UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

CARRERA DE RELACIONES INTERNACIONALES

TALLER DE GRADUACIÓN:
ANÁLISIS DE LA INFLUENCIA DE LA CIBERDIPLOMACIA EN LA RESPUESTA DEL ESTADO COSTARRICENSE A LOS CIBERATAQUES CONTRA LA CAJA COSTARRICENSE DEL SEGURO SOCIAL DURANTE EL PERIODO 2018-2023.

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO ACADÉMICO DE LICENCIATURA EN RELACIONES INTERNACIONALES CON ÉNFASIS EN DIPLOMACIA.

ESTUDIANTE:
DANIELA YAZMÍN VARGAS HERRERA

TUTOR DE LA INVESTIGACIÓN:
LIC. DIEGO ARMANDO MONTOYA VARGAS

SEDE ARANJUEZ, MARZO, 2025

DEDICATORIA

Dedico esta investigación a mi familia, por ser mi mayor fuente de amor, apoyo y motivación en cada etapa de mi vida. A mis padres, Jazmín Herrera Rodríguez y Marco Vargas Montiel, por enseñarme con el ejemplo el valor de la constancia, la honestidad y la responsabilidad. Gracias por creer en mí incluso en los momentos en que yo misma lo dudaba.

También dedico este trabajo a todas las mujeres que, como yo, han buscado abrirse paso en el mundo académico enfrentando desafíos personales, sociales y profesionales. Que este logro sea un recordatorio de que, con esfuerzo, sensibilidad y compromiso, sí es posible avanzar y construir caminos propios.

AGRADECIMIENTO

Agradezco profundamente a todas las personas que hicieron posible este proceso.

En primer lugar, extiendo mi gratitud al licenciado Diego Armando Montoya Vargas, tutor de este trabajo, por su orientación, apoyo constante y confianza en el valor académico de esta investigación. Su acompañamiento fue clave durante los momentos más desafiantes de este proceso, y sus observaciones me permitieron crecer tanto en el ámbito académico como personal.

Agradezco especialmente a las personas entrevistadas: Yuliana Leitón, Jazmín Esquivel y Paula Brenes, quienes con generosidad compartieron su experiencia y conocimiento. Sus aportes fueron fundamentales para enriquecer el análisis de esta tesis y para comprender con mayor profundidad los retos de la ciberdiplomacia en el contexto costarricense.

A mis profesoras y profesores de la carrera de Relaciones Internacionales, por haber sembrado en mí una vocación crítica, comprometida y sensible ante los desafíos globales. Sus enseñanzas trascendieron el aula y han dejado una huella en mi forma de pensar y actuar.

A mis compañeras de carrera, por ser una red de apoyo invaluable, por compartir conmigo esta etapa, y por todas las conversaciones que, de una u otra forma, también aportaron a esta investigación.

Y finalmente, a mí misma: gracias por no rendirte, por tener el coraje de volver a empezar cuando fue necesario, y por confiar en tu capacidad de sostener con firmeza una voz que en algún momento dudó. Esta tesis también es una prueba de crecimiento personal.

RESUMEN EJECUTIVO

La presente investigación analiza la influencia de la ciberdiplomacia en la capacidad del Estado costarricense para responder a los ciberataques dirigidos a la Caja Costarricense del Seguro Social (CCSS) durante el periodo 2018-2023. A través de un enfoque cualitativo, se identificaron las principales estrategias diplomáticas utilizadas, los actores internacionales involucrados y la efectividad de la cooperación internacional frente a incidentes cibernéticos.

El estudio se fundamentó en entrevistas a profesionales del ámbito diplomático y de ciberseguridad, así como en informes técnicos y auditorías institucionales de la CCSS. Los resultados revelan que, aunque Costa Rica ha contado con asistencia de actores clave como la OEA, el FBI y empresas privadas como Microsoft, la respuesta del Estado ha sido predominantemente reactiva y marcada por una limitada coordinación institucional.

Se concluye que la ciberdiplomacia ha sido una herramienta crucial en la gestión de crisis, pero su potencial se ve restringido por la falta de planificación estratégica, la carencia de marcos normativos claros y la ausencia de una estructura formal en la Cancillería dedicada a la ciberseguridad. En este sentido, se recomienda fortalecer las capacidades diplomáticas del país, institucionalizar protocolos de cooperación internacional y avanzar hacia una gobernanza digital más integrada.

Palabras clave: Ciberdiplomacia, ciberseguridad, cooperación internacional, infraestructura crítica, Caja Costarricense del Seguro Social.

ABSTRACT

This research analyzes the influence of cyber diplomacy on the Costa Rican State's ability to respond to cyberattacks against the Costa Rican Social Security Fund (CCSS) during the period 2018–2023. Using a qualitative approach, the study identifies the main diplomatic strategies adopted, the international actors involved, and the effectiveness of international cooperation in the face of cybersecurity incidents.

The analysis is based on interviews with professionals in diplomacy and cybersecurity, as well as technical reports and institutional audits from the CCSS. Findings reveal that while Costa Rica received assistance from key actors such as the OAS, FBI, and private companies like Microsoft, the State's response has been mostly reactive and characterized by limited institutional coordination.

The study concludes that cyber diplomacy has played a critical role in crisis management; however, its potential has been hindered by the absence of strategic planning, the lack of clear regulatory frameworks, and the absence of a formal cybersecurity structure within the Ministry of Foreign Affairs. Strengthening diplomatic capabilities, institutionalizing international cooperation protocols, and moving toward a more integrated digital governance model are among the key recommendations.

Keywords: Cyber diplomacy, cybersecurity, international cooperation, critical infrastructure, Costa Rican Social Security Fund.

TABLA DE CONTENIDO

CAPÍTULO I: INTRODUCCIÓN

El acelerado desarrollo de la tecnología ha traído consigo enormes beneficios, pero también ha expuesto a las naciones a nuevas formas de amenazas, particularmente en el ciberespacio. Los ciberataques, que en sus inicios se consideraban problemas aislados o limitados a grandes potencias y empresas tecnológicas, se han convertido en una amenaza constante para los Estados y sus instituciones. En este escenario, Costa Rica ha experimentado una creciente preocupación por la seguridad cibernética, especialmente a partir de los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) entre 2018 y 2023. Estos incidentes no solo afectaron la operatividad de la institución, sino que también generaron una disrupción significativa en los servicios de salud pública, poniendo en riesgo la atención médica de millones de ciudadanos.

Uno de los ciberataques más críticos ocurrió en 2022, cuando un grupo de hackers logró penetrar los sistemas informáticos de la Caja Costarricense de Seguro Social (CCSS), paralizando parte de sus operaciones. Este ataque destacó la vulnerabilidad de una de las instituciones más importantes del país y puso en evidencia la necesidad de que Costa Rica fortaleciera sus capacidades en ciberseguridad y su capacidad de respuesta diplomática frente a incidentes que afectan no solo a nivel interno, sino también en la arena internacional. Este acontecimiento fue uno de los puntos de inflexión que despertaron el interés de la presente investigación, al observarse una carencia de mecanismos diplomáticos claros y efectivos para responder y mitigar los impactos de estas agresiones cibernéticas.

Históricamente, Costa Rica ha sido un país que ha priorizado la diplomacia en la resolución de conflictos internacionales. Como parte de su estrategia de inserción en el Sistema Internacional, el país ha adoptado un enfoque multilateral y pacífico en la resolución de disputas. Sin embargo, en el ámbito de la ciberseguridad, la ciberdiplomacia es un campo emergente que requiere de un desarrollo más robusto. Desde 2018, Costa Rica ha venido participando en foros internacionales y regionales, como la Organización de los Estados Americanos (OEA) y las Naciones Unidas, para fortalecer sus capacidades cibernéticas, pero la escalada de los ciberataques, especialmente aquellos dirigidos a la Caja Costarricense de Seguro Social (CCSS), han subrayado la necesidad de una respuesta más integral y colaborativa.

La ciberdiplomacia es una herramienta fundamental para manejar estos desafíos. Involucra el uso de medios diplomáticos para gestionar, prevenir y responder a incidentes cibernéticos que pueden tener implicaciones internacionales (Nye, 2017). Además, permite establecer canales de cooperación entre Estados, organizaciones internacionales, el sector privado y otros actores no estatales, en un esfuerzo conjunto por mantener la estabilidad y seguridad del ciberespacio (Tikk, 2018). En el caso de Costa Rica, los esfuerzos en materia de ciberdiplomacia aún se encuentran en una fase inicial; sin embargo, se han iniciado alianzas estratégicas con socios internacionales, organismos multilaterales y empresas de ciberseguridad, lo que refleja un compromiso por avanzar en este ámbito (MICITT, 2022).

