en cinco ejes que busca "proteger a las personas y al país" (www.trentic, 2023), se detalla que los ciudadanos cada vez más emplean la tecnología para ingresar a su banco, hacer trámites, compran cosas, entregando información sensible de su patrimonio y de su seguridad personal.

Esto obliga al Estado a disponer de instituciones que garanticen la seguridad de sus datos, sea en el interior, como desde el exterior del Estado. "Todo el trabajo y los avances que estamos haciendo en materia de brecha digital, en esta política de ciberseguridad, de protección de datos, son medidas que se articulan para poder avanzar hacia una transformación digital más justa, basada en una perspectiva de derechos y también de perspectiva de género». (www.trentic, 2023)

Esta nueva propuesta de la política de Ciberseguridad está diseñada sobre la base a cinco objetivos estratégicos:

a. Infraestructura resiliente: preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una perspectiva de gestión de riesgos;

b. Derechos de las personas: promoviendo la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materias de ciberseguridad;

c. Cultura de ciberseguridad: en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas;

d. Coordinación nacional e internacional: con el sector público como privado, e internacionalmente con países, organismos, instituciones, y otros actores internacionales, para enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio; y

e. Fomento a la industria y la investigación científica: promover el desarrollo de una industria de la ciberseguridad, y fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad.

## Estrategia Nacional de Ciberseguridad

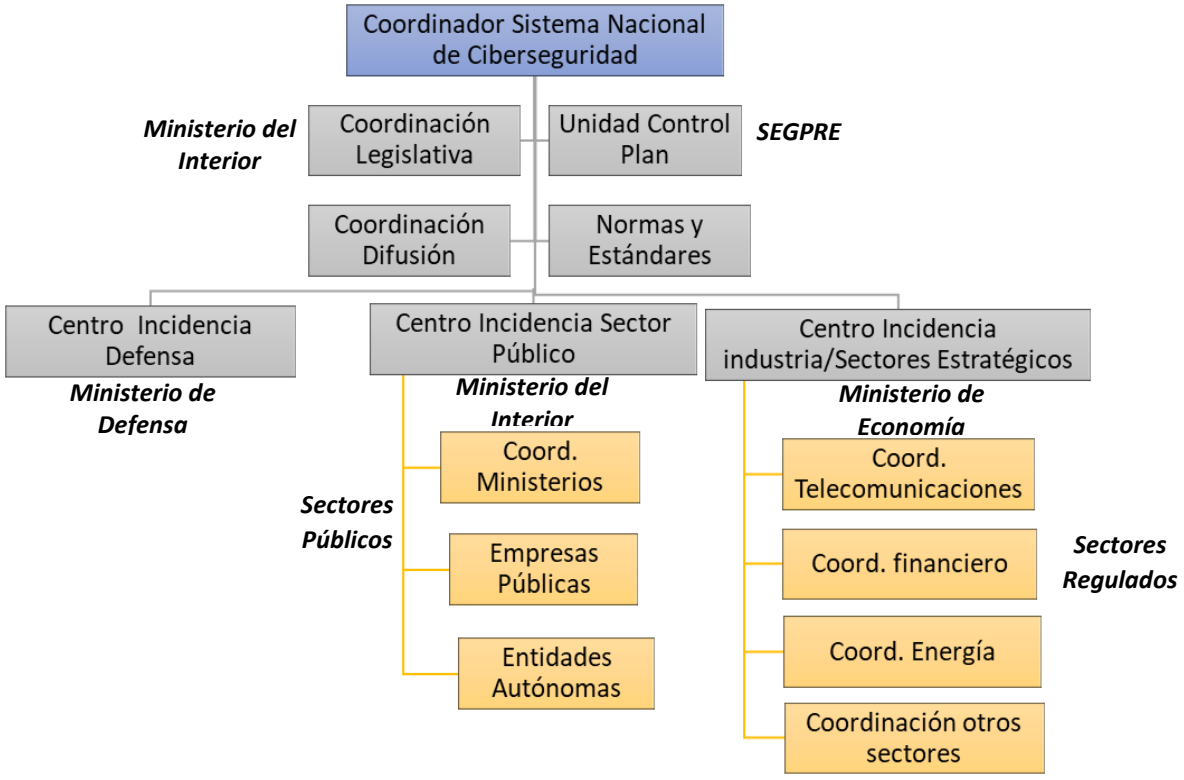
Para enfrentar las ciberamenazas que evolucionan permanentemente y que afectan a las naciones, a los ciudadanos, empresas, instituciones y al gobierno, en Chile la Estrategia Nacional de Ciberseguridad incluye al Gobierno Nacional, a los organismos de control, instituciones judiciales, Gobiernos Autónomos Descentralizados, empresas privadas, entidades académicas y financieras.

Sobre la protección de la infraestructura crítica, se indica que "es la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud". (https.//www.diarioconstitucional.cl >2023702/04, 2023)

En Chile la ciberseguridad está encabezada por el Coordinador del Sistema Nacional de Ciberseguridad, que tiene al Ministerio del Interior, como el ente coordinador, y responsable de la implementación de las normas que deben regir a los sectores públicos o privados que busque alcanzar el desarrollo digital más seguro.

En la estructura se considera la participación del Ministerio de Defensa, a cargo de los incidentes de defensa nacional, el Ministerio del Interior en el sector público, y el Ministerio de Economía en la coordinación con las distintas industrias y sectores estratégicos y la Secretaría General de la Presidencia que tendrá la gestión legislativa y llevar el control de gestión del plan.

Contribuyendo con este propósito las Fuerzas Amadas disponen del Comando de Ciberdefensa, unidad que es responsable de la protección y defensa de los sistemas y activos de información del país contra amenazas cibernéticas, y la Policía Nacional a través de la Dirección Nacional de Tecnologías de la Información y Comunicación con la sección de Ciberseguridad es la responsable de proporcionar alertas de los ciberataques que utilizan una amplia variedad de estrategias para acceder a un dispositivo o red, extorsionar o robar información valiosa.




Nota. Tomado de la Estrategia Nacional de Ciberseguridad de Chile

## Desafíos a la Ciberseguridad en Chile

La Ciberseguridad sin lugar a duda marca enormes desafíos para Chile, país que se ubica en el puesto 74 a nivel mundial en cuanto a las acciones realizadas en este campo, y que requiere ser afrontados con una mayor decisión, recursos y coordinación, entre los principales desafíos tenemos (https://www..camara.cl, 2022):

a. Avanzar en la legislación en lo que refiere a los delitos informáticos, ley marco de ciberseguridad, protección de datos personales;

b. Cierre de brechas, definición de estándares mínimos, enfoque colaborativo, coordinación en el manejo de crisis, entrenamiento;

c. Profundizar los mecanismos de coordinación internacional; y

d. Educación a través de campañas, foros, mediante una estrecha colaboración público-privada.

## Conclusión Parcial

La ciberseguridad es un tema que va ganando mayor importancia, debido a la tendencia mundial de los ciberataques. Chile ha sufrido varios ataques desde el ciberespacio, lo que ha exigido el establecimiento de leyes, políticas y estrategias, que requieren una evaluación y sobre todo continuidad, uno de los obstáculos más relevantes que enfrenta esta nación.

Las instituciones del Estado, y dentro de ellas las Fuerzas Armadas se encuentran preparándose para contrarrestar los efectos de las acciones de los perpetradores que abarcan los campos de la ciberseguridad, ciberdefensa, cibercrimen, ciberguerra, ciberinteligencia que son empleadas por esta amenaza.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# COLOMBIA

## Generalidades

La República de Colombia está ubicada al Norte de América del Sur, limita al Este con Venezuela y Brasil, al Sur con Perú y Ecuador y al Noreste con Panamá, posee costas sobre el Mar Caribe y sobre el Océano Pacífico, posee las islas de San Andrés, Providencia y Santa Catalina, frente a las costas de Costa Rica y Nicaragua, a 775 km de la costa continental. Su capital es Bogotá.

Población: la población aproximada es de 47.000.000 de habitantes.

Área: La República de Colombia posee una superficie de 2.070.408 km2, de los cuales 1.141.748 km2 corresponden al territorio continental y el resto al litoral marítimo.

Tipo de gobierno: es una República presidencialista.

PIB: El PBI se estima en unos 314.500 millones de dólares USD. Cuarta economía de América Latina, sexto productor de petróleo de toda América, gran productor y exportador de carbón, de piedras preciosas como las esmeraldas, los diamantes y el oro, tercer productor mundial de Café. Otro de los fuertes ingresos de divisas viene por el lado del turismo.

IDH (Índice de Desarrollo Humano): Según el informe del Programa de las Naciones Unidas para el Desarrollo (PNUD) de 2021, Colombia ocupa el puesto 88 entre 191 países evaluados con un puntaje de 0.752

Idioma: El idioma oficial de la República de Colombia es el español.

Historia de la República de Colombia: A principios del siglo XIX, las ideas independentistas se propagaron en Colombia, lideradas por figuras como Simón Bolívar y Francisco de Paula Santander. El 20 de julio de 1810, se inició el proceso de independencia con el grito de independencia en Bogotá. Después de una larga lucha, Colombia finalmente alcanzó su independencia de España el 7 de agosto de 1819 en la Batalla de Boyacá.

A principios del siglo XX, Colombia vivió cambios políticos y económicos significativos. En 1903, Panamá se separó de Colombia con el apoyo de Estados Unidos para formar su propio país. Colombia enfrentó períodos de inestabilidad política, guerras civiles y conflictos armados. En el nuevo milenio, Colombia continuó lidiando con desafíos, incluyendo el conflicto armado con grupos guerrilleros y narcotraficantes. Sin embargo, se realizaron esfuerzos significativos para lograr la paz, como los acuerdos de paz alcanzados con las FARC en 2016.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

Las Fuerzas Armadas Colombianas están integradas por unos 286.000 efectivos que prestan sus servicios en el Ejército, la Marina y la Fuerza Aérea.

El ejército Nacional fue creado en 1919, hoy lo integran unos 250.000 efectivos distribuidos en las 8 regiones militares en los que está dividido el territorio Nacional.

La Armada Nacional tiene su inicio en 1810 tras la conformación de la Comandancia General de Marina, en 1822 se creó la Escuela de Náutica, recién en 1907 se funda la Escuela Naval, la cual deja de funcionar junto con toda la Armada en 1909. Tras los acontecimientos bélicos con


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Perú de 1932, reaparece y toma forma la actual Armada de la República de Colombia. Hoy la fuerza está integrada por unos 35.000 efectivos de los cuales unos 24.000 componen el cuerpo de infantería de marina. En la actualidad la marina colombiana opera desde 7 fuerzas operativas y comandos.

La Fuerza Aérea Colombiana fue creada en 1919, participó activamente en la guerra que Colombia mantuvo con Perú entre 1932 y 1933. Durante la IIGM efectuó tareas de patrulla costera en el Pacifico y el Mar Caribe. En la actualidad al igual que las demás fuerzas, realiza tareas de Contra insurgencia dentro del territorio nacional. Hoy la FAC dispone de unos 13000 efectivos que prestan sus servicios desde diferentes Comandos Aéreos y Grupos Aéreos.