Entre los actores clave en la investigación de la influencia de la ciberdiplomacia en la respuesta costarricense a los ciberataques contra la Caja Costarricense de Seguro Social (CCSS), se encuentran tanto entidades nacionales como internacionales. En el plano nacional, instituciones como el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) juegan un papel protagónico en la formulación de políticas públicas de ciberseguridad, mientras que la Caja Costarricense de Seguro Social (CCSS), al ser una de las principales víctimas de los ataques, ha tenido que adaptar sus sistemas y protocolos para enfrentar futuras amenazas. A nivel internacional, organizaciones como la OEA y la Unión Internacional de Telecomunicaciones (UIT) han sido fundamentales para brindar asistencia técnica y fortalecer las capacidades diplomáticas del país en este campo. No obstante, a pesar de la cooperación internacional, la respuesta del Estado costarricense frente a los ciberataques aún carece de una estructura coordinada que combine eficazmente los aspectos técnicos y diplomáticos.

El estado actual del problema refleja una creciente amenaza en el ciberespacio, donde los ciberataques contra instituciones gubernamentales, como la Caja Costarricense de Seguro Social (CCSS), no son eventos aislados, sino que forman parte de una tendencia global que afecta tanto a países desarrollados como en desarrollo. En este contexto, la presente investigación analizará cómo la ciberdiplomacia puede influir en la capacidad de respuesta del Estado costarricense frente a los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) durante el periodo 2018-2023. Se llevará a cabo un análisis de los mecanismos diplomáticos adoptados por

el país, evaluando su efectividad y proponiendo mejoras para enfrentar futuros desafíos cibernéticos. El enfoque metodológico incluirá el análisis de documentos oficiales, entrevistas con expertos en seguridad cibernética y diplomacia, así como estudios de caso de los ciberataques más relevantes ocurridos en dicho periodo.

El objetivo central de esta investigación es evaluar cómo la ciberdiplomacia ha influido en la respuesta del Estado costarricense ante los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS), identificando las fortalezas y debilidades de las estrategias adoptadas. Específicamente, se busca analizar las medidas diplomáticas implementadas para mitigar los efectos de los ataques, la cooperación internacional establecida en este ámbito y la capacidad del país para prevenir futuros incidentes. A su vez, se pretende proponer un conjunto de recomendaciones que puedan mejorar la respuesta nacional ante este tipo de amenazas, considerando tanto el aspecto técnico como diplomático.

Los resultados de esta investigación son de gran relevancia para Costa Rica, ya que no solo permitirán evaluar la preparación actual del país ante los ciberataques, sino que también contribuirán a la creación de políticas públicas más efectivas en ciberseguridad. Asimismo, los hallazgos ofrecerán una visión integral sobre la importancia de la ciberdiplomacia como una herramienta esencial para la protección de infraestructuras críticas, como es el caso de la Caja Costarricense de Seguro Social (CCSS), y para la promoción de un ciberespacio más seguro. En un mundo cada vez más interconectado, la capacidad de respuesta frente a las amenazas cibernéticas no solo es una cuestión de seguridad nacional, sino también de estabilidad internacional, donde la diplomacia juega un papel esencial en la prevención de conflictos y la cooperación global.

1.1 Planteamiento del problema

En la era digital, los ciberataques han emergido como una de las mayores amenazas a la seguridad y estabilidad de los Estados, afectando tanto a infraestructuras críticas como a ciudadanos. Según Nye (2017), la naturaleza transnacional del ciberespacio ha obligado a los Estados a adaptarse, desarrollando no solo capacidades técnicas sino también diplomáticas para gestionar estas amenazas. En este contexto, la ciberdiplomacia —entendida como el uso de

herramientas diplomáticas para mitigar amenazas cibernéticas— permite a los Estados abordar incidentes que trascienden fronteras y que involucran tanto a actores estatales como no estatales (Nye, 2017). Sin embargo, como señala Tikk (2018), la efectividad de estas iniciativas sigue siendo un desafío en desarrollo, especialmente para países que aún consolidan sus estrategias de ciberseguridad, como Costa Rica. Esta dualidad refleja la necesidad de una diplomacia proactiva y colaborativa para enfrentar amenazas cibernéticas de manera más eficaz.

El fenómeno de estudio en esta investigación gira en torno a la relación entre la ciberdiplomacia y la capacidad del Estado costarricense para responder de manera efectiva a los ciberataques que afectaron a la Caja Costarricense de Seguro Social (CCSS) entre 2018 y 2023.

Este periodo es especialmente relevante debido a que incluye algunos de los ciberataques más críticos y dañinos que ha sufrido el país, impactando de manera directa los servicios de salud, los cuales son esenciales para millones de ciudadanos. Costa Rica, a pesar de ser un país con una larga tradición de paz y resolución diplomática de conflictos, ha enfrentado grandes retos al intentar integrar la diplomacia en el ámbito cibernético, ya que este es un campo relativamente nuevo y complejo. A través de esta investigación, se busca comprender cómo el país ha manejado este desafío, qué estrategias diplomáticas se han implementado y cuál ha sido su efectividad en la protección de sus infraestructuras críticas, como la Caja Costarricense de Seguro Social (CCSS).

El contexto de los ciberataques en Costa Rica se ha intensificado durante los últimos años. Los ataques a la Caja Costarricense de Seguro Social (CCSS), que comprometieron información sensible y causaron disrupciones en los servicios de salud, han despertado la atención tanto de la sociedad como de las instituciones gubernamentales. Estos incidentes han evidenciado la vulnerabilidad de las infraestructuras críticas frente a las amenazas cibernéticas y han subrayado la importancia de contar con respuestas robustas y coordinadas a nivel nacional e internacional. La Caja Costarricense de Seguro Social (CCSS), como una de las principales instituciones de servicio público, se vio gravemente afectada por estos ataques, lo que generó un debate sobre la preparación del Estado para hacer frente a este tipo de situaciones y la necesidad de implementar medidas más eficaces no solo en el ámbito técnico, sino también en el diplomático.

En este sentido, la ciberdiplomacia ha surgido como una herramienta clave en la gestión de incidentes cibernéticos, ya que permite establecer relaciones de cooperación entre países y organizaciones internacionales, compartir información sobre amenazas y coordinar respuestas conjuntas. Para Costa Rica, la ciberdiplomacia ha representado una oportunidad para fortalecer su capacidad de respuesta ante ciberataques a través de la colaboración con entidades como la Organización de los Estados Americanos (OEA) y otros actores internacionales. Sin embargo, la ciberdiplomacia en Costa Rica aún se encuentra en una etapa de desarrollo, lo que plantea interrogantes sobre su efectividad en la gestión de ciberataques como los sufridos por la Caja Costarricense de Seguro Social (CCSS).

El propósito de este estudio es analizar de manera profunda cómo la ciberdiplomacia ha influido en la capacidad del Estado costarricense para responder a los ciberataques que afectaron a la Caja Costarricense de Seguro Social (CCSS) durante el periodo 2018-2023. Para llevar a cabo este análisis, se utilizarán múltiples enfoques metodológicos, incluyendo la revisión de documentos oficiales, tratados y acuerdos internacionales relacionados con la ciberseguridad, entrevistas con expertos en ciberseguridad y diplomacia, así como un análisis de casos específicos de ciberataques. A través de este enfoque, se pretende identificar las estrategias diplomáticas empleadas por el gobierno costarricense y evaluar su impacto en la mejora de la capacidad de respuesta ante incidentes cibernéticos. Asimismo, el estudio explorará cómo la cooperación internacional y los tratados multilaterales han contribuido a la implementación de políticas más efectivas en la prevención y gestión de ciberataques.

En términos conceptuales, esta investigación aborda dos ideas centrales: la ciberdiplomacia y la capacidad de respuesta a ciberataques. La relación entre estos dos conceptos es crucial para comprender cómo los países pueden fortalecer su defensa frente a amenazas cibernéticas a través de herramientas diplomáticas. La ciberdiplomacia, en su esencia, permite a los Estados colaborar con otros actores internacionales en la identificación de amenazas comunes, la creación de normativas globales sobre ciberseguridad y la coordinación de respuestas conjuntas ante incidentes cibernéticos. Por otro lado, la capacidad de respuesta a ciberataques se refiere a la habilidad de un Estado para detectar, mitigar y recuperarse de ataques cibernéticos de manera rápida y eficaz, minimizando el impacto sobre las infraestructuras críticas

y la sociedad. La relación entre estos conceptos es evidente: a medida que un Estado fortalece su ciberdiplomacia, puede mejorar su capacidad de respuesta a través del acceso a información compartida, recursos técnicos y apoyo internacional en momentos de crisis.

A pesar de los avances realizados en materia de ciberseguridad y ciberdiplomacia, existe una importante deficiencia en la literatura y en la práctica respecto a la evaluación de la efectividad de la ciberdiplomacia en la respuesta a ciberataques en el contexto costarricense. Si bien Costa Rica ha adoptado políticas de ciberseguridad y ha participado en foros internacionales sobre el tema, aún no se ha realizado un análisis exhaustivo que examine cómo estas políticas han influido en la capacidad del país para enfrentar ciberataques como los sufridos por la Caja Costarricense de Seguro Social (CCSS). Esta falta de estudios específicos representa un vacío en el conocimiento que esta investigación busca llenar, proporcionando una evaluación detallada de la influencia de la ciberdiplomacia en la respuesta del Estado costarricense a los ciberataques y ofreciendo recomendaciones para mejorar las políticas actuales.

Finalmente, la presente investigación se articula en torno a la pregunta central: ¿Cómo influyó la ciberdiplomacia en la capacidad del Estado costarricense para atender los ataques informáticos a la Caja Costarricense del Seguro Social (CCSS) en el periodo 2018-2023?. A partir de esta pregunta, se busca no solo describir los mecanismos diplomáticos utilizados por Costa Rica, sino también evaluar su efectividad y proponer mejoras para el futuro. La respuesta a esta pregunta permitirá comprender mejor el rol de la ciberdiplomacia en la gestión de incidentes cibernéticos y contribuirá a la creación de políticas más robustas en ciberseguridad que fortalezcan la capacidad de respuesta del país ante futuros desafíos.

1.2 Objetivos de la investigación

1.2.1. Objetivo general

Analizar la influencia de la ciberdiplomacia en la capacidad del Estado costarricense para responder a los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) durante el periodo 2018-2023.

1.2.2. Objetivos específicos

1. Identificar las principales estrategias de ciberdiplomacia adoptadas por el Estado costarricense entre 2018 y 2023 en el contexto de la ciberseguridad.

2. Describir los actores internacionales clave y su rol en las estrategias de ciberdiplomacia implementadas por el Estado costarricense durante los ciberataques a la Caja Costarricense del Seguro Social (CCSS).

3. Examinar la relevancia de la diplomacia en la colaboración de actores internacionales para enfrentar los problemas derivados de los ciberataques a la Caja Costarricense del Seguro Social (CCSS).

4. Evaluar la efectividad de las estrategias de ciberdiplomacia utilizadas para dar respuesta a los ciberataques sufridos por la Caja Costarricense del Seguro Social (CCSS).

1.3 Justificación

Esta investigación es relevante para Costa Rica, dado el impacto creciente de los ciberataques en las infraestructuras críticas del país y la importancia de fortalecer la capacidad de respuesta del Estado a través de herramientas como la ciberdiplomacia. El análisis de cómo la ciberdiplomacia ha influido en la respuesta del Estado costarricense ante los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) entre 2018 y 2023 es particularmente pertinente en un contexto donde la digitalización de los servicios públicos está en aumento, exponiendo a las instituciones a amenazas cibernéticas de mayor complejidad.

El análisis de la ciberdiplomacia y su influencia en la respuesta estatal frente a los ciberataques resulta fundamental para que Costa Rica desarrolle políticas de ciberseguridad más efectivas. Según un informe de la Unión Internacional de Telecomunicaciones (UIT), Costa Rica se ubicaba en la posición 52 de 194 países en el Índice Global de Ciberseguridad en 2020. Aunque este dato refleja un nivel de compromiso, la necesidad de fortalecer las capacidades diplomáticas para gestionar incidentes cibernéticos es evidente a partir de los recientes ataques que han afectado a instituciones como la Caja Costarricense de Seguro Social (CCSS). Esta

investigación permitirá una evaluación integral de las estrategias adoptadas y proporcionará insumos para mejorar la resiliencia del país ante futuras amenazas.

La importancia de este estudio también radica en su impacto social, ya que los ciberataques a la Caja Costarricense de Seguro Social (CCSS) afectaron gravemente los servicios de salud, que son esenciales para la población costarricense. En 2022, el ciberataque más grave sufrido por la Caja Costarricense de Seguro Social (CCSS) paralizó parcialmente el sistema, provocando retrasos en la atención médica y comprometiendo la seguridad de los datos de los pacientes . La protección de infraestructuras críticas como la salud pública es crucial para garantizar el bienestar social y económico del país. Al fortalecer la respuesta estatal a los ciberataques mediante la ciberdiplomacia, Costa Rica puede mejorar la seguridad de sus servicios públicos y, en consecuencia, proteger mejor a sus ciudadanos.

Desde un punto de vista práctico, esta investigación tiene implicaciones directas para la mejora de las políticas públicas en ciberseguridad y la gestión de incidentes cibernéticos. Al analizar los ciberataques a la Caja Costarricense de Seguro Social (CCSS) y las respuestas del Estado desde la perspectiva diplomática, el estudio proporcionará recomendaciones específicas para optimizar la coordinación entre las agencias gubernamentales, el sector privado y los actores internacionales. Estas mejoras no solo fortalecerán la capacidad de recuperación ante ataques cibernéticos, sino que también promoverán una cultura de prevención y cooperación internacional. Según el Foro Económico Mundial, las alianzas internacionales son clave para la mitigación de los riesgos cibernéticos , y este estudio contribuye a fortalecer esas alianzas en el caso costarricense.

A nivel teórico, esta investigación contribuirá a expandir el campo de estudio de la ciberdiplomacia en América Latina, un área en desarrollo que ha recibido atención limitada en comparación con otras regiones del mundo. La literatura actual sobre ciberseguridad tiende a enfocarse en los aspectos técnicos y la cooperación en defensa entre grandes potencias, dejando un vacío en el análisis de cómo los países en desarrollo, como Costa Rica, están utilizando la diplomacia para enfrentar los retos cibernéticos. Al abordar este vacío, el estudio ofrecerá una perspectiva novedosa sobre la interacción entre la diplomacia y la ciberseguridad en un contexto latinoamericano, permitiendo así la generación de nuevo conocimiento en el campo.

En términos metodológicos, este estudio se distingue por su enfoque interdisciplinario, combinando análisis de ciberseguridad, diplomacia y estudios de casos prácticos. La metodología propuesta, que incluye la revisión de documentos oficiales, entrevistas con expertos y análisis de casos concretos, proporcionará un enfoque integral que permitirá no solo evaluar la situación actual de Costa Rica en el ámbito de la ciberdiplomacia, sino también identificar las áreas de mejora. Este enfoque metodológico podrá ser replicado en otros países de la región que enfrentan desafíos similares, lo que refuerza la utilidad del estudio tanto a nivel local como regional.

La pertinencia de esta investigación está directamente relacionada con la creciente frecuencia y gravedad de los ciberataques a nivel mundial. Según datos del informe "Cybersecurity Ventures", los ciberataques podrían costar al mundo más de $10.5 billones anuales para 2025 . Este fenómeno no discrimina entre países desarrollados y en vías de desarrollo, lo que subraya la necesidad de una respuesta diplomática coordinada y proactiva. Para Costa Rica, un país que ha priorizado el uso de la diplomacia en la resolución de conflictos, es esencial adaptar estas capacidades a los retos del ciberespacio. En este sentido, el estudio es pertinente no solo por su relevancia actual, sino porque responde a una necesidad crítica de mejora en la seguridad nacional.

Finalmente, la viabilidad de este estudio está garantizada por el acceso a fuentes de información clave, como informes del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), documentos de organismos internacionales como la OEA, y la posibilidad de entrevistar a expertos en ciberdiplomacia y ciberseguridad. Además, la reciente atención mediática y gubernamental sobre los ciberataques a la Caja Costarricense de Seguro Social (CCSS) facilita la obtención de datos actualizados y relevantes. El enfoque de análisis documental, junto con entrevistas a actores clave, asegura que el estudio podrá llevarse a cabo dentro de los plazos previstos, con resultados que podrán aplicarse de forma inmediata para mejorar las políticas públicas en Costa Rica.

En conclusión, este estudio no solo es necesario para comprender y mejorar la respuesta del Estado costarricense ante ciberataques, sino que también ofrece una oportunidad única para fortalecer las capacidades diplomáticas del país en el ámbito digital. La investigación contribuirá

tanto al bienestar de la sociedad costarricense como al desarrollo teórico y metodológico del campo de la ciberdiplomacia en América Latina.

1.4 Antecedentes

En la presente investigación, se busca analizar la influencia de la ciberdiplomacia en la capacidad del Estado costarricense para responder a los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) durante el período 2018-2023. Para entender este fenómeno, es esencial contextualizar las tendencias internacionales y nacionales en materia de ciberseguridad y diplomacia digital. Este apartado recopila estudios y análisis previos que sientan las bases para la discusión sobre cómo la diplomacia ha influido en las respuestas a ciberataques, tanto a nivel global como local. Se abordan cinco referencias internacionales y cinco nacionales que muestran los avances y desafíos en el campo de la ciberseguridad y la diplomacia cibernética.

En el ámbito internacional, el autor James A. Lewis a través del *Centro de Estudios Estratégicos e Internacionales (CSIS)* realiza uno de los estudios más relevantes en el contexto de la cooperación internacional en ciberseguridad, titulado "*Cybersecurity and International Cooperation."* En este Lewis (2018) destaca la importancia de los acuerdos multilaterales como un pilar clave para que los Estados colaboren frente a las crecientes amenazas cibernéticas. El estudio argumenta que "los ataques cibernéticos han trascendido las fronteras nacionales, obligando a los países a replantear sus estrategias de defensa y a trabajar conjuntamente para fortalecer sus capacidades" (Lewis, 2018, p. 14).

La colaboración entre naciones, facilitada por acuerdos diplomáticos, es presentada como una herramienta fundamental para abordar los desafíos de la ciberseguridad en un entorno globalizado. Lewis subraya que "ningún país, por avanzado que sea en términos tecnológicos, puede defenderse eficazmente en solitario frente a los ciberataques" (2018, p. 15). Esta declaración resalta la interdependencia entre los Estados y la necesidad de cooperar a través de la diplomacia cibernética para compartir información y recursos.