## Estructura de Ciberseguridad

Política Nacional de Seguridad Digital

El Consejo Nacional de Política Económica y Social República de Colombia define cinco áreas centrales de acción, que comprenden el Plan de Acción y Seguimiento:

a) Establecimiento de un marco institucional claro en torno a la seguridad digital;

b) Creación de condiciones que permitan a las partes interesadas gestionar el riesgo de seguridad digital en sus actividades;

c) Fortalecer la seguridad de las personas y del Estado en un entorno digital a nivel nacional y transnacional;

d) Fortalecer la defensa y la seguridad nacional con un enfoque de gestión de riesgos;

e) Creación de mecanismos permanentes para promover la cooperación, colaboración y asistencia en seguridad digital.

Ministerio de Defensa, Policía Nacional de Colombia

- Encargado de la ciberseguridad en el territorio colombiano, ofreciendo información, asistencia y protección contra el ciberdelito;
- Las actividades incluyen la prevención, asistencia, investigación y persecución de delitos informáticos en el país;
- Tiene un observatorio del cibercrimen (observatorio cibercrimen).

## Estructura de Ciberdefensa

Ministerio de Defensa Nacional

- Responsable de la coordinación en acciones de ciberseguridad y ciberdefensa para la protección de la infraestructura crítica de Colombia en caso de emergencias que amenacen o comprometan la seguridad y defensa nacional;
- Desarrolla y promueve procedimientos, protocolos y guías de buenas prácticas y recomendaciones en materia de ciberdefensa y ciberseguridad para infraestructuras críticas, y vela por su implantación y cumplimiento.

El Consejo Nacional de Política Económica y Social República de Colombia define tres objetivos específicos:

a) Implementar mecanismos apropiados para prevenir, brindar asistencia, controlar y ofrecer recomendaciones sobre incidentes cibernéticos y/o emergencias para la protección de infraestructura crítica;

b) Diseñar y ejecutar planes de formación especializados en ciberseguridad y ciberdefensa; y

c) Fortalecer el marco legal y la aplicación de la ley.

## Conclusión parcial

La República de Colombia ha desarrollado una Estrategia Nacional de Ciberseguridad para guiar las acciones y esfuerzos en este ámbito. Esta estrategia busca fortalecer la capacidad de respuesta y prevención en ciberseguridad, promover la conciencia y la educación sobre el tema, y coordinar los esfuerzos de diferentes entidades gubernamentales.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# ECUADOR

## Generalidades

Situado en la región noroeste de América del Sur, es un país diverso y geográficamente impresionante. Limita al norte con Colombia, al sur y al este con Perú, y al oeste con el océano Pacífico. Su ubicación en la línea ecuatorial le da su nombre y contribuye a su variada topografía, que abarca playas, montañas, selvas tropicales e Islas Galápagos.

La capital y ciudad más grande es Quito, mientras que Guayaquil, Cuenca, Ambato y Santo Domingo son otros centros urbanos significativos. Aunque el español es el idioma oficial, Ecuador valora sus lenguas indígenas como parte de su patrimonio cultural.

Con una población diversa que incluye grupos indígenas, mestizos y afroecuatorianos, Ecuador es conocido por su rica herencia cultural. Las Islas Galápagos, famosas por su biodiversidad y vínculo con Charles Darwin, destacan como un punto clave en la teoría de la evolución.

La economía ecuatoriana es variada, abarcando sectores como petróleo, agricultura, manufactura, turismo y servicios. El petróleo es un recurso de exportación crucial y una fuente de ingresos vital.

Ecuador atrae a turistas con su belleza natural, desde los majestuosos Andes hasta la selva amazónica y las playas costeras, sin olvidar las emblemáticas Islas Galápagos. Tanto Quito como Cuenca, ciudades con arquitectura colonial, han sido designadas Patrimonio de la Humanidad por la UNESCO.

La forma de gobierno en Ecuador es una república democrática presidencialista, con el presidente como jefe de Estado y de Gobierno. El país también destaca por su compromiso con la conservación ambiental, destacando las Islas Galápagos como un importante destino turístico ecológico y un centro de investigación científica

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

*Las Fuerzas Armadas de Ecuador* se componen de tres ramas principales: el Ejército Ecuatoriano, la Fuerza Aérea Ecuatoriana y la Armada del Ecuador, cada rama tiene sus propias responsabilidades y funciones específicas en la defensa y seguridad del país.

Misión: La misión principal de las Fuerzas Armadas es garantizar la soberanía, la integridad territorial y la seguridad del Ecuador. Esto incluye la protección de las fronteras, la participación en operaciones de ayuda humanitaria y la contribución a la estabilidad interna.

Historia: Las Fuerzas Armadas de Ecuador tienen una larga historia que se remonta a los procesos de independencia y la formación de las primeras fuerzas militares en el siglo XIX. A lo largo de los años, han participado en diversos eventos históricos y desafíos nacionales.

Participación Internacional: Las Fuerzas Armadas de Ecuador han participado en misiones de paz y cooperación internacional en diferentes partes del mundo, contribuyendo a esfuerzos internacionales para mantener la paz y la seguridad.

Educación y Formación: Las Fuerzas Armadas ecuatorianas cuentan con instituciones educativas y academias militares donde se capacita y forma a los miembros del ejército, la fuerza aérea y la armada.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Equipo y Tecnología: A lo largo de los años, Ecuador ha modernizado su equipo militar y ha invertido en tecnología para mejorar sus capacidades en áreas como defensa aérea, naval y terrestre.

Roles Adicionales: Además de su función principal de defensa y seguridad, las Fuerzas Armadas de Ecuador también pueden ser llamadas para ayudar en situaciones de desastre natural, como terremotos o inundaciones, brindando asistencia humanitaria y apoyo a la población civil.

Relación Civil-Militar: Las Fuerzas Armadas de Ecuador mantienen una relación civil-militar en la que están subordinadas al poder civil y respetan la autoridad democráticamente elegida.

Presupuesto y Recursos: El presupuesto asignado a las Fuerzas Armadas de Ecuador varía de acuerdo con las prioridades nacionales y las necesidades de defensa. Los recursos financieros se destinan a entrenamiento, equipo, operaciones y otros aspectos relevantes.

## Estructura de Ciberseguridad

El Ecuador reconoce y valora en gran medida la vital importancia de una *estructura de ciberseguridad* como un pilar fundamental en la protección tanto de la seguridad ciudadana como de la estatal en el vasto e interconectado ciberespacio. Esta conciencia responde a la creciente relevancia que ha adquirido la tecnología digital en todos los aspectos de la vida moderna, desde la comunicación y la economía hasta la administración gubernamental y la interacción social.

El país se posiciona en línea con una tendencia global en la que numerosos estados están reforzando sus capacidades de ciberseguridad para enfrentar los retos y amenazas que surgen en la era digital. Este enfoque estratégico se fundamenta en la premisa de que la seguridad cibernética se ha convertido en un elemento esencial para el éxito en el entorno digital actual.

La naturaleza sin fronteras de la seguridad informática resalta la importancia de la colaboración internacional en este ámbito. Las amenazas y los desafíos cibernéticos pueden trascender las barreras geográficas y afectar a múltiples naciones. En este sentido, Ecuador ha reconocido la necesidad de trabajar en conjunto con otras naciones y organizaciones internacionales para abordar de manera efectiva los riesgos cibernéticos y fortalecer las defensas en línea.

La contribución y respaldo de programas destacados, como el CICTE/OEA y CYBER4DEV, han sido elementos clave para el desarrollo y la formulación de la Estrategia Nacional de Ciberseguridad. Esta estrategia, diseñada para un período de tres años, presenta un enfoque holístico que abarca seis ejes de acción. Estos ejes, que incluyen la Gobernanza, la Resiliencia cibernética, la Prevención y el combate a la ciberdelincuencia, la Ciberdefensa, las Habilidades y capacidades de ciberseguridad, y la Cooperación internacional, forman un enfoque integral para abordar los desafíos cibernéticos desde múltiples perspectivas.

Es crucial resaltar que la ciberseguridad va más allá de la mera protección de datos y transacciones financieras. Su impacto se extiende al desarrollo digital, al fomento de la confianza en línea y a la salvaguardia de datos personales. En un mundo donde la información y los datos personales son considerados un activo valioso y se han convertido en un recurso crítico para la toma de decisiones, la ciberseguridad se convierte en una herramienta esencial para proteger estos activos y garantizar la privacidad de los ciudadanos.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Estructura de Ciberdefensa

*La ciberdefensa en el Ecuador* podemos destacar al Grupo de Defensa en el ámbito de las Ciberoperaciones desempeña un papel fundamental en la protección y salvaguardia de la infraestructura tecnológica de las Fuerzas Armadas. Su cometido es ejecutar y mantener medidas y acciones diseñadas para contrarrestar posibles amenazas y agentes hostiles en el ciberespacio. Esta tarea abarca una serie de funciones críticas:

El grupo de detección de actividades maliciosas está a cargo de monitorear de manera constante la actividad en línea para identificar patrones y comportamientos que puedan indicar actividades maliciosas o intentos de ataque cibernético.

En la Prevención y Mitigación de Ataques Cibernéticos, podemos indicar que la detección temprana es clave, pero también lo es la capacidad de prevenir y minimizar los efectos perjudiciales de los ataques. Este grupo trabaja en estrategias proactivas para evitar la infiltración y propagación de ataques cibernéticos.

Una tarea esencial es evaluar constantemente la seguridad de los sistemas de tecnologías de la información y comunicaciones (TIC) propios. La identificación de vulnerabilidades permite tomar medidas correctivas antes de que se conviertan en vectores de ataque.

El Grupo de Defensa se encarga de manejar el incidente de manera eficiente y llevar a cabo la recuperación de los sistemas afectados. La agilidad en la respuesta es esencial para minimizar el impacto.

El Grupo de Exploración se dedica a recolectar información detallada sobre las cibercapacidades y vulnerabilidades de los sistemas de información y comunicaciones del posible adversario. Esta labor se conoce como ciberinteligencia y es esencial para comprender y anticipar las tácticas, técnicas y procedimientos de posibles amenazas:

La Ciberinteligencia, a través de técnicas avanzadas de recolección de información en línea, este grupo busca obtener un conocimiento profundo sobre las capacidades cibernéticas de actores adversarios. Esto incluye identificar posibles puntos débiles que puedan ser explotados.

El Grupo de Respuesta opera en la ofensiva, ejecutando acciones en función de las necesidades operativas del Centro de Operaciones Cibernéticas (COCIBER). Su objetivo es neutralizar, interrumpir, alterar o incluso destruir amenazas y ataques de posibles adversarios:

En caso de que se detecten ataques cibernéticos en curso, este grupo está preparado para responder de manera rápida y efectiva, contrarrestando la amenaza y minimizando su impacto.

Cuando es necesario, el Grupo de Respuesta puede llevar a cabo operaciones ofensivas dirigidas a la infraestructura crítica digital del enemigo. Esto busca generar efectos deseados, como interrumpir sus operaciones o neutralizar sus capacidades.