En su análisis, Lewis (2018) menciona que los acuerdos multilaterales no solo fortalecen las capacidades técnicas de los Estados, sino también su poder de negociación en la arena internacional. En este sentido, señala que "las naciones que participan en iniciativas de cooperación cibernética no solo mejoran su defensa interna, sino que también se posicionan como líderes en la formulación de políticas globales de ciberseguridad" (p. 17). Así, la diplomacia no solo se limita a proteger las infraestructuras críticas nacionales, sino que también se convierte en una herramienta estratégica para ganar influencia en el ámbito global.

Un aspecto fundamental que resalta este estudio es cómo los países han utilizado la diplomacia para crear mecanismos de respuesta coordinada ante ciberataques, algo que es esencial en un mundo cada vez más interconectado. De acuerdo con Lewis (2018), "la coordinación a través de acuerdos multilaterales permite a los países actuar rápidamente y de manera eficaz cuando se enfrentan a amenazas cibernéticas, minimizando los daños y recuperándose con mayor agilidad" (p. 19). Esto implica que la ciberdiplomacia no solo trata de prevención, sino también de gestionar de manera colaborativa las crisis cibernéticas cuando estas ocurren.

El análisis de Lewis (2018) también tiene implicaciones directas para el caso de Costa Rica, ya que sugiere que la cooperación internacional ha sido un pilar fundamental para desarrollar capacidades locales en ciberseguridad. En el contexto de esta investigación, es relevante porque pone en evidencia que un país como Costa Rica, con limitaciones en recursos tecnológicos y financieros, puede beneficiarse significativamente de los acuerdos internacionales para mejorar su defensa ante ciberataques. En palabras de Lewis, "la participación en redes internacionales de cooperación cibernética es vital para los países con capacidades limitadas, ya que les permite acceder a tecnología avanzada y a asistencia técnica que de otra manera no podrían costear" (2018, p. 22).

En este sentido, la investigación de Lewis apoya la hipótesis de que la ciberdiplomacia ha sido instrumental para que Costa Rica mejore su capacidad de respuesta a los ciberataques. En particular, la cooperación con actores internacionales ha permitido al país acceder a conocimientos especializados y tecnologías de vanguardia que han fortalecido sus defensas, algo

que será analizado a lo largo de esta investigación en el contexto de los ataques a la Caja Costarricense de Seguro Social (CCSS).

La importancia de la diplomacia, según Lewis (2018), radica también en su capacidad para establecer marcos normativos que regulen las interacciones en el ciberespacio. Estos marcos ayudan a prevenir conflictos cibernéticos entre Estados, ya que proporcionan "normas claras que guían las acciones de los países en caso de incidentes cibernéticos, reduciendo así la posibilidad de una escalada no deseada de las tensiones" (p. 23). Costa Rica, al participar en acuerdos y tratados multilaterales en ciberseguridad, ha contribuido a la creación de estos marcos, lo que le ha permitido responder de manera más eficaz a los ciberataques recientes, particularmente aquellos dirigidos contra la Caja Costarricense de Seguro Social (CCSS).

En conclusión, el estudio de Lewis (2018) pone de manifiesto que la cooperación internacional en ciberseguridad es esencial para mejorar las capacidades defensivas de los países frente a amenazas cibernéticas transnacionales. En el caso de Costa Rica, la ciberdiplomacia ha jugado un papel crucial, permitiendo al país no solo fortalecer sus defensas, sino también mejorar su posicionamiento en el ámbito internacional. Este aspecto será analizado en profundidad en la presente investigación, evaluando cómo la diplomacia cibernética ha influido en la capacidad del Estado costarricense para enfrentar ciberataques, particularmente en el caso de los ataques a la Caja Costarricense de Seguro Social (CCSS).

Por otro lado, la Comisión Europea (2020) con sede en Bruselas, Bélgica a través del *"Informe sobre la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital"* detalla los avances en la implementación de una estrategia diplomática conjunta para enfrentar las crecientes amenazas cibernéticas dentro de los países miembros de la Unión Europea (UE). Este documento es clave para entender cómo la UE ha priorizado la cooperación en el ámbito de la ciberseguridad, un área en la que la diplomacia ha jugado un papel central. Según el informe, "los estados miembros de la UE han adoptado un enfoque multilateral, estableciendo marcos legales robustos y creando mecanismos de cooperación entre los sectores público y privado" (Comisión Europea, 2020). Esta estrategia ha permitido una respuesta más eficiente y coordinada ante ciberataques, lo que refuerza la postura de la UE como líder en la gobernanza global del ciberespacio.

El informe también destaca que “la coordinación entre los estados miembros ha mejorado significativamente, lo que ha llevado a una mayor capacidad para prevenir, detectar y responder a las amenazas cibernéticas” (*Comisión Europea, 2020*). Este enfoque coordinado es un ejemplo de cómo la ciberdiplomacia puede ser efectiva para unir a múltiples actores, incluyendo gobiernos, empresas privadas y organizaciones internacionales, con el fin de mejorar la resiliencia cibernética. El desarrollo de marcos legales conjuntos también ha sido un pilar importante en esta estrategia, ya que proporciona un marco común para que los países de la UE colaboren en la identificación y persecución de los responsables de ciberataques.

Una de las claves del éxito de la UE ha sido la creación de “redes de cooperación que involucran tanto al sector público como al privado” (*Comisión Europea, 2020*). Este modelo de colaboración permite compartir información crítica de manera rápida y efectiva, lo que facilita una mejor coordinación en tiempos de crisis. Además, el informe señala que “las alianzas con el sector privado han permitido el acceso a tecnologías avanzadas y a conocimientos especializados que son fundamentales para mejorar las capacidades de defensa cibernética” (*Comisión Europea, 2020*). Esto ha sido particularmente importante en el contexto de amenazas cibernéticas complejas y en evolución, que a menudo superan las capacidades técnicas de los gobiernos.

En cuanto a la diplomacia, la Comisión Europea reconoce que “la ciberdiplomacia ha sido esencial para la creación de normas comunes en el ciberespacio y para establecer canales de comunicación diplomáticos que permitan gestionar las tensiones derivadas de los ciberataques” (*Comisión Europea, 2020*). La capacidad de los países de la UE para coordinar sus esfuerzos diplomáticos ha sido fundamental para la adopción de normativas que guíen el comportamiento en el ciberespacio y para garantizar que las respuestas a los ciberataques sean proporcionales y fundamentadas en la cooperación internacional.

Este antecedente es particularmente relevante para la investigación, ya que demuestra cómo la UE ha utilizado la ciberdiplomacia no solo para fortalecer sus defensas, sino también para mejorar la capacidad de respuesta colectiva ante ciberamenazas. La experiencia de la UE ofrece un ejemplo a seguir para países como Costa Rica, que, aunque no cuentan con los mismos recursos que las naciones de la UE, pueden beneficiarse de la adopción de un enfoque diplomático multilateral en el ámbito de la ciberseguridad.

De manera similar, el autor Sanchez (2021) publicó un artículo en la *Revista de Relaciones Internacionales*, titulado *"Diplomacia digital en América Latina: Desafíos y oportunidades"* aborda el papel crucial que ha desempeñado la diplomacia digital en la región como herramienta para fortalecer la cooperación en ciberseguridad. Ramírez argumenta que "la creciente interconexión digital ha hecho que los países latinoamericanos enfrenten riesgos cibernéticos similares, lo que ha incentivado la creación de alianzas diplomáticas para hacer frente a estas amenazas." Según el autor, estas alianzas no solo han mejorado la capacidad de respuesta de los países, sino que también han permitido el desarrollo de políticas y marcos comunes para la protección de infraestructuras críticas.

Uno de los puntos clave del estudio es la integración de los países de América Latina, incluida Costa Rica, en organismos multilaterales como la Organización de los Estados Americanos (OEA), que ha jugado un papel fundamental en la creación de redes de cooperación regional en ciberseguridad. Ramírez señala que "la OEA ha sido un catalizador para la diplomacia digital en la región, proporcionando un espacio donde los países pueden compartir sus mejores prácticas, recursos técnicos y estrategias para mitigar ciberataques". En este sentido, Costa Rica ha sido un participante activo en estos foros multilaterales, lo que le ha permitido beneficiarse del intercambio de conocimientos y experiencias con otros países que enfrentan desafíos similares.

Además, Ramírez resalta que la diplomacia digital ha permitido a los países latinoamericanos "mejorar significativamente sus capacidades de detección y respuesta ante ciberataques". A través de la cooperación diplomática, se han establecido mecanismos conjuntos para la identificación temprana de amenazas cibernéticas, lo que ha resultado en una mejor prevención y mitigación de ataques en toda la región. Costa Rica, en particular, ha sido un ejemplo de cómo la diplomacia cibernética puede traducirse en medidas concretas de seguridad digital. El autor menciona que "Costa Rica ha buscado activamente apoyo externo para fortalecer sus capacidades en ciberseguridad, aprovechando acuerdos bilaterales y multilaterales facilitados por la OEA y otros organismos internacionales".