## Conclusión Parcial

Finalmente se puede concluir que Ecuador concede gran importancia a la ciberseguridad para proteger tanto la seguridad ciudadana como estatal en un mundo digitalmente interconectado, el país se une a la tendencia mundial de fortalecer la ciberseguridad y reconoce la necesidad de colaboración internacional debido a la naturaleza global de las amenazas cibernéticas. La Estrategia Nacional de Ciberseguridad, basada en seis ejes de acción busca establecer una estructura robusta, organizada, moderna, va más allá de proteger datos; también impulsa el desarrollo digital y protege la privacidad. La estructura de ciberdefensa de Ecuador incluye grupos especializados en la defensa, exploración y respuesta ofensiva en el ciberespacio.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# GUYANA

## Generalidades

Guyana, oficialmente la República Cooperativa de Guyana (en inglés, *Co-operative Republic of Guyana*) es un país de América del Sur, ubicado en la costa norte de América del Sur, miembro de la UNASUR, CELAC y miembro asociado del Mercosur. Limita al norte con el océano Atlántico, al este con Surinam, al oeste con Venezuela y Brasil, y al sur con Brasil. De 1831 a 1966 constituyó la colonia denominada Guayana británica. La ciudad más poblada es su capital Georgetown.

CAPITAL Georgetown.
POBLACIÓN 743.699 (165°).
IDIOMA Oficial es el inglés.
FORMA DE GOBIERNO Semipresidencialista.
PRESIDENTE Irfaan Ali.
PRIMER MINISTRO Mark Phillips.
SUPERFICIE 214.969 km².
FRONTERAS 2933 Km y línea de costa 459 km.
PIB USD 29.517 millones (138°).
IDH (2021) 0,714 (108°) El IDH, tiene en cuenta tres variables: vida larga y saludable, conocimientos y nivel de vida digno.
MONEDA Dólar guyanés.
ECONOMIA La agricultura, que ocupa la mayor de la PEA.

Entre las principales exportaciones agrícolas de Guyana es el cacao, el café y, sobre todo, el azúcar. La actividad pesquera, favorecida por la plataforma continental, permite la venta al exterior de camarones. Otra gran riqueza del país es la bauxita (industria del aluminio). Existen yacimientos de diamantes y oro, y notables reservas madereras, han surgido algunas industrias de bienes de consumo (textiles). Desde el descubrimiento de importantes reservas de petróleo crudo frente a la costa atlántica ha tenido un gran impacto en el PIB de Guyana desde que comenzó la perforación en 2019. El PIB creció considerablemente (43 %) durante el año de la pandemia de COVID-19 de 2020, y se prevé que continúe a un ritmo alto nivel en 2021 (estimado en 20%). También es fuente de ingreso para su economía la emisión de sellos postales destinados, principalmente, al coleccionismo filatélico.

Historia

Guyana es un país ubicado en la costa norte de América del Sur. Su historia está marcada por una serie de influencias culturales y coloniales, así como por su lucha por la independencia y el desarrollo como nación. Aquí hay un resumen breve de la historia de Guyana:

Época Precolombina: Antes de la llegada de los europeos, la región que ahora es Guyana estaba habitada por diversas comunidades indígenas, incluidos los arawakos y los caribes.

Colonización Europea: A fines del siglo XV, exploradores europeos como los españoles y los neerlandeses llegaron a la región. Los neerlandeses establecieron una colonia llamada Essequibo en el área que es ahora Guyana. Más tarde, los británicos tomaron el control de varias partes de la región.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Dominio Británico: En el siglo XIX, la Guayana Británica (como se llamaba entonces) se convirtió en una colonia británica. La economía se basaba en la producción de azúcar, arroz y otros cultivos, utilizando el trabajo forzado de los esclavos africanos e, más tarde, de los trabajadores contratados.

Movimiento hacia la Independencia: Después de la Segunda Guerra Mundial, hubo un creciente movimiento hacia la independencia en la Guayana Británica. En 1966, obtuvo el autogobierno y se convirtió en un estado autónomo dentro del Imperio Británico.

Independencia: El 26 de mayo de 1966, Guayana se convirtió en una nación independiente, pero siguió siendo parte de la Mancomunidad de Naciones (Commonwealth) con la reina Isabel II como su jefa de Estado.

Desarrollo Político y Étnico: La política guyanesa a menudo ha estado influenciada por tensiones étnicas entre las comunidades indo-guyanesas y afro guyanesas. Esto ha llevado a veces a conflictos y desafíos en la estabilidad política.

Años de Gobierno Autoritario: Durante las décadas de 1970 y 1980, Guyana experimentó un período de gobierno autoritario bajo el presidente Forbes Burnham y su partido, el Congreso Nacional del Pueblo (PNC).

Democracia y Cambio Político: En la década de 1990, Guyana experimentó una transición hacia la democracia. En 1992, el PNC fue derrotado en las elecciones generales y el poder pasó al Partido Progresista del Pueblo (PPP).

Descubrimiento de Petróleo: En los últimos años, Guyana ha experimentado un cambio significativo en su economía con el descubrimiento de importantes reservas de petróleo en aguas marítimas. Esto ha impulsado el crecimiento económico y plantea desafíos y oportunidades para el país.

## Datos de las Fuerzas Armadas

Las Fuerzas de Defensa de Guyana conocidas por sus siglas en inglés como GDF fueron creadas el 1 de noviembre de 1965, el alistamiento en la institución es de carácter voluntario para los oficiales y soldados. La formación básica se realiza dentro de las escuelas de formación de las GDF, que también ha entrenado oficiales y soldados de otros territorios del Caribe vinculados a la Commonwealth. Sin embargo, los oficiales también se forman en dos de las escuelas de formación británicas oficiales de renombre mundial: La Real Academia Militar de Sandhurst (Royal Military Academy Sandhurst) en donde se entrena la Infantería; y el Real Colegio Naval Britannia (Britannia Royal Naval College) que es el encargado de la formación de la Guardia Costera. (WIKIPEDIA). Hasta el 2021 disponían de 4.000 efectivos

En la actualidad Guyana mantiene diferendos limítrofes con otros países, especialmente Venezuela y Surinán , aproximadamente las tres cuartas partes del oeste del país son reclamadas por Venezuela, específicamente 159 542 km², lo que representa el 74,21 % del territorio, zona llamada por esta como Guayana Esequiba. Su otro vecino, Surinam, reclama para sí una parte del territorio oriental al sureste del país, concretamente unos 15 600 km² denominada Región de Tigri, lo que representa actualmente el 7,26 % del país.

## Estructura de Ciberseguridad

Guyana es una democracia parlamentaria en la que la libertad de expresión y el derecho a la información están garantizados por la Constitución, pero la ley no siempre se aplica con rigor. Las

autoridades no dudan en recurrir a las demandas por difamación contra los medios críticos, y la amenaza del acoso judicial puede ser suficiente para disuadir a los periodistas de continuar una investigación. En los últimos años, el país ha adoptado una legislación dirigida a amordazar a los periodistas no afines con las autoridades. Los textos incluyen un proyecto de ley contra la difamación que prevé multas y penas de prisión de hasta dos años "para detener a los periodistas que se oponen a los partidos políticos". (RSF)

Actualmente Guyana no cuenta con una legislación en materia de delitos informáticos. (Portal Interamericano de Delitos Cibernéticos), pero existen una legislación que penaliza delitos contra la interceptación de las comunicaciones, adicional con fecha 16 de agosto se publica una ley que penaliza el cibercrimen.

No se tiene información específica sobre la estructura exacta de la ciberdefensa y ciberseguridad de Guyana. En general, la ciberdefensa y ciberseguridad de un país suelen organizarse en varias capas y agencias gubernamentales, en colaboración con el sector privado y otras entidades. Alguna de las posibles características de la estructura de ciberseguridad de Guyana puede ser:

Agencia Nacional de Ciberseguridad: Muchos países establecen una agencia gubernamental central encargada de la ciberseguridad. Esta agencia suele ser responsable de coordinar y supervisar los esfuerzos de ciberseguridad en todo el país, así como de desarrollar políticas y estrategias relacionadas con la ciberseguridad.

Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT): Estos equipos son responsables de manejar y responder a incidentes de seguridad cibernética en el país. Trabajan para identificar y mitigar amenazas cibernéticas, así como para proporcionar asistencia a organizaciones afectadas.

Colaboración con el sector privado: La colaboración entre el gobierno y el sector privado es esencial para fortalecer la ciberseguridad. Las empresas suelen desempeñar un papel crítico en la detección y respuesta a amenazas cibernéticas, y el gobierno puede trabajar en estrecha colaboración con ellas para compartir información y mejores prácticas.

Educación y Concienciación: Las campañas de educación y concienciación son fundamentales para promover buenas prácticas de ciberseguridad en toda la población. Esto puede incluir la capacitación de empleados en empresas, la promoción de hábitos seguros en línea y la educación de estudiantes sobre la importancia de la ciberseguridad.

Leyes y Regulaciones: Muchos países implementan leyes y regulaciones relacionadas con la ciberseguridad para establecer estándares mínimos de seguridad y establecer responsabilidades legales en caso de incidentes.

Cooperación Internacional: La ciberseguridad es un problema global, por lo que la cooperación internacional es esencial. Guyana podría colaborar con otros países, organizaciones internacionales y agencias de seguridad cibernética en la lucha contra amenazas cibernéticas transfronterizas.

## Estructura de Ciberdefensa

De igual manera a lo que se describió en ciberseguridad no se pudo encontrar la bibliografía donde se pueda detallar el aspecto de ciberdefensa de Guyana.

## Conclusión parcial

La ciberdefensa y ciberseguridad son dos conceptos fundamentales para la protección de la infraestructura tecnológica y la información digital sensible de un país. Al vivir en un mundo cada vez más interconectado y digitalizado, las amenazas cibernéticas son constantes y evolucionan rápidamente. La falta de una estrategia sólida de ciberdefensa y ciberseguridad podría exponer a un país a riesgos como el robo de información, ataques cibernéticos a infraestructuras críticas, espionaje y sabotaje cibernético, entre otros.

Es esencial que los gobiernos y las organizaciones en todo el mundo, incluida Guayana, reconozcan la importancia de invertir en la ciberdefensa y ciberseguridad para la protección de su información. Esto implica la implementación de leyes, medidas técnicas, regulaciones, políticas y programas de concientización para proteger tanto los activos digitales como la privacidad de los ciudadanos.

Ante la evolución de las amenazas de la información digital, se vuelve imperioso que se mantenga un enfoque proactivo y se esté dispuesto a adaptarse a medida que aparezca nuevas formas de ataques y vulnerabilidades. La cooperación con otros países se vuelve imperioso para abordar estos nuevos desafíos referente a la seguridad en la era digital.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# GUAYANA FRANCESA (FRANCIA)

## Generalidades

La Guayana Francesa es un territorio francés de ultramar en América del Sur. Limita con el Océano Atlántico al norte y al este, Brasil al sur y Surinam al oeste. Su capital es Cayena.

Población: a partir de 2021, la población estimada fue de aproximadamente 294.071 habitantes.

Superficie: Guayana Francesa cubre un área de aproximadamente 83.534 kilómetros cuadrados, lo que la convierte en la región más grande de Francia.