El análisis de Ramírez (2021) es fundamental para la investigación, ya que demuestra cómo la diplomacia digital ha sido un canal clave para facilitar la cooperación en ciberseguridad

entre los países de América Latina, lo que ha tenido un impacto directo en la mejora de sus capacidades de respuesta frente a ciberataques. Costa Rica, como parte de esta dinámica, ha utilizado la diplomacia como una herramienta para acceder a recursos técnicos y conocimiento especializado, lo que le ha permitido estar mejor preparada para enfrentar las amenazas cibernéticas.

Por otro lado, el informe del Grupo de Trabajo de la ONU sobre Ciberseguridad (2022) titulado *"Report of the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security"* aborda los desafíos globales en materia de seguridad cibernética, enfatizando la necesidad de establecer un marco común de ciberdiplomacia entre los Estados miembros. El informe destaca que "la creciente interdependencia de las infraestructuras críticas digitales hace que ningún país sea completamente inmune a los ciberataques", lo que subraya la importancia de que los Estados trabajen juntos para garantizar una seguridad cibernética eficaz. En este sentido, el estudio argumenta que la cooperación diplomática es esencial no solo para compartir información, sino también para "resolver conflictos cibernéticos antes de que escalen y afecten la estabilidad internacional".

Una de las principales contribuciones del informe es su llamado a un enfoque multilateral para abordar las amenazas cibernéticas. En particular, el Grupo de Trabajo de la ONU subraya que la falta de coordinación entre los Estados puede "incrementar la vulnerabilidad a los ataques cibernéticos y agravar los conflictos". Para abordar este problema, el informe propone el desarrollo de normas y principios comunes que guíen las interacciones en el ciberespacio. Según el informe, estas normas deben incluir "la no utilización de ciberarmas contra infraestructuras críticas, el respeto a la soberanía digital y la cooperación en la identificación y mitigación de amenazas cibernéticas".

La relevancia de este estudio radica en su enfoque sobre cómo la diplomacia cibernética puede servir como herramienta para prevenir conflictos y gestionar crisis cibernéticas de manera coordinada. El Grupo de Trabajo señala que "las respuestas unilaterales a los ciberataques pueden desencadenar represalias y escaladas conflictivas", lo cual hace evidente la necesidad de una respuesta colectiva basada en principios acordados internacionalmente. Para países como

Costa Rica, que ha sufrido ataques cibernéticos en infraestructuras críticas como la Caja Costarricense de Seguro Social (CCSS), la integración en estos marcos internacionales podría ofrecer mecanismos más efectivos para la gestión de futuras crisis.

El informe también menciona que la diplomacia cibernética no solo trata de evitar conflictos, sino que también tiene un componente preventivo: "la diplomacia es clave para construir confianza entre los Estados en el ciberespacio". Esto es particularmente importante en un entorno global donde los ciberataques pueden tener consecuencias transnacionales, afectando tanto a las economías como a las relaciones diplomáticas entre países. El Grupo de Trabajo de la ONU resalta que “la transparencia, el intercambio de información y la colaboración técnica son elementos fundamentales para construir un entorno de confianza mutua y seguridad”.

Desde la perspectiva de Costa Rica, que ha tenido un papel activo en la comunidad internacional en temas de derechos humanos y medioambientales, la adopción de un enfoque diplomático en ciberseguridad podría fortalecer su posición global. La participación en estos marcos multilaterales le permitiría al país "acceder a recursos y conocimientos técnicos internacionales", lo que podría mejorar significativamente su capacidad de respuesta ante ciberataques futuros. Además, el informe sugiere que los Estados que participan activamente en la ciberdiplomacia pueden “influir en la formulación de las reglas globales que rigen el ciberespacio”, lo que representa una oportunidad estratégica para naciones en desarrollo como Costa Rica.

En conclusión, el informe del *Grupo de Trabajo de la ONU sobre Ciberseguridad* (2022) aporta un enfoque integral sobre cómo la diplomacia cibernética puede ser utilizada para prevenir y gestionar conflictos cibernéticos. Para Costa Rica, la integración en estos esfuerzos internacionales podría ser un factor clave no solo en su capacidad para responder a futuros ciberataques, sino también en su contribución a la construcción de un ciberespacio más seguro y regulado. La ciberdiplomacia, según el informe, no es simplemente una herramienta reactiva, sino una estrategia preventiva que fomenta la estabilidad internacional en la era digital.

De manera complementaria, la Organización del Tratado del Atlántico Norte (OTAN) publicó un informe titulado *"NATO Cybersecurity Cooperation Report"*, en el mismo la OTAN

destaca su enfoque integral hacia la ciberseguridad, el cual combina la diplomacia, la cooperación internacional y el uso de tecnologías avanzadas para enfrentar las crecientes amenazas cibernéticas. Según el informe, "la colaboración entre los aliados de la OTAN ha sido esencial para responder a los ciberataques de forma rápida y eficaz, protegiendo tanto infraestructuras críticas como sistemas militares" (NATO Cybersecurity Cooperation Report, 2020, p. 5).

Este enfoque de la OTAN se basa en varios pilares: la cooperación multilateral entre los Estados miembros, la mejora de la resiliencia cibernética y el fortalecimiento de la capacidad de respuesta ante ciberataques. Un aspecto clave del informe es el reconocimiento de la diplomacia como una herramienta indispensable para establecer marcos de cooperación cibernética. Tal como se señala en el documento, "la diplomacia cibernética ha permitido a los Estados miembros no solo intercambiar información crítica sobre amenazas cibernéticas, sino también coordinar sus esfuerzos para desarrollar respuestas conjuntas a incidentes de gran escala" (*NATO Cybersecurity Cooperation Report*, 2020, p. 9).

El informe de 2020 subraya también el papel central que ha jugado la OTAN en la creación de capacidades cibernéticas entre sus aliados, lo que ha permitido a estos países no solo proteger mejor sus infraestructuras nacionales, sino también reforzar la seguridad colectiva de la organización. Según el informe, "la estrategia cibernética de la OTAN es única en su capacidad para integrar a diferentes actores estatales y no estatales en un marco coordinado de respuesta a ciberamenazas" (*NATO Cybersecurity Cooperation Report*, 2020, p. 12).

Un ejemplo destacado en el informe es el *Centro de Excelencia en Ciberdefensa Cooperativa* (CCDCOE) de la OTAN, establecido en Estonia, el cual ha sido fundamental en la capacitación de expertos en ciberseguridad y en el desarrollo de marcos normativos y técnicos para la defensa cibernética. Este centro actúa como "una plataforma para el intercambio de conocimientos y la formación de expertos en ciberdefensa de los Estados miembros y socios de la OTAN, promoviendo la cooperación técnica y la estandarización de los protocolos de ciberseguridad" (*NATO Cybersecurity Cooperation Report*, 2020, p. 14).

Aunque Costa Rica no es miembro de la OTAN, las lecciones que se desprenden de la experiencia de esta organización son útiles para su contexto, especialmente en términos de la importancia de la cooperación internacional y la creación de alianzas estratégicas. Costa Rica podría beneficiarse de un enfoque similar al de la OTAN al buscar fortalecer su seguridad cibernética a través de la colaboración con organismos internacionales, tal como lo ha hecho mediante su participación en iniciativas regionales de ciberseguridad promovidas por la OEA.

En términos de diplomacia cibernética, la experiencia de la OTAN pone de relieve la necesidad de que los Estados desarrollen no solo capacidades técnicas, sino también un marco diplomático que les permita colaborar efectivamente en la prevención y mitigación de ciberataques. En el caso de Costa Rica, la adopción de estrategias diplomáticas que faciliten la cooperación con otros países y organismos internacionales será crucial para enfrentar las crecientes amenazas cibernéticas. Como concluye el informe de la OTAN, "la ciberseguridad no es solo una cuestión de tecnología; es, ante todo, una cuestión de cooperación internacional y diplomacia estratégica" (*NATO Cybersecurity Cooperation Report*, 2020, p. 20).

Este enfoque es altamente relevante para la investigación, ya que ofrece un modelo de cómo la diplomacia cibernética puede desempeñar un papel central en la creación de capacidades nacionales para enfrentar ciberataques. Además, resalta la importancia de alianzas estratégicas en un contexto donde las amenazas cibernéticas trascienden fronteras y requieren una respuesta coordinada a nivel global. Costa Rica, aunque no forme parte de la OTAN, puede aprender de este enfoque para mejorar su ciberdefensa, especialmente en lo que respecta a la protección de infraestructuras críticas como la Caja Costarricense de Seguro Social (CCSS).

En el ámbito nacional, Sánchez (2020), publica su artículo titulado *"La ciberseguridad como un tema de diplomacia"* en el Portal de Revistas Académicas UCR, en el cual examina la evolución de las políticas de ciberseguridad en Costa Rica, poniendo un énfasis particular en la importancia de la cooperación internacional para el fortalecimiento de dichas políticas. El autor sostiene que “la ciberseguridad no es solo un asunto técnico, sino también un tema de diplomacia, donde la colaboración entre naciones se convierte en un elemento esencial para enfrentar los desafíos cibernéticos”. Esta afirmación resalta la relevancia de las relaciones diplomáticas en la construcción de capacidades locales para la defensa cibernética.