Tipo de gobierno: Gobierno local, es parte integral de la República Francesa y está sujeta a la ley y la soberanía francesas.

PIB: La economía de la Guayana Francesa está vinculada a Francia y se beneficia de los programas y fondos de la Unión Europea. Su PIB se basa en sectores como la aviación, la pesca, la agricultura, la minería y el turismo.

IDH (Índice de Desarrollo Humano): (0,862) según el informe del Programa de las Naciones Unidas para el Desarrollo (PNUD) de 2020, el IDH de la Guayana Francesa es alto y está por encima del promedio mundial.

Idioma: El francés es el idioma oficial de la Guayana Francesa, ya que es un territorio francés de ultramar. Historia de la Guayana Francesa:

La historia de la Guayana Francesa está fuertemente ligada a la colonización europea. Los exploradores franceses llegaron a la región en el siglo XVI. Durante siglos hubo un conflicto territorial entre Francia y los Países Bajos (ahora Surinam) por el control de la región. Más tarde, en el siglo XIX, la mayor parte de la Guayana Francesa quedó bajo control francés. En el siglo XIX y principios del XX, la Guayana Francesa fue eliminada como lugar de exilio para prisioneros y convictos, lo que llevó a la famosa prisión de la Isla del Diablo (Îles du Salut). Con el tiempo, la población de la Guayana Francesa se diversificó con la llegada de inmigrantes de todo el mundo, incluidos africanos, asiáticos e indios.

## Datos de Fuerzas Armadas

Las Fuerzas de Defensa de Guayana o (Guyana Defence Force) fueron creadas el 1 de noviembre de 1965. Las GDF no solo cumplen con su función militar, sino que también contribuyen a mejorar la infraestructura del país con la construcción de rutas y aeródromos.

Las GDF distribuyen sus elementos en el Comando del Ejército, el Comando de Aviación y el Comando de Guarda Costas.

La unidad de tierra de la Guyana Defence Force cuenta con unos 900 efectivos más otros 500 pertenecientes a la reserva.

Principales misiones:

- Defender la integridad territorial de Guayana.
- Ayudar al poder civil en el mantenimiento de la ley y el orden cuando de ser necesario hacerlo.
- Contribuir al desarrollo económico de Guayana.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

- Contribuir a la paz de la región
-

## Estructura de Ciberseguridad

La Estrategia Nacional de Seguridad Digital tiene como objetivo acompañar la transición digital de la sociedad francesa y abordar los nuevos desafíos de los usos cambiantes de la tecnología digital y las amenazas asociadas.

A mediados de 2009 se creó la Agencia Nacional para la Seguridad de Sistemas de Información (ANSSI) con la misión de proteger los sistemas nacionales de información y proponer las normas que debían aplicarse para la protección de los sistemas estatales y verificar la aplicación de las medidas adoptadas.

En febrero de 2011, la ANSSI presentó la Estrategia Nacional de Ciberseguridad de Francia. Sobre la base de lo establecido en su Libro Blanco de Defensa y la Seguridad, el documento establece cuatro objetivos:

- Convertir a Francia en una potencia mundial en defensa cibernética.
- Salvaguardar la capacidad de Francia para tomar decisiones a través de la protección de la información relacionada con su soberanía y las autoridades gubernamentales y actores de gestión de crisis deben disponer de los recursos para comunicarse en cualquier situación y en total confidencialidad por medio de redes que cumplan con esta necesidad, en particular a nivel local, lo que garantice la confidencialidad de la información que circula por ellas.
- Fortalecer la ciberseguridad de las infraestructuras nacionales críticas para que funcionen correctamente, en las que la sociedad es cada vez más dependiente de sistemas de información y redes, en particular Internet. Evitar cualquier ataque con éxito sobre un sistema de información crítico de Francia que pudiera tener consecuencias económicas graves o humanas. Estrechar la colaboración con los fabricantes y operadores de equipos pertinentes para que el estado garantice y mejore la seguridad de estos sistemas críticos.
- Garantizar la seguridad en el espacio cibernético en el que las amenazas a los sistemas de información afectan simultáneamente los servicios públicos, privados, empresas y ciudadanos. Los servicios públicos deben operar de manera ejemplar y mejorar la protección de los sistemas de información y los datos que se les encomienden.

Para cumplir estos objetivos, la estrategia identificó siete áreas de acción:

- Anticipar y analizar el espacio cibernético para la efectiva toma de decisiones
- Detectar y bloquear ataques, estar alerta y apoyar a las víctimas potenciales
- Mejorar y mantener medios humanos, científicos, técnicos, industriales y las capacidades con el fin de mantener independencia
- Proteger los sistemas de información del Estado y los operadores de infraestructuras críticas para garantizar una mejor capacidad de recuperación nacional
- Adaptar la legislación francesa para incorporar los avances tecnológicos y nuevas prácticas
- Desarrollar iniciativas de colaboración internacional en las áreas de información,
- Sistemas de seguridad, ciberdefensa y lucha contra la delincuencia informática con el fin de proteger los sistemas de información nacionales
- Comunicar, informar y convencer para aumentar la comprensión por parte de la población, de la magnitud de los desafíos relacionados con la seguridad en los sistemas

Doctrina nacional en caso de ciberagresión:

- Protección robusta y resistente de los sistemas de información del Estado y la infraestructura de información crítica; Capacidad gubernamental para responder adecuadamente a agresiones de todas las escalas, a través de medios diplomáticos, legales y policiales.
-

## Estructura de Ciberdefensa

En septiembre de 2021, la estructura de ciberdefensa de Francia se basó en varias instituciones y agencias que trabajan en conjunto para proteger las infraestructuras críticas, sistemas gubernamentales y redes privadas del país contra amenazas cibernéticas. Algunas de las principales entidades involucradas en la ciberdefensa de Francia incluyen:

- Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI): Es la agencia gubernamental encargada de la ciberseguridad y la ciberdefensa en Francia.
- Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN): El Secretariado General de Defensa y Seguridad Nacional es una agencia francesa que coordina las políticas de seguridad y defensa del país. Aunque no está centrado exclusivamente en ciberseguridad, también juega un papel importante en la formulación de políticas y la toma de decisiones estratégicas relacionadas con la ciberdefensa.
- Ministerio de Defensa: El Ministerio de Defensa de Francia también está involucrado en cuestiones de ciberseguridad y ciberdefensa, especialmente cuando se trata de la protección de infraestructuras críticas y la seguridad de las redes militares.
- Empresas y Sectores Privados: Además de las instituciones gubernamentales, las empresas y sectores privados en Francia también están involucrados en la ciberdefensa, protegiendo sus propios sistemas y colaborando con las autoridades gubernamentales en la lucha contra las amenazas cibernéticas.

En el caso de Francia, en el Libro Blanco de la Seguridad y la Defensa de 2008, se puso de relieve como nueva amenaza, el espacio cibernético, centrándose en la seguridad de los "sistemas de información, centros nerviosos reales de nuestra sociedad", donde "todos los sectores de actividades ya sean estatales, industriales, financieras o comerciales, dependen más de la tecnología y redes de comunicaciones electrónicas".

Esa apreciación distingue tres escenarios principales:

- Un ataque contra los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos que pudiesen provocar destrozos similares o superiores a los de un bombardeo físico.
- Un ataque contra la parte visible de Internet, esto es, las webs y las intranets de administraciones clave, como presidencia, policía, impuestos y hospitales con la consiguiente provocación de un caos y desprestigio del Estado ante sus ciudadanos y ante las potencias extranjeras.
- La integración de cualquiera de esos ataques informáticos en el marco de una secuencia clásica de guerra convencional.

Por medio del Centro Operacional de la Seguridad de Sistemas de Información (COSSI), se detectarían y responderían los ataques, se vigilarían las redes más sensibles de la administración y se desarrollarían nuevas capacidades defensivas. La (SGDSN) se basa en dos pilares esenciales y complementarios:

- La preservación de la soberanía de Francia, otorgándose medios de acción e influencia y participación en la seguridad internacional, registrando sus acciones en una legitimidad.
- La Revisión Estratégica de Ciberdefensa establece una doctrina para gestionar las crisis cibernéticas. Esta revisión aclara los objetivos de una estrategia nacional de defensa cibernética y confirma la relevancia del modelo francés y la responsabilidad principal del gobierno en este campo.
-

## Conclusión parcial

Las oportunidades de ataque en el ciberespacio llegaron para quedarse. Las grandes potencias las utilizaron en su competencia geopolítica directa, y otras las siguen para continuar con el nuevo método de intimidación.

La cibercriminalidad, espionaje, propaganda, sabotaje o explotación excesiva de datos personales representan una amenaza para la confianza y la seguridad en el ámbito digital y exigen una respuesta colectiva y coordinada en torno a cinco objetivos estratégicos.

La defensa del ciberespacio se centra en iniciativas defensivas para proteger la infraestructura crítica.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# PARAGUAY

## Generalidades

Paraguay es un país que se encuentra situado en América del Sur, cuenta con una superficie de 406 752 km2 y con una población de 6.854.536 habitantes (Paraguay, 2023). Se ubica en el puesto 103 a nivel global en el índice de desarrollo humano, con 0,728 puntos en 2020, siendo su IDH alto. El PIB (PPA) per cápita de Paraguay es de 15 977 y el PIB (PPA) en millones es 108 338 según los datos del Banco Mundial (Mundial, 2022). De acuerdo con el último texto constitucional, constituye un Estado social de derecho, unitario, indivisible, y descentralizado, adoptando para su gobierno la democracia representativa, participativa y pluralista, fundada en el reconocimiento de la dignidad humana. El Paraguay es un país bilingüe, se habla los idiomas guaraní y español. (Exteriores, 2022)

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

Las Fuerzas Armadas de Paraguay cuentan con 20.000 soldados en Servicio Activo y están compuestas por el Ejército, la Armada y la Fuerza Aérea. Son responsables de la defensa y seguridad del país, así como de la participación en operaciones de ayuda humanitaria y mantenimiento de la paz (Wikipedia, Paises por tamaño de sus Fuerzas Armadas, 2023). Conflictos librados: Guerra de la Triple Alianza (1864-1870, Guerra del Chaco (1932-1935), Operación Cóndor (década de 1970 y 1980. En el siglo XXI Paraguay ha estado principalmente enfocado en mantener la estabilidad interna y participar en operaciones de paz de la ONU (Wikipedia, Fuerzas armadas de Paraguay, 2023).

## Estructura de Ciberseguridad

Paraguay de forma conjunta con el sector privado, la academia y la sociedad civil, ha desarrollado el Plan Nacional de Ciberseguridad, para coordinar las políticas públicas de ciberseguridad e integrar a todos los actores interesados en esta tarea. Los siete ejes estructurales de este Plan Nacional son: Sensibilización y Cultura; Investigación, Desarrollo e Innovación; Protección de Infraestructuras Críticas; Capacidad de Respuesta ante Incidentes Cibernéticos; Capacidad de Investigación y Persecución de la Ciberdelincuencia; Administración Pública y Sistema Nacional de Ciberseguridad. El Sistema Nacional de Ciberseguridad tendrá los siguientes componentes: El Coordinador Nacional de Ciberseguridad y La Comisión Nacional de Ciberseguridad (Báez, 2017).

Los componentes en la estructura de ciberseguridad de Paraguay incluyen: Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs); Ley de Delitos Informáticos; Equipo de Respuesta a Incidentes Informáticos (CSIRT); Colaboración Internacional; Capacitación y Concienciación; Protección de Infraestructuras Críticas (Báez, 2017).


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Estructura de Ciberdefensa

La seguridad cibernética se ha erigido como un pilar fundamental para la preservación de la infraestructura digital y la salvaguardia de los activos nacionales.

La estructura de Ciberdefensa está compuesta por: la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), el Equipo de Respuesta a Incidentes Informáticos (CSIRT), las Fuerzas Armadas y Agencias de Seguridad y la Colaboración Internacional.

Las fuerzas de ciberdefensa podrían constar de: el Equipo de Monitoreo y Detección, el Equipo de Respuesta a Incidentes, la Unidad de Análisis Forense Digital, y el Grupo de Inteligencia Cibernética.

Las acciones cibernéticas pueden incluir medidas preventivas, tales como mejorar la infraestructura de seguridad, así como respuestas a incidentes, como investigaciones de ciberataques, mitigación de amenazas y protección de sistemas críticos.

## Conclusión parcial

La estructura de Ciberseguridad y Ciberdefensa en Paraguay ha experimentado avances significativos en la última década, evidenciando el compromiso del país para proteger su entorno digital. Sin embargo, aún existen desafíos por superar, como la concienciación pública, la asignación de recursos adecuados y la regulación actualizada. Para garantizar un entorno cibernético seguro y resistente, Paraguay debe continuar fortaleciendo su enfoque en la ciberseguridad, colaborando a nivel nacional e internacional y manteniendo un enfoque proactivo en la identificación y mitigación de amenazas en línea. Paraguay debe seguir desarrollando su estructura de ciberdefensa, fortaleciendo su capacidad para prevenir y responder a los ciberataques y garantizando así la seguridad de su infraestructura digital y activos nacionales.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# PERÚ

## Generalidades

Perú tiene una superficie de 1.285.215 km2, siendo el tercer país de mayor extensión en América del Sur, después de Brasil y Argentina. Posee, además, 200 millas marinas y derechos territoriales sobre una superficie de 60 millones de hectáreas en la Antártida.

El territorio peruano presenta tres regiones bien definidas: COSTA, SIERRA y SELVA o AMAZONIA. La Costa es una faja de 40 Km. a 880 Km. de ancho, arenosa y árida, con excepción de algunos valles fértiles. La Sierra está constituida por los Andes que atraviesan el país de Norte a Sur. En esta región se encuentran los principales yacimientos minerales (Perú es uno de los mayores productores mundiales de vanadio, cobre y plata, y extrae apreciables cantidades de zinc, plomo, oro y hierro).

El Índice de Desarrollo Humano, IDH, de Perú en 2019 fue de 0.777, lo que sitúa al país en la categoría de desarrollo humano alto y en el 79º lugar de 189 países y territorios.

El Perú se encuentra organizado políticamente en 24 departamentos, además del Callao, provincia constitucional. Tiene una población de 33.715.471 habitantes. Un 72,3% corresponde a población urbana y un 27,7% a rural. Sobre el idioma, en el Perú el español es el idioma de uso común, pero coexisten una multitud de lenguas nativas. El quechua es una importante herencia del pasado inca y en muchas regiones del país aún se habla con ligeras variantes según la zona. Un 80,3% de la población habla español, un 16,2% Quechua y un 3% habla otros dialectos. La moneda oficial del Perú es el Nuevo Sol (S/.). La tasa de cambio es aproximadamente de 2,65 nuevos soles por cada dólar estadounidense.

El Gobierno del Perú se caracteriza por ser una república democrática, donde el Presidente y los miembros del Congreso son elegidos cada cinco años por votación universal. Su deuda pública en 2022 fue de 76.759 millones de euros, con una deuda del 33,37% del PIB.

Densidad de población: 26.1 hab/Km2. Renta per cápita: 6.977$ (2019) (Datos BM). Coeficiente GINI: 0,45 (2018) Esperanza de vida: 73,83 años para los varones y 79,28 años para las mujeres (2018). Crecimiento de la población: 1.06 % (INEI 2019). IDH: 0,77 (puesto 78 Informe Desarrollo Humano 2020). Tasa de natalidad: 17,42 nacimientos/1.000 habitantes. (Datos BM 2018). Tasa de fertilidad: 2,25 infantes nacidos/mujer (Datos BM 2018).

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

Las Fuerzas Armadas del Perú, se componen del ejército, marina de guerra y fuerza aérea, tienen como finalidad primordial garantizar la independencia, la soberanía y la integridad territorial de la República. La conforman 150.000 efectivos entre Ejército (101.000), Marina de Guerra (34.000) y Fuerza Aérea (15.000).

Los principales conflictos bélicos con sus vecinos han sido: La guerra del Pacífico, conflicto armado ocurrido entre 1879 y 1884, que enfrentó a Chile y a los aliados Bolivia y Perú. Con Ecuador en 1941, Paquisha en 1981 y durante el gobierno de Alberto Fujimori en 1995 (Guerra


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

del Cenepa), que dio como resultado un breve, pero intenso enfrentamiento que finalizó con el Acuerdo de Paz de Itamaraty.

## La Ciberseguridad en el Perú

Antes de adentrarnos en la importancia de la ciberseguridad en Perú, es fundamental comprender qué implica este término. La ciberseguridad se refiere a las prácticas y medidas que se implementan para proteger los sistemas informáticos, las redes y los datos de posibles amenazas cibernéticas. Esto incluye ataques de hackers, malware, robo de identidad y cualquier otro intento de comprometer la seguridad digital.

La ciberseguridad se ha convertido en un tema de suma importancia en el mundo digital actual. Perú, al igual que muchos otros países, enfrenta desafíos en términos de seguridad en línea. En este artículo, explicaremos la importancia de la ciberseguridad en Perú y cómo puede protegerse contra las amenazas cibernéticas. Desde la protección de datos personales hasta la seguridad de las empresas y la infraestructura nacional, la ciberseguridad desempeña un papel fundamental en la sociedad moderna.

## Situación de Ciberataques en el Perú

Perú recibió 15 mil millones de intentos de ciberataques en 2022, según los resultados del último informe semestral del panorama global de amenazas de FortiGuard Labs. Esto es un crecimiento del 35% frente a 2021, según señala la compañía.

La región de América Latina y el Caribe sufrió más de 360 mil millones de intentos de ciberataques en 2022. México recibió la mayor cantidad de intentos de ataques (187 mil millones), seguido de Brasil (103 mil millones), Colombia (20 mil millones) y Perú (15 mil millones).

En base a lo anterior, a continuación, se presentan un breve resumen de los avances de ciberdefensa del Perú:




Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Si bien Perú aún no cuenta con una estrategia nacional de seguridad cibernética, sí ha puesto en marcha una política nacional de ciberseguridad que, entre otras cosas, destaca la necesidad de crear una estrategia nacional de ciberseguridad y un comité nacional de ciberseguridad.

Objetivo Nacional sobre Ciberdefensa:

Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.

Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia.

Políticas Nacionales de Perú sobre Ciberdefensa

Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un Entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.

Para lograr este objetivo es necesario involucrar a todos los sectores y entidades del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo en el que participen representantes del sector privado, sociedad y la academia, donde cada uno aporte y actúe a propósitos comunes, estrategias concertadas y esfuerzos coordinados. Asimismo, es de vital importancia crear conciencia y sensibilizar a la población respecto de la importancia de la seguridad de la información (ciberseguridad); así como, fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública.

Este objetivo permitirá generar y fortalecer las capacidades existentes en materia de seguridad cibernética, con el propósito de afrontar las amenazas que atentan contra los propósitos planteados.

Inicialmente, se capacitará a los funcionarios y servidores que estén directamente involucrados en la atención y manejo de incidentes cibernéticos. Gradualmente se extenderá esta capacitación a las demás entidades del Estado. Entre los planes de capacitación, el Pe-CERT con el apoyo del Comité Interamericano Contra el Terrorismo (CICTE) de la OEA, entre otros, elaborará un Plan de Capacitación para los demás funcionarios y servidores del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general. De la misma forma, el Ministerio del Interior (MININTER) buscará la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa (teórico-prácticas) en las escuelas de formación y de capacitación de oficiales y suboficiales.

## Estructura de Ciberdefensa

El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

Para ello Perú establece que toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa, el cual, dentro del contexto de las operaciones de ciberdefensa, está sujeto a los principios de legalidad, necesidad y oportunidad.

Según la Ley N.º 30.618 de 2017 de Perú, define la seguridad digital como la "situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado". La Ley también define que la "Dirección Nacional de Inteligencia" es responsable por "realizar actividades y establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia".

El Decreto Supremo N.º 106-2017-PCM "aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales", que son "recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales o que están destinados a cumplir dicho fin".

Perú tiene un equipo de respuesta a incidentes en seguridad informática nacional, CSIRT, cuya unidad Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública, PeCERT, tiene como misión coordinar la prevención, el tratamiento y la respuesta a incidentes de seguridad cibernética de instituciones del sector público, así como elaborar estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado.

PeCERT se encuentra bajo la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y es miembro de la red CSIRT Américas. Además, según el Centro de Ciberseguridad Industrial, Perú está desarrollando una ley para la protección de la infraestructura crítica.

El tema del gobierno digital es importante para Perú, por ello se dictó la Ley de Gobierno Digital, la cual "tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno".

Además, se ha declarado de "interés nacional las estrategias, acciones, actividades e iniciativas para el desarrollo del gobierno digital, la innovación y la economía digital en el Perú con enfoque territorial" en 2018, y también se aprobaron los "lineamientos para la formulación del Plan de Gobierno Digital".

## Conclusión parcial

La Política Nacional define el "qué hacer"; por consiguiente, resulta imprescindible contar con una Política Sectorial de Ciberdefensa, cuyos objetivos y lineamientos permitan fortalecer el desarrollo de capacidades para neutralizar las amenazas y ataques en y mediante el ciberespacio, impulsando tanto la cultura y la educación en ciberdefensa en las Fuerzas Armadas, como la Investigación, Desarrollo e Innovación (I+D+i) en ciberdefensa entre las Instituciones Armadas, así como, la cooperación nacional e internacional a fin de contar con una seguridad cooperativa en el entorno digital.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# SURINAM

## Generalidades

La república de Surinam, (capital Paramaribo) fue inicialmente colonizada por los británicos, luego pasó a manos de los holandeses por lo que es conocida como la Guyana holandesa, la misma que obtuvo su independencia el 25 de noviembre de 1975. Limita al norte con el océano Atlántico, al este con la Guayana francesa, al oeste con la Guyana y al sur con Brasil. Su extensión es de 164.000 km

Su población es multicultural y multilingüe, conformado por hindúes, criollos, javaneses, marroquíes, indonesios, chinos. Son de religión variada predomina el catolicismo y protestantes. Su gobierno es democrático con un sistema parlamentario, dispone de cerca de 600.000 habitantes y su PIB va de 4 mil millones de dólares (25/33), su economía se basa en la exportación de Bauxita.