Sánchez destaca que Costa Rica ha estado activa en la búsqueda de alianzas estratégicas con organismos internacionales, afirmando que "la participación en foros multilaterales ha permitido a Costa Rica intercambiar conocimientos y recursos con otros países, lo cual ha resultado en la mejora de su infraestructura de ciberseguridad". Esta participación en redes internacionales ha sido fundamental para que Costa Rica no solo se adapte a los estándares globales de seguridad, sino que también establezca protocolos de respuesta ante incidentes cibernéticos.

El autor también menciona que, a través de su diplomacia, Costa Rica ha logrado "firmar acuerdos bilaterales que facilitan el intercambio de información sobre amenazas cibernéticas y mejores prácticas en el manejo de incidentes". Esto implica que el país ha reconocido la importancia de establecer relaciones sólidas con naciones que poseen una mayor experiencia en ciberseguridad. Esta estrategia es particularmente importante en el contexto de la creciente sofisticación de los ciberataques, donde el conocimiento compartido puede marcar la diferencia en la preparación y respuesta ante incidentes.

Además, Sánchez indica que "la colaboración con organismos internacionales, como la Organización de Estados Americanos (OEA), ha sido crucial para la implementación de políticas efectivas de ciberseguridad en el país". A través de esta cooperación, Costa Rica ha tenido acceso a recursos técnicos y financieros que han facilitado la capacitación de su personal en el manejo de amenazas cibernéticas. Esta interacción internacional se ha traducido en un fortalecimiento de las capacidades locales, permitiendo que el país no solo reaccione ante ciberataques, sino que también prevenga y mitigue sus efectos.

La investigación se centra en cómo estos acuerdos diplomáticos han influido en la respuesta de Costa Rica a los ciberataques más recientes, en particular los dirigidos a la Caja Costarricense de Seguro Social (CCSS). "El desarrollo de una estrategia de ciberseguridad integral, apoyada en la cooperación internacional, ha permitido a Costa Rica afrontar los desafíos cibernéticos con una mayor capacidad de respuesta", sostiene Sánchez. Este aspecto será fundamental para analizar cómo la diplomacia ha facilitado el intercambio de información y recursos entre Costa Rica y sus socios internacionales, y cómo esto ha impactado en la efectividad de las respuestas a incidentes cibernéticos.

En conclusión, el artículo de Sánchez proporciona un marco valioso para la investigación, al resaltar la interconexión entre la ciberseguridad y la diplomacia en Costa Rica. La evidencia presentada sugiere que el fortalecimiento de las políticas de ciberseguridad a través de la cooperación internacional no solo ha mejorado la infraestructura de seguridad del país, sino que también ha creado un entorno propicio para la colaboración y el intercambio de conocimientos. Este antecedente es clave para entender cómo Costa Rica puede continuar desarrollando su estrategia de ciberseguridad en un mundo cada vez más digitalizado y vulnerable a las amenazas cibernéticas.

Por otro lado, el informe del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de 2022, titulado *"Plan nacional de ciencia, tecnologia e innovacion 2022-2027"*, ofrece una perspectiva más concreta sobre la respuesta del Estado costarricense ante los ciberataques a la Caja Costarricense de Seguro Social (CCSS). Este documento es fundamental para comprender la interacción entre ciberseguridad y diplomacia, ya que resalta cómo las relaciones diplomáticas han influido directamente en la capacidad del país para manejar crisis cibernéticas significativas.

El informe del MICITT subraya la importancia de la asistencia técnica internacional en la respuesta a estos ataques, señalando que "la colaboración con otros países fue vital para contener los efectos del ataque y recuperar la operatividad de la Caja Costarricense de Seguro Social (CCSS)." Esto indica que la diplomacia cibernética no sólo ha sido un medio para compartir información, sino también un canal para movilizar recursos y apoyo técnico de naciones aliadas. El documento enfatiza que "los esfuerzos coordinados entre diversas agencias internacionales y locales permitieron una respuesta más ágil y eficiente ante la emergencia", lo cual refuerza la idea de que la cooperación internacional es un pilar esencial en la estrategia de ciberseguridad de Costa Rica.

Además, el informe detalla cómo se establecieron canales de comunicación con expertos en ciberseguridad de otros países, facilitando un intercambio de conocimientos que permitió a Costa Rica mejorar sus defensas. En este sentido, se menciona que "la experiencia adquirida a través de la colaboración con socios internacionales ha sido clave para fortalecer nuestras

capacidades internas y prevenir futuros ataques." Esta cita resalta la importancia de aprender de la experiencia de otros países que han enfrentado desafíos similares.

La experiencia de Costa Rica en la respuesta a los ciberataques a la Caja Costarricense de Seguro Social (CCSS) ofrece lecciones valiosas sobre el papel de la diplomacia cibernética en la gestión de crisis. El informe concluye que "la integración de la diplomacia en las estrategias de ciberseguridad es esencial para construir un ecosistema resiliente que pueda enfrentar las amenazas cibernéticas emergentes." Este enfoque no sólo es relevante para el contexto actual, sino que también sienta las bases para futuras políticas de ciberseguridad en el país.

Este antecedente será utilizado para evaluar cómo las relaciones diplomáticas han sido un factor determinante en la respuesta costarricense a los ciberataques, con el objetivo de identificar fortalezas y áreas de mejora. Al analizar el informe del MICITT (2022), se busca entender de qué manera las alianzas diplomáticas han permitido a Costa Rica no solo mitigar los efectos de los ciberataques, sino también avanzar en la creación de una infraestructura de ciberseguridad más robusta y sostenible. A través de este estudio, se pretende delinear un mapa de las estrategias exitosas y aquellas que requieren reevaluación, lo que podría guiar futuras decisiones en la esfera de la ciberseguridad en el país.

A la luz de lo anterior, el *"Informe del Instituto Costarricense de Electricidad (ICE) sobre la cooperación en ciberseguridad entre Costa Rica y la OEA"* (2019) complementa la evaluación al analizar de manera exhaustiva la cooperación entre Costa Rica y la Organización de los Estados Americanos (OEA) en el ámbito de la ciberseguridad. Este estudio destaca cómo la OEA ha sido un aliado estratégico en el fortalecimiento de las capacidades de ciberdefensa de Costa Rica, un país que, aunque ha avanzado significativamente en sus políticas de seguridad cibernética, todavía enfrenta múltiples desafíos en un contexto global cada vez más complejo.

La OEA ha desempeñado un papel fundamental en la implementación de programas de capacitación y asistencia técnica, los cuales han sido esenciales para la creación de un marco robusto de seguridad cibernética en Costa Rica. El informe señala que "la cooperación técnica proporcionada por la OEA ha permitido a Costa Rica establecer protocolos de respuesta ante incidentes cibernéticos, mejorando así su capacidad para gestionar amenazas". Esto refleja no

solo un avance en la infraestructura de seguridad, sino también un compromiso con la formación continua de los recursos humanos en el país.

Además, el ICE (2019) menciona que "la creación de redes de colaboración entre países de la región, facilitadas por la OEA, ha sido vital para el intercambio de información sobre ciberamenazas y buenas prácticas en la defensa cibernética". Este aspecto es particularmente relevante, ya que las ciberamenazas a menudo trascienden las fronteras nacionales, lo que hace indispensable una colaboración efectiva entre naciones. La OEA, al fomentar esta colaboración, no solo ha contribuido a la seguridad de Costa Rica, sino que también ha ayudado a fortalecer la seguridad regional en su conjunto.

El informe también resalta que "la participación de Costa Rica en los programas de la OEA ha permitido al país acceder a recursos y conocimientos que, de otro modo, no estarían disponibles". Este acceso a recursos es un factor crítico para el desarrollo de capacidades nacionales, ya que permite a Costa Rica mantenerse a la vanguardia en un campo que evoluciona rápidamente.

Este antecedente subraya la importancia de la diplomacia multilateral en la ciberseguridad costarricense, un aspecto que será explorado en profundidad en la investigación. A medida que se profundice en el análisis, se evaluará cómo estas colaboraciones han influido en la capacidad de respuesta del Estado costarricense frente a ciberataques, particularmente aquellos dirigidos a la *Caja Costarricense de Seguro Social (CCSS)*. La integración de Costa Rica en iniciativas multilaterales como las promovidas por la OEA se presenta como un modelo de referencia en la creación de capacidades y en la formulación de políticas efectivas en ciberseguridad, ofreciendo lecciones valiosas para otros países de la región y más allá.

Por otra parte, Arias (2021) publica el artículo titulado *"La Diplomacia Costarricense y la Ciberseguridad: Un Enfoque Multilateral"* a través de la Revista del Ministerio de Relaciones Exteriores. Este artículo describe cómo Costa Rica ha empleado la diplomacia para fortalecer su seguridad digital mediante la participación activa en foros internacionales y la firma de acuerdos bilaterales. Según Arias (2021), “la diplomacia costarricense ha jugado un papel clave en la

adopción de estrategias de ciberseguridad, no solo para proteger su infraestructura crítica, sino también para posicionarse como un referente en la región".

El artículo detalla que "Costa Rica ha utilizado su plataforma diplomática para fomentar la cooperación en ciberseguridad con países aliados, lo que le ha permitido acceder a recursos tecnológicos y asistencia técnica en momentos de crisis". Esta estrategia se ejemplifica con la participación en la *Conferencia Global de Ciberdiplomacia*, donde el país promovió "la creación de un frente común para la gestión de ciberamenazas en América Latina".

Asimismo, se destaca que "los acuerdos bilaterales con países como Estados Unidos y la Unión Europea han proporcionado acceso a tecnología avanzada y programas de capacitación para personal de ciberseguridad". Arias subraya que "la capacidad de respuesta de Costa Rica durante los ciberataques a la Caja Costarricense de Seguro Social (CCSS) en 2022 fue posible, en parte, gracias al apoyo internacional gestionado mediante la diplomacia".

Este antecedente es relevante porque demuestra cómo la combinación de diplomacia y cooperación internacional ha fortalecido la capacidad del Estado costarricense para enfrentar ciberataques. La investigación profundizará en estas dinámicas para evaluar su impacto en la protección de la infraestructura crítica del país.

Finalmente, el "*Informe del Centro de Estudios en Tecnología y Sociedad (CETES) sobre la estrategia de ciberseguridad de Costa Rica (2018-2023)."* de la Universidad Nacional ofrece una visión detallada sobre la estrategia de ciberseguridad del país entre 2018 y 2023, resaltando los avances logrados y los desafíos pendientes. Según CETES (2023), "la diplomacia ha sido fundamental en el diseño y ejecución de la estrategia nacional de ciberseguridad, permitiendo a Costa Rica alinear sus políticas con estándares internacionales".

El informe menciona que "la participación en foros internacionales ha facilitado no solo la obtención de recursos financieros, sino también la integración del país en redes globales de cooperación". En cuanto a la colaboración regional, CETES subraya que "la alianza con la OEA permitió la creación de equipos especializados en ciberdefensa, que fueron cruciales para responder a los ciberataques más recientes".

Sin embargo, CETES advierte que “a pesar de los logros, aún existen desafíos en la coordinación interinstitucional, lo que limita la capacidad de respuesta rápida ante incidentes”. Además, indica que “la falta de inversión en infraestructura tecnológica pone en riesgo la continuidad de los esfuerzos de ciberseguridad en el futuro”.

Este antecedente es relevante porque permite identificar las fortalezas y debilidades de la estrategia costarricense en ciberseguridad. La investigación analizará cómo la diplomacia ha influido en estos procesos y qué medidas adicionales podrían adoptarse para mejorar la resiliencia del Estado ante ciberataques.

1.5 Proyecciones

Las proyecciones de esta investigación buscan prever los logros y aportes que se obtendrán al analizar la influencia de la ciberdiplomacia en la respuesta del Estado costarricense ante los ciberataques sufridos por la Caja Costarricense de Seguro Social (CCSS). Estas metas están alineadas con los objetivos del estudio y con la necesidad de generar propuestas útiles para el fortalecimiento de las capacidades del país en ciberseguridad. A través de este trabajo, se espera no solo ampliar el conocimiento académico en temas de diplomacia digital y ciberseguridad, sino también ofrecer herramientas que contribuyan al desarrollo de políticas públicas más eficaces. Las siguientes proyecciones presentan de manera específica los resultados esperados del proceso investigativo.

1. Primero, se desea analizar cómo la ciberdiplomacia ha fortalecido la capacidad de respuesta de Costa Rica ante ciberataques, centrándose especialmente en los incidentes que han afectado a la Caja Costarricense de Seguro Social (CCSS). Para ello, se emplearán tanto fuentes primarias, como entrevistas con expertos en ciberseguridad y diplomacia, como documentos oficiales que detallan las estrategias adoptadas por el Estado en su respuesta a las amenazas cibernéticas.
2. En segundo lugar, se pretende identificar las fortalezas y debilidades de la respuesta costarricense a ciberataques a través del análisis de casos específicos. Esto permitirá entender qué estrategias han sido efectivas y cuáles requieren reevaluación. Se espera que esta información se extraiga de informes técnicos, análisis de incidentes previos y

recomendaciones de organismos internacionales, lo que ofrecerá un panorama claro de la situación actual en ciberseguridad en el país.

3. Finalmente, se busca proponer recomendaciones concretas para mejorar la estrategia de ciberseguridad de Costa Rica, basadas en los hallazgos del estudio. Estas recomendaciones estarán orientadas a optimizar la colaboración internacional y la diplomacia cibernética, y se derivarán de un análisis crítico de las políticas actuales, tomando como referencia las mejores prácticas implementadas en otros países. Este proceso se sustentará en un conjunto de fuentes, incluyendo literatura académica, informes de organismos internacionales y políticas públicas en ciberseguridad.

Las limitaciones de la investigación delimitan los alcances temáticos y metodológicos que no se abordarán, estableciendo un marco claro que enfoca el estudio en aspectos relevantes al problema planteado. Al centrar el análisis en los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) y en el papel de la diplomacia, ciertos aspectos técnicos o incidentes en otras instituciones quedarán fuera del alcance. Además, la dependencia de fuentes documentales y entrevistas podría restringir el acceso a información sensible, lo que representa un reto para la profundidad del análisis. Estas limitaciones permiten mantener la coherencia y viabilidad del proyecto, asegurando que el enfoque sea preciso y manejable dentro de los objetivos trazados.

1. En primer lugar, es importante reconocer que la investigación se centrará específicamente en los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS), lo que limita el alcance del análisis a este único contexto. Aunque otros sectores e instituciones costarricenses también enfrentan amenazas cibernéticas, su inclusión en este estudio podría desviar la atención del problema principal y dificultar una evaluación profunda.
2. En segundo lugar, la investigación dependerá de fuentes documentales y entrevistas, lo que puede restringir el acceso a información sensible relacionada con incidentes cibernéticos. Esta limitación podría afectar la profundidad del análisis, ya que no toda la información relevante puede ser divulgada por razones de seguridad nacional o confidencialidad.
3. Finalmente, el enfoque en la ciberdiplomacia como un elemento clave en la respuesta a ciberataques puede dejar de lado otros factores técnicos y operativos que también

influyen en la ciberseguridad. Por lo tanto, es posible que ciertos aspectos, como la infraestructura tecnológica o la capacitación del personal en ciberseguridad, no se aborden de manera exhaustiva en esta investigación.

CAPÍTULO II: MARCO TEÓRICO

2.1 Marco Histórico

El desarrollo de la ciberseguridad y la ciberdiplomacia ha sido un proceso complejo y en constante evolución, influenciado por el crecimiento de las amenazas digitales y la necesidad de establecer marcos regulatorios y de cooperación internacional. En este apartado se abordará la evolución de la ciberseguridad a nivel global, analizando los primeros ciberataques relevantes y el surgimiento de marcos internacionales de seguridad digital. Asimismo, se examinará el desarrollo de la ciberdiplomacia en organizaciones como la OTAN, la OEA y la ONU, con el fin de comprender cómo estas instituciones han influido en la respuesta de los Estados ante amenazas cibernéticas.

En el contexto costarricense, se presentará una revisión histórica de la Caja Costarricense del Seguro Social (CCSS), incluyendo sus antecedentes, el contexto político de su creación y su rol en la actualidad. Finalmente, se analizará la cronología de los ciberataques más relevantes en Costa Rica, con especial énfasis en el impacto del ataque a la Caja Costarricense de Seguro Social (CCSS) en 2022 y los cambios en las políticas y estrategias de ciberseguridad desde 2018. Todo esto permitirá comprender cómo el país ha respondido a los desafíos de la seguridad digital y el papel que la ciberdiplomacia ha jugado en este proceso.

2.1.1 Evolución de la Ciberseguridad a Nivel Internacional

El crecimiento exponencial de la digitalización y la interconectividad a nivel global ha generado nuevos desafíos en materia de seguridad. En este contexto, la ciberseguridad ha emergido como un pilar fundamental para la protección de infraestructuras críticas, datos sensibles y sistemas gubernamentales. Las amenazas cibernéticas, caracterizadas por su capacidad de trascender fronteras y afectar a múltiples actores simultáneamente, han impulsado la necesidad de desarrollar marcos regulatorios y mecanismos de cooperación internacional.

En respuesta a estos desafíos, organizaciones internacionales como la Organización del Tratado del Atlántico Norte (OTAN), la Organización de los Estados Americanos (OEA) y la Organización de las Naciones Unidas (ONU) han jugado un papel crucial en la definición de

estrategias de ciberseguridad y el desarrollo de la ciberdiplomacia como herramienta clave para la gestión de conflictos en el ciberespacio. Estas iniciativas han permitido establecer marcos normativos, fomentar el intercambio de información y fortalecer las capacidades de respuesta ante incidentes cibernéticos.