## Datos de las Fuerzas Armadas (descripción, efectivos, conflictos actuales e históricos)

Las FF. AA de Surinam está conformado por el Ejército que además de proteger la soberanía nacional, mantiene la paz interna y apoya en situaciones de emergencia y desastres naturales. La fuerza aérea también cumple misiones de búsqueda y rescate, transporte y misiones humanitarias y la guardia costera, antes fuerza naval, actualmente rinde cuentas al Ministerio del Interior sin embargo permanece bajo control militar, su misión principal es proteger las aguas territoriales. Su equipamiento y modernización fue orientada a equipos de comunicación, sistemas de vigilancia para mejorar su capacidad de respuesta y eficiencia combativa mediante la capacitación continua de sus tropas, las mismas que afianzan esta actividad mediante la cooperación internacional con otros ejércitos y organizaciones internacionales especialmente en las operaciones conjuntas.

El efectivo de las fuerzas militares es de aproximadamente de unos 2500 efectivos, el Ejército dispone de las siguientes unidades:

- Un batallón de infantería ligera
- Un cuerpo de fuerzas especiales
- Una unidad de apoyo
- Un cuerpo de policía militar

En contraste con el ejército, la guardia costera de Surinam ha sufrido un grave deterioro de su capacidad por el abandono prolongado, su material fuera de servicio fue reemplazado por embarcaciones de menor capacidad operativa.

El estado de la Fuerza Aérea es similar al de la Guardia Costera, dispone de cinco aviones, cuatro helicópteros y tres aviones Cessna.

Este país históricamente no se encuentra involucrado en conflictos militares internacionales, pero existe una disputa y tensiones en torno a temas fronterizos por recursos naturales (oro, gas y petróleo) en la región conocida como la región del Tigri, que se encuentra en la frontera con Guyana.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Estructura de ciberseguridad (estrategia nacional de ciber, órganos civiles y militares de ciber, organigrama CTIR)

Surinam aún no ha aprobado una estrategia nacional de ciberseguridad, pero a fines de 2014 el gobierno inició el proceso de desarrollar una en colaboración con la OEA. Además, la "Visión 2020 de las TIC de Surinam" exige la mejora de la ciberseguridad y una mayor conciencia de las amenazas cibernéticas.

Las FAS contribuyen a los esfuerzos nacionales para prevenir a la seguridad cibernética y sus coordinaciones son del más alto nivel con la creación de la Dirección de Seguridad Nacional, si bien no están bien desarrollados, pero toman medidas serias como la implementación de un plan estratégico de ciberseguridad a través de frecuentes compromisos con los departamentos locales para crear conciencia en este tema, de igual manera empezaron a formar ciberanalistas que ayudan a mantener una conciencia en el ámbito cibernético.

En relación con los servicios de ciberseguridad, hay algunas empresas que los brindan, aunque en forma limitada. En cuanto a formación, existen algunas oportunidades para continuar la educación superior en ciberseguridad; el gobierno está comenzando a brindar capacitación sobre el tema, y el país ha recibido apoyo de organizaciones internacionales en capacitación técnica y análisis sobre ciberseguridad.

Recientemente, el país incluyó el delito cibernético en su legislación, y también avanzó en la redacción de un proyecto de ley sobre privacidad y protección de datos, que actualmente está en curso en el Parlamento, mismo que fue aprobado en 2018.

## Estructura de ciberdefensa (organigrama, fuerzas de ciber, mando conjunto, acciones de ciber realizadas)

Surinam también enfrenta desafíos de la ciberseguridad por ello la ciberdefensa es crucial para proteger sus sistemas de información críticos, incluidos aquellos relacionados con el gobierno, infraestructuras esenciales, servicios públicos, financieros y comunicacionales.

La institución encargada de la ciberdefensa en Surinam es la Agencia de Seguridad Cibernética, que también se la conoce como el Centro Nacional de Ciberseguridad de Surinam, esta institución es responsable de coordinar y supervisar la ciberseguridad en el país, así como de responder a incidentes cibernéticos y proteger las infraestructuras críticas.

Los esfuerzos regionales y nacionales sobre ciberdefensa son multifacéticos y se centran en:

• Desarrollo de políticas, que involucren a todas las partes interesadas y se adapten a la situación legal, cultural, económica y estructural del país.

• Creación de capacidades para establecer equipos de respuesta antes los ciberataques y brindar la respectiva asistencia técnica y personalizada. Fortalecer a las instituciones y organizaciones gubernamentales

• Investigación y divulgación mediante herramientas e informes para orientar a los responsables de emitir las políticas estatales, así como la organización privada que hacer conocer las problemáticas actuales y desafíos de ciberseguridad en el país.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Conclusión parcial

Surinam inicia sus actividades de ciberdefensa con apoyo internacional. En Surinam no se encuentra adecuadamente socializado la información sobres las actividades de Ciberdefensa, así como, no se registra ataques de ciberdefensa de importancia a la infraestructura crítica del estado.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# TRINIDAD Y TOBAGO

## Generalidades

Oficialmente la República de Trinidad y Tobago, es un país soberano insular ubicado en el mar Caribe, en la región septentrional de América del Sur, formado por las islas principales, Trinidad y Tobago, y otras numerosas y mucho más pequeñas, está situado a 130 kilómetros al sur de Granada y a 11 kilómetros de la costa del noreste de Venezuela.

Es un país con escasa proyección internacional dado su pequeño tamaño y su economía volcada principalmente en la exportación de petróleo y gas natural, muy dependiente por tanto de la evolución de los precios internacionales.

Población: Tiene una población de aproximadamente 1.3 millones de habitantes (estimación de 2016). El país obtuvo la independencia en 1962 y se convirtió en república en 1976.

Tiene una economía de renta alta con un PIB per cápita 57,7 % más elevado que el promedio regional para América Latina y El Caribe.

Su extensión territorial es de 5128 Km.2, la actividad agrícola más importante es el cultivo de la caña de azúcar, al que se asocia la producción de azúcar en los seis ingenios del oeste de la isla, así como de mieles y de ron. Le siguen en importancia el cacao, el grano y su beneficio, las frutas cítricas y el café.

Idioma: inglés (oficial), inglés criollo de Trinidad, inglés criollo de Tobago, indostaní del Caribe (un dialecto del hindi), francés criollo de Trinidad, español y chino. Religión: católicos (24%), anglicanos (9,1%), hindúes (22.5%), baptistas (7.2%) y musulmanes (11%).

## Datos de Fuerzas Armadas

La Fuerza de Defensa de Trinidad y Tobago (TTDF) es la organización militar responsable de la defensa de la República de Trinidad y Tobago. Está formada por el Regimiento, la Guardia Costera, la Guardia Aérea y las Reservas de la Fuerza de Defensa. Creada en 1962 tras la independencia de Trinidad y Tobago del Reino Unido, la TTDF es una de las mayores fuerzas militares del Caribe anglófono.

Su misión es «defender el bien soberano de la República de Trinidad y Tobago, contribuir al desarrollo de la comunidad nacional y apoyar al Estado en el cumplimiento de sus objetivos nacionales e internacionales». Las Fuerzas de Defensa han participado en incidentes nacionales, como el intento de golpe de Estado de 1990, y en misiones internacionales, como la Misión de las Naciones Unidas en Haití entre 1993 y 1996.

En 2019, Trinidad y Tobago firmó el tratado de la ONU sobre la prohibición de las armas nucleares.

## Estructura de Ciberseguridad

Mancomunidad de Naciones (Commonwealth of Nations) Cooperación Bilateral y Multilateral con Reino Unido, es una organización compuesta por 56 países soberanos independientes y semiindependientes que, con la excepción de Togo, Gabón, Mozambique y Ruanda, comparten lazos históricos con el Reino Unido. En el pasado, Irlanda y Zimbabue también formaron parte de ella.



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Su principal objetivo es la cooperación internacional en el ámbito político y económico, así como también existe el compromiso del Reino Unido de ayudar a los países de la Commonwealth a fortalecer su seguridad cibernética o ciberseguridad contra grupos criminales y actores estatales hostiles, incluida Trinidad y Tobago.

La red mundial interdependiente de infraestructuras digitales de Tecnologías de la Información y la Comunicación (TIC) conocida como "ciberespacio" constituye la fuerza que impulsa el crecimiento de la economía mundial del conocimiento. La realidad de este entorno es que todas las oportunidades que traen consigo las TIC se ven acompañadas, asimismo, por riesgos a la seguridad.

El ciberespacio proporciona el entorno que facilita ataques virtuales organizados contra activos de información y contra la infraestructura física, que incluso pueden llevarse a cabo mediante la utilización de tecnologías de consumo de fácil acceso.

Los delincuentes cibernéticos altamente capacitados pueden ocultar su identidad, su ubicación y sus vías de acceso. Pueden aprovechar el ciberespacio para perturbar comunicaciones y ocultar o demorar una respuesta defensiva, ofensiva o de emergencia. Un ejemplo es el del virus Stuxnet8/, descubierto en 2010, diseñado para atacar sistemas utilizados para controlar y operar instalaciones industriales tales como centrales eléctricas, refinerías petroleras y gasoductos.

La estrategia de Trinidad Tobago se basa en el papel que cumple las TIC en la promoción del desarrollo del país. Sus principales objetivos son los siguientes:

- Crear un entorno digital seguro que permita a todos los usuarios gozar plenamente de los beneficios que ofrece la Internet.
- Proporcionar un marco de gobernanza en relación con todos los asuntos de seguridad cibernética mediante la identificación de las estructuras institucionales y administrativas necesarias, incluidas las de recursos humanos, capacitación y desarrollo de capacidades, y las relativas a las necesidades presupuestarias.
- Proteger los activos físicos, virtuales e intelectuales de los ciudadanos, las instituciones y el Estado a través de la creación de un mecanismo eficaz para responder a las amenazas cibernéticas, sea cual fuere su origen.
- Facilitar la seguridad de todos los ciudadanos promoviendo la sensibilización frente a los riesgos cibernéticos y elaborando medidas de protección eficaces y apropiadas para mitigar riesgos y ataques.
- Ayudar a prevenir ataques cibernéticos contra la infraestructura crítica y redes de información segura generando competencias entre los principales interesados y el público en general.

Con esta estrategia, el Gobierno pretende crear un entorno cibernético seguro y sólido, basado en la mutua colaboración de todos los interesados clave, que permita aprovechar las TIC en beneficio de todos y para la prosperidad de todos. (Cibernética, 2012).

## Estructura de Ciberdefensa

La Agencia de Seguridad Cibernética de Trinidad y Tobago a través del Ministerio de Seguridad Nacional.

- En proceso de establecimiento, según lo dispuesto por la Estrategia Nacional de Seguridad

Cibernética (ver el Proyecto de Ley de la Agencia de Seguridad Cibernética);

- Sería responsable, entre otras cosas, de actuar como punto de contacto nacional para todos los asuntos relacionados con la seguridad cibernética, remitir los asuntos a la policía, preparar, revisar y actualizar periódicamente y, en todo caso, al menos anualmente, una estrategia nacional de seguridad cibernética, brindar asesoramiento sobre asuntos relacionados con la seguridad cibernética, desarrollar y publicar estándares para productos y servicios sobre seguridad cibernética, realizar investigación y desarrollo en el área de seguridad cibernética y coordinar ejercicios de seguridad cibernética.

La Agencias y departamentos dedicados a Unidad de Delitos Cibernéticos y Servicio de Policía de Trinidad y Tobago (TTPS)

- Las tareas incluyen recopilar información con respecto a delitos informáticos y enjuiciar a los delincuentes y empresas que acceden ilegalmente a datos confidenciales y explotan sistemas y redes informáticos que afectan la funcionalidad.

Cooperación de Acuerdos Multilaterales Convención sobre Ciberdelincuencia (Convención de Budapest)

- Aborda los delitos basados en Internet y las redes informáticas, en particular las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las infracciones de la seguridad de la red.
- Contiene una serie de facultades y procedimientos como el registro de redes informáticas y la interceptación.
- Persigue una política penal común encaminada a la protección de la sociedad frente a la ciberdelincuencia, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Ley Modelo sobre Informática y Delitos Relacionados con la Informática.

- Tres secciones: definiciones, delitos y derecho procesal
- Los delitos se relacionan con el acceso ilegal, la interferencia con los datos, la interferencia con un sistema informático, la interceptación ilegal de datos, los dispositivos ilegales y la pornografía infantil utilizando un sistema informático o un medio de almacenamiento de datos informáticos. (UNIDIR, 2019)
- Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por su sigla en inglés): un órgano de servicio encargado de recibir, examinar y responder a informes y actividades en materia de incidentes de seguridad informática.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# URUGUAY

## Generalidades

*Uruguay*, cuyo nombre oficial es república Oriental del Uruguay, se encuentra en América del Sur, su capital y ciudad más poblada es Montevideo. Limita al norte y noreste con la República Federativa del Brasil, al sur y sureste con el Río de la Plata, al oeste, el Río Uruguay, lo separa de la República Argentina., su extensión territorial abarca 176.220 km2, siendo el segundo país más pequeño de Sudamérica, después de Surinam.

La República Oriental del Uruguay es una República Democrática con dos Cámaras Legislativas, el Senado y la Cámara de Representantes (Diputados). Su idioma oficial es el español, su moneda es el peso uruguayo.

Tiene una población de 3.426.260 personas, se encuentra en la posición 134, mantiene una baja densidad de población, 19 habitantes por km2. (Expansión / Datos macro. com, 2023).

El PIB anual del Uruguay en el año 2022 se encontraba en 67.583 euros y el PIB per capital del Uruguay al año 2022, fue de 19.725 euros, por lo que se encuentra en el puesto 50 de los 196 países del ranking de PIB per-capital.

En cuanto al índice de Desarrollo Humano o IDH, según el instituto vasco de estadísticas los uruguayos cuentan con un 0.809 para medir el progreso de un país y que nos muestra el nivel de vida de sus habitantes, y se encuentran en el puesto 59. (estadisticas, 2022)

Su gobierno se divide en tres poderes independientes: Poder Ejecutivo ejercido por el presidente de la república, Poder Legislativo ejercido por la Asamblea General y Poder Judicial encabezado por la Suprema Corte de Justicia. Además, existen de tres organismos públicos autónomos de control: la Corte Electoral, el tribunal de lo Contencioso administrativo y el Tribunal de cuentas de la Republica.

El país es miembro integral del Foro Iberoamericano de Ciberdefensa, promoviendo la cooperación internacional con otros 10 países de América, además de Portugal y España.

## Datos de Fuerzas Armadas

Uruguay cuenta con unas *Fuerzas Armadas* que están compuestas por un Ejército el cual cuenta aproximadamente de unos 15.190 efectivos organizados en cuatro divisiones y su Reserva General, una Armada que cuenta con unos 4.600 efectivos y está organizada en cuatro mandos: el Comando de la Flota (COMFLO), la Prefectura Nacional Naval (PRENA), la Dirección General de Material Naval (DIMAT) y la Dirección General de Personal Naval (DIPER y una Fuerza Aérea la cual cuenta de unos 2.600 efectivos y está organizada en tres Brigadas Aéreas (I, II y III) y 7 Escuadrones. (HEMISFERICA, 2023)

Estas tres ramas están constitucionalmente subordinadas al presidente constitucional de Uruguay a través del Ministerio de Defensa Nacional. Su principal misión es cumplir los requerimientos de la Defensa Nacional, a fin de salvaguardar la soberanía, la independencia e integridad territorial del país, así como cuidar los recursos estratégicos y contribuir al mantenimiento de la paz interna.

Las principales guerras donde ha participado Uruguay encontramos a la guerra Grande 1836-1851, La Guerra del Paraná 1845-1850, Guerra Platina 1851-1852 y la guerra de la Triple Alianza (Guerra del Paraguay) 1856-1870. (Uruguay).



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

Uruguay no cuenta con una estrategia nacional de *ciberseguridad*, sin embargo, cuenta con un marco de ciberseguridad organizado con estándares internacionales que implementa regulaciones nacionales para mejorar la seguridad cibernética y protección de la infraestructura critica, el marco seleccionado es FRAMEWORK[13] de NITS (National Institute of Standards and Technology de los EE. UU.), el marco exige 68 requisitos de seguridad que fueron adaptados a la realidad de Uruguay. Se dispone de la agenda política digital, la cual procura desarrollar habilidades digitales, utilizar la innovación, realizar inversión estratégica en infraestructura, crear economía digital e innovación para la competitividad, gestionar con inteligencia las emergencias, fortalecer el gobierno integrado e inteligente, ofrecer confianza y seguridad en el uso de las tecnologías digitales, producir de estadísticas nacionales relacionadas con las TIC.

Esta agenda, estructuras líneas de acción con una sociedad digital inclusiva, impulso a la competitividad e innovación en sectores estratégicos, transparencia, eficiencia y rectoría del sector público, potenciar la infraestructura de telecomunicaciones, la conectividad y la ciberseguridad a nivel nacional, un marco normativo habilitante de la política digital nacional. El Plan de Gobierno Digital 2025 busca alcanzar la transformación digital de los procesos y servicios, fortalecimiento de la sociedad de la información, innovación, tecnologías emergentes y ciberseguridad. (ONU, 2022)

## Estructura de Ciberseguridad

La estructura de ciberseguridad a nivel nacional tiene como máximo organismo dependiente de Presidencia de la República, a la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) que tiene como misión, mejorar los servicios al ciudadano, utilizando las posibilidades que brindan las TIC. La Agesic promueve políticas de ciberseguridad orientadas a fortalecer la capacitación, generación de cultura de seguridad, generar capacidades, generar y actualizar la normativa. Adicional se encuentra conformado el Sistema de monitoreo que la Agesic articula con todos los organismos involucrados.

El Centro Nacional de Respuesta a Incidentes de Seguridad Informática y Cibernéticos (CERTuy), controla el cumplimiento de la normativa, regula la protección de activos de información críticos del estado, difunde las mejores prácticas en temas de seguridad de la información y protección de información crítica, proporciona apoyo implementación buenas prácticas, desarrolla, administrar la identificación y certificación electrónica. El CERTuy cuenta con un Centro de Operaciones de Seguridad (SOC) que funciona todos los días las 24 horas desde el 2016. CERTuy también es miembro de la red CSIRT Américas, por lo que puede aprovechar la naturaleza colaborativa de la red.

Según el reporte sobre Ciberseguridad 2020 realizado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), Uruguay se encuentra liderando la región en cuatro de las cinco dimensiones del modelo de madurez en ciberseguridad: Política y Estrategia de Seguridad Cibernética; Cultura Cibernética y Sociedad; Formación, Capacitación y Habilidades de Seguridad Cibernética; Marcos Legales y Regulatorios; y Estándares, Organizaciones y Tecnologías. Además, Uruguay es el segundo país de América Latina y octavo en el mundo en seguridad informática, según el índice de seguridad global UIT. (Unión Internacional de Telecomunicaciones, 2020)

[13] FRAMEWORKS: Un framework es un entorno o marco de trabajo, un conjunto de prácticas, conceptos y criterios a seguir estandarizados. (BELLO, 2021)



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

## Estructura de Ciberdefensa

La Política Militar de Defensa puso en ejecución el proyecto de creación del Comando Conjunto de *Ciberdefensa (COMCIBERuy),* dependiente del Estado Mayor de la Defensa y conformado por tres departamentos, es responsable de la dirección, gestión, control y monitoreo de todas las acciones relativas al ciberespacio en la Defensa Nacional. En la figura siguiente se muestra la estructura del COMCIBERuy.

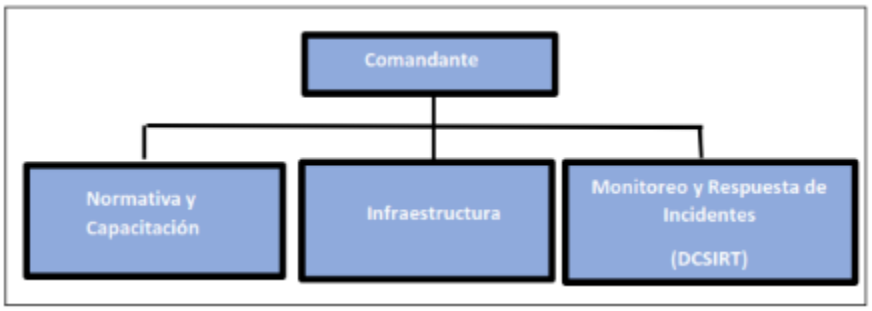



Figura 1. Estructura del COMCIBERuy.
Fuente: Proyecto de creación del COMCIBERuy

Uruguay no define y determina aún la infraestructura nacional crítica, la responsabilidad sobre su protección recae en el D-CSIRT, el CSIRT perteneciente al Ministerio de Defensa según el Decreto Nº 36/015 que lo creó.

Actualmente, Uruguay no cuenta con una legislación específica que aborde los delitos informáticos o delitos digitales de manera integral. Hay algunos proyectos de ley sobre delito cibernético, el país cuenta con legislación sobre la protección de datos personales y privacidad, cifrada en la Ley Nº 18.331, que se aplica a las bases de datos de los sectores público y privado. (Profesionales Uruguay, 2023)

El estado Uruguayo asigna el presupuesto para el fortalecimiento de la seguridad de la información, tiene algunos proveedores de servicios de seguridad cibernética, el gobierno ofrece cursos de seguridad y defensa cibernéticas, que están disponibles para participantes del sector público y privado. Actualmente Uruguay tiene un portal gubernamental, Uruguay. gub.uy, que brinda una serie de servicios web, para el uso de firmas electrónicas y para obtener información relevante. (BID, 2020)

## Conclusión parcial

Se puede *concluir* que Uruguay ha elaborado la normativa de ciberseguridad mediante decretos y agendas a fin de construir una estructura, disponer de legislación básica y unas capacidades que se encuentran en constante desarrollo mediante la Agesic, se resalta la creación del COMCIBERuy con competencia en el área de ciberdefensa. Uruguay se encuentra liderando la región en cuatro de las cinco dimensiones del modelo de madurez en ciberseguridad. Además, Uruguay es el segundo país de América Latina y octavo en el mundo en seguridad informática, según el índice de seguridad global UIT.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# VENEZUELA

## Generalidades

Oficialmente llamada República Bolivariana de Venezuela, es un país soberano constituido por un área continental y por un gran número de islas en el mar Caribe. Su capital es Caracas y tiene una superficie de 916 445 km².

Venezuela posee límites al Norte con el mar del Caribe y con el Océano Atlántico, al Oeste con Colombia, al Sur con Brasil y al Este con Guyana, país con quien mantiene una controversia territorial. Su población estimada (censo de 2023) es de 30.518.260 habitantes, lo que le confiere una densidad poblacional de 35,7 hab./km². Su moneda oficial "El Bolívar" y actualmente corresponde a 0,033 unidades de dólar estadounidense.

El idioma hablado en Venezuela es el castellano, sin embargo, los idiomas indígenas también son de uso oficial para los pueblos indígenas y deben ser respetados en todo el territorio de la república. El PIB es estimado en 96.628 millones de dólares, producto de las exportaciones de petróleo.

## Datos de Fuerzas Armadas

Es la institución armada al servicio de la defensa de Venezuela y se constituye por cinco componentes: Ejército Bolivariano (EB), Armada Bolivariana (AB), Aviación Militar Bolivariana (AMB), Guardia Nacional Bolivariana (GNB) y la Milicia Bolivariana (MB).

El numérico de personal militar es de: 123000 (Activos: 115000 / Reserva: 8000)(Gobierno de la República Bolivariana de Venezuela , 2008)

## Estructura de Ciberseguridad

La República Bolivariana de Venezuela no ha permanecido inmune a los ataques que utilizan el ciberespacio para atentar contra los más variados aspectos de seguridad, comprometiendo así el funcionamiento de la Industria Petrolera en el año 2009, los servicios de pago electrónico en el año 2014, la conectividad prestada por la empresa de telecomunicaciones de propiedad del estado "Movilnet" en el año 2016, intrusiones en las redes sociales y páginas web de instituciones públicas durante los años 2016 - 2018, ataques de ciberterrorismo entre los años 2019 - 2020 mediante drones y el sabotaje al Sistema Eléctrico Nacional en repetidas ocasiones, a partir de estos ataques naciones aliadas como Rusia y China han llamado la atención de cómo preparar a los organismos responsables de la estrategia Nacional de Ciberseguridad con el de que puedan prever, responder y en última instancia lograr adaptación y control al momento de ocurrir un evento de esta naturaleza.

Ahora para hacer frente a los desafíos relacionados con la ciberseguridad la República Bolivariana de Venezuela apunta en la dirección de generar una contextualización sobre las nueve Organizaciones del Estado dedicadas al tema de la ciberseguridad como son: Superintendencia de Servicios de Certificación Electrónica (SUCERTE), Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT), Centro Nacional de Informática Forense (CENIF), Centro Nacional de Tecnologías de Información (CNTI), Comisión Nacional de Tecnologías de Información



Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

(CONATI), Comisión Nacional de Telecomunicaciones (CONATEL), Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL), Consejo Superior de Ciberdefensa, Dirección Conjunta de Ciberdefensa de la Fuerza Armada Nacional Bolivariana (DICOFANB).

Es así que reconociendo las amenazas a la seguridad de la Nación antes citadas, resulta imprescindible estructurar un modelo de organización del Comando Cibernético Nacional, con el fin de que asuma la rectoría a nivel nacional en materia de Ciberseguridad, de manera tal de minimizar las vulnerabilidades que hoy emergen de la explotación del Ciberespacio desde tres grandes dominios: Primeramente el propósito, el cual refleja la intención en materia de ciberseguridad por parte del Presidente Nicolás Maduro Moros, que marca la ruta para que desde la Asamblea Nacional Constituyente se efectúe el debate del anteproyecto de Ley Constitucional del Ciberespacio para de cierta forma combatir la guerra cibernética a la que el país en su conjunto y con ella su infraestructura critica ha estado sometido, a continuación las capacidades que enfatizan las tecnologías presentes y requeridas por el Comando Cibernético Nacional que determinan los modos de funcionamiento y criterios para la elección de cursos de acción y finalmente el dominio de las relaciones en referencia al dominio de las coordinaciones las cuales se enmarcan en la participación e interconexión de todos los actores internos y externos quienes coadyuvan u obstaculizan la implementación exitosa del Comando Cibernético Nacional.

Al relacionar estos dominios con la estructura organizativa del Comando Cibernético Nacional, resulta posible alcanzar la propuesta y aspiraciones plasmadas en el Plan de la Patria 2019 - 2025 (Diaz, 2020)

En cuanto al resultado del Índice Mundial de Ciberseguridad2020 (ICG) publicado por la Unión Internacional de Telecomunicaciones (UIT)para medir el grado de compromiso de sus 193 Estados miembros con el fin de ayudarles a determinar los aspectos susceptibles de mejora e instar a tomar medidas, vemos que Venezuela luego de alcanzar una puntuación global se ubica en el lugar 19 de la clasificación regional, lo que muestra la voluntad de la República Bolivariana de Venezuela para la adopción de buenas prácticas para gestionar la ciberseguridad a escala nacional e internacional (Unión Internacional de Telecomunicaciones, 2021)

## Estructura de Ciberdefensa

La eventual intromisión en los sistemas de comando y control, de las Fuerzas Armadas Nacionales, así como a las bases de datos de los servicios de inteligencia, permiten suponer una amenaza directa a la seguridad de la nación.

Razón por la cual mediante resolución del Ministerio del Poder para la Defensa, fue creada y activada con la misión de ser el órgano rector en materia de ciberseguridad y ciberdefensa la Dirección Conjunta de Seguridad Informática (DICOCEI) de la Fuerza Armada Nacional adscrita al Comando Estratégico Operacional, la cual estará organizada por: Una Dirección, una División de Ciberseguridad, una División de Ciber defensa y una División de Sistemas y Tecnologías de la Información (Nacho Pandavenes, 2023).

## Conclusión Parcial

La conclusión a la que se ha llegado es que la infraestructura digital de la República Bolivariana de Venezuela debe ser considerada como un activo estratégico nacional ya que la intromisión en la infraestructura critica podría causar un fallo catastrófico y más aún cuando la

identidad del atacante puede ser un misterio, ratificando de esta forma la idea de que para el Comando Cibernético Nacional, debe contar con un mandato claro que le permita conducir las operaciones de amplio espectro para defender el ciberespacio.

El Índice Mundial de Ciberseguridad 2020 (ICG) publicado por la Unión Internacional de Telecomunicaciones (UIT) ubica a la República Bolivariana de Venezuela en el lugar 116 de 182 países, lo que evidencia una insuficiente voluntad del país en la adopción de buenas prácticas para gestionar la ciberseguridad a escala nacional e internacional.

En cuanto a la normativa jurídica que rige la ciberseguridad existe la sugerencia de que el país en referencia a sus principios comunes elabore un marco jurídico sobre el uso del espacio cibernético, ya que las ideas sobre derecho internacional en este nuevo espectro fueron elaboradas por los Estados europeos o por especialistas del Norte Global.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# CONCLUSIÓN FINAL

Después de la recopilación y presentación de los datos, se observa que las estructuras del sector cibernético en los veintiséis países analizados son bien distintas, variando desde Brasil que ocupa la posición 18 en el Índice Mundial de Ciberseguridad (*IGC*/2020), hasta Haití que ocupa la posición 167 entre los 182 países que compuseron el estudio de la Unión Internacional de Telecomunicaciones - organismo de las Naciones Unidas en las TIC.

En realidad, el aporte presupuestario destinado al sector ha permitido el incremento de las capacidades destinadas a la Ciberseguridad y la Ciberdefensa, contribuyendo bastante para que avances importantes fuesen dados en dirección a la mejoría continuada y consolidación de los sectores en los países.

Cabe decir que fue, en grande parte de los países estudiados, a partir de la estructura de Ciberdefensa que pasos consistentes hacia la implantación de la estructura de Ciberseguridad fueron realizados, caracterizando claramente un proceso ***bottom up*** que ha se mostrando bien eficiente, ya que ha colaborado de modo efectivo en la formación de una conciencia de Ciberseguridad a nivel nacional, la cual tiene como objetivo proteger el ciberespacio de sectores estratégicos e Infraestructuras Críticas.

Seguramente, a partir de la publicación de una **Estrategia Nacional de Ciberseguridad** se permite una mayor participación política en los asuntos relacionados al sector, abriendo espacio para aspectos sustanciales hacia el fortalecimiento del sector cibernético de los países, puesto que el asunto pasará a ser tratado del más alto nivel (político).

Algunos aspectos que los países podrían tener en común en términos de ciberseguridad incluyen:

1. **Amenazas Comunes:** Los ciberataques, la desinformación, el robo de datos y otros tipos de ciberamenazas son problemas que afectan a todos los países en diferentes grados.
2. **Legislación y Normativas:** Los países pueden estar trabajando en el desarrollo de leyes y regulaciones de ciberseguridad para proteger a sus ciudadanos, instituciones y activos.
3. **Necesidad de Concientización:** En todos estos países, puede haber esfuerzos para educar y aumentar la conciencia pública sobre la importancia de la ciberseguridad y cómo protegerse en línea.
4. **Colaboración Internacional:** La colaboración y el intercambio de información sobre amenazas cibernéticas pueden ser áreas en las que estos países buscan cooperar con otros países y organizaciones internacionales.
5. **Protección de Infraestructuras Críticas:** Los países pueden estar trabajando en la identificación y protección de sus infraestructuras críticas frente a posibles ataques cibernéticos.
6. **Capacidad de Respuesta a Incidentes:** Establecer capacidades de respuesta a incidentes puede ser importante para mitigar y recuperarse de ciberataques.
7. **Educación en Ciberseguridad:** Promover la educación en ciberseguridad en las escuelas y en la sociedad en general puede ser una preocupación compartida.

Finalmente es fundamental e importante recordar que la ciberseguridad es un campo en constante evolución y que en estos países debe ser considerada ya que están ubicados en un lugar estratégico para países del primer mundo.


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu

# REFERENCIAS BIBLIOGRAFICAS

Debido a la gran cantidad de Referencias Bibliográficas, todas las fuentes han sido enumeradas y están disponibles para su consulta en el siguiente enlace, así como la lista nominal de todos los oficiales que participaron en el estudio e investigación de campo durante el Curso Conjunto de Comando y Estado Mayor Conjunto. Academia de Defensa Militar (ADEMIC):

Enlace: Referências Bibliográficas

Enlace: https://iadc-my.sharepoint.com/:f:/g/personal/alexander_ferreira_iadc_edu/ErptCvdZ43BKotcljXEppooBjXCpo8bIKeiOiY_eaASvLg?e=GOxmbn


Coronel ALEXANDER Eduardo Vicente Ferreira (Brasil) – Profesor de Ciberseguridad del Colegio Interamericano de Defensa
Curso de Comando y Estado Mayor Conjunto – ADEMIC – Ecuador
Atualizado en AGOSTO de 2023 E-mail: alexander.ferreira@iadc.edu