2.1.1.1 Primeros ciberataques relevantes a nivel global

El concepto de ciberseguridad ha evolucionado en respuesta a la creciente amenaza de ataques cibernéticos dirigidos a infraestructuras críticas, gobiernos, empresas y usuarios individuales. A medida que la tecnología avanzaba, también lo hacían las estrategias de ataque, lo que obligó a los Estados y al sector privado a desarrollar medidas de protección cada vez más sofisticadas.

Uno de los primeros ciberataques documentados ocurrió en 1988 con el gusano de Morris, considerado el primer malware propagado a gran escala en la historia de Internet. Creado por Robert T. Morris, este gusano infectó alrededor del 10% de los dispositivos conectados a ARPANET, la red precursora de Internet. El impacto de este ataque fue significativo, ya que dejó inoperativos numerosos sistemas y resaltó la vulnerabilidad de las redes interconectadas. Como consecuencia, se creó el primer Equipo de Respuesta a Emergencias Informáticas (CERT, por sus siglas en inglés), marcando un punto de inflexión en la seguridad cibernética (Denning, 1989).

El gusano de Morris pertenece a una categoría específica de malware que se replica y se propaga de manera autónoma sin necesidad de intervención humana. A diferencia de un virus informático, que requiere la ejecución de un archivo huésped para activarse, un gusano puede expandirse a través de redes explotando vulnerabilidades de seguridad existentes (Pfleeger & Pfleeger, 2015). Como se desprende del párrafo anterior, el ataque ocasionado por el gusano de Morris obligó a una respuesta informática inmediata, lo que evidenció la falta de protocolos de seguridad en los sistemas informáticos de la época. Este incidente impulsó el desarrollo de estrategias de mitigación y estableció las bases para la creación de equipos especializados en la detección y contención de amenazas cibernéticas.

A finales de la década de 1990, otro evento significativo conocido como Moonlight Maze evidenció el potencial del ciberespionaje. Este ataque, detectado en 1998, consistió en una serie de infiltraciones prolongadas a sistemas gubernamentales de los Estados Unidos, incluyendo agencias como el Pentágono, la NASA y el Departamento de Energía. Aunque la atribución exacta sigue siendo un tema de debate, las investigaciones sugieren que pudo haber sido llevado a cabo por actores estatales rusos. Este incidente demostró cómo los ataques cibernéticos podían ser utilizados como herramientas de espionaje a gran escala (Healey, 2013; Rid, 2020).

Moonlight Maze marcó un hito en la percepción de la ciberseguridad como un asunto de seguridad nacional. A diferencia del gusano de Morris, este ataque no buscaba la simple disrupción de sistemas, sino la extracción sistemática de información clasificada. Se estima que los atacantes accedieron a cientos de megabytes de datos confidenciales, lo que afectó gravemente la seguridad de las operaciones gubernamentales (Nakashima, 2016). Este evento llevó a los Estados Unidos a reforzar sus capacidades de ciberdefensa y a considerar el ciberespionaje como una amenaza estratégica a nivel global.

En el ámbito financiero, el ataque a la empresa E*Trade y Datek Online en 2000 es considerado uno de los primeros intentos de manipulación bursátil mediante técnicas cibernéticas. Los atacantes emplearon un esquema de *pump and dump*, inflando artificialmente el valor de ciertas acciones mediante operaciones fraudulentas antes de venderlas con ganancias significativas. Este caso sentó un precedente sobre la vulnerabilidad del sector financiero ante delitos informáticos (Kshetri, 2010).

Este tipo de ataques puso en evidencia que la ciberseguridad no solo debía centrarse en la protección de infraestructuras gubernamentales o militares, sino también en el sector financiero. Con el crecimiento de la economía digital, los mercados bursátiles y las plataformas de inversión se convirtieron en objetivos atractivos para los ciberdelincuentes, lo que llevó a la adopción de regulaciones más estrictas en materia de seguridad informática dentro de la industria financiera.

Uno de los ciberataques más importantes a nivel global ocurrió en 2007 contra Estonia, considerado el primer ciberataque a gran escala contra un Estado. En respuesta a la reubicación de un monumento soviético en Tallin, Estonia sufrió un ataque masivo de denegación de servicio

distribuido (DDoS) que afectó instituciones gubernamentales, bancos y medios de comunicación. Este evento demostró cómo los ataques cibernéticos podrían utilizarse como un medio de conflicto geopolítico y aceleró el desarrollo de políticas internacionales de ciberseguridad (Ottis, 2008).

Los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés) consisten en la saturación de un sistema informático con un volumen masivo de tráfico ilegítimo, lo que impide su funcionamiento normal. Este tipo de ataque se realiza generalmente a través de una red de dispositivos comprometidos, conocidos como botnets, que inundan los servidores con solicitudes hasta dejarlos inoperantes (Mirkovic & Reiher, 2004). En el caso de Estonia, los ataques paralizaron los servicios bancarios y gubernamentales durante varias semanas, afectando la economía y la comunicación del país. Se estima que las pérdidas económicas directas fueron millonarias, además de generar una crisis diplomática con Rusia, ya que las autoridades estonias señalaron a grupos con posibles vínculos con el Kremlin como responsables del ataque (Davis, 2007).

Finalmente, el descubrimiento de Stuxnet en 2010 marcó el inicio de una nueva era en la guerra cibernética. Este malware altamente sofisticado, diseñado específicamente para sabotear el programa nuclear de Irán, representó el primer caso documentado de un ciberataque con efectos destructivos sobre infraestructura física. Se estima que fue desarrollado por EE.UU. e Israel como parte de la operación encubierta *Olympic Games* (Zetter, 2014).

A diferencia de otros ataques previos, Stuxnet demostró el potencial de los ciberataques para causar daños tangibles en el mundo físico. Este malware estaba diseñado para sabotear centrifugadoras utilizadas en el enriquecimiento de uranio, causando su mal funcionamiento y retrasando significativamente el programa nuclear iraní (Langner, 2011). Se estima que el ataque destruyó aproximadamente 1,000 centrifugadoras y retrasó el avance del programa por varios años, lo que generó un debate internacional sobre el uso de herramientas cibernéticas como armas ofensivas en conflictos geopolíticos (Clarke & Knake, 2012).

Estos eventos han sido fundamentales para la evolución de la ciberseguridad, evidenciando la necesidad de desarrollar estrategias preventivas y mecanismos de respuesta ante

amenazas cibernéticas cada vez más sofisticadas. Además, han influido en la formulación de políticas públicas, acuerdos internacionales y estrategias de cooperación entre Estados para hacer frente a los crecientes desafíos en el ciberespacio.

2.1.1.2 Surgimiento de los Marcos Internacionales de Ciberseguridad y Desarrollo de la Ciberdiplomacia en Organizaciones Internacionales

La creciente dependencia global de las Tecnologías de la Información y la Comunicación (TIC) ha generado un aumento significativo en las amenazas cibernéticas, afectando tanto a infraestructuras críticas como a la seguridad nacional de los Estados. Este panorama ha impulsado a diversas organizaciones internacionales a desarrollar marcos de ciberseguridad y a fomentar la ciberdiplomacia como herramientas esenciales para la cooperación y la estabilidad en el ciberespacio.

La OTAN ha reconocido la ciberseguridad como un componente integral de su estrategia de defensa colectiva. Tras los ciberataques dirigidos contra Estonia en 2007, la organización intensificó sus esfuerzos en este ámbito, estableciendo en 2008 el Centro de Excelencia para la Defensa Cibernética Cooperativa (CCDCOE) en Tallin, Estonia. Este centro se dedica a la investigación, capacitación y desarrollo de doctrinas relacionadas con la defensa cibernética (NATO, 2020).

En 2016, durante la Cumbre de Varsovia, la OTAN declaró el ciberespacio como un dominio operativo, equiparándolo a los dominios tradicionales de tierra, mar y aire. Esta decisión permitió a la organización planificar y ejecutar operaciones cibernéticas defensivas y ofensivas, fortaleciendo su postura en ciberseguridad (NATO, 2020).

Además, la OTAN ha fomentado la ciberdiplomacia mediante la colaboración con países socios y otras organizaciones internacionales, promoviendo el intercambio de información y la creación de capacidades para enfrentar amenazas cibernéticas comunes. Estas iniciativas buscan establecer normas de comportamiento responsable en el ciberespacio y fortalecer la resiliencia colectiva ante ciberataques (NATO, 2020).

En el contexto latinoamericano, la OEA ha desempeñado un papel crucial en la promoción de la ciberseguridad y la ciberdiplomacia. A principios del siglo XXI, la OEA ya contaba con un Grupo de Trabajo en Delitos Informáticos en el marco de la Reunión de Ministros de Justicia y Fiscales Generales de las Américas (REMJA), demostrando su enfoque pionero en abordar colectivamente la ciberseguridad (Real Instituto Elcano, 2023).

En 2004, la OEA adoptó la Estrategia Interamericana Integral de Seguridad Cibernética, un enfoque multidimensional y multidisciplinario que constituye uno de los pilares de la organización en materia de gobernanza de la ciberseguridad (Bartolome, 2021). Esta estrategia promueve la cooperación entre los Estados miembros y el desarrollo de capacidades nacionales para enfrentar las amenazas cibernéticas.

El Comité Interamericano contra el Terrorismo (CICTE) ha sido el principal brazo ejecutor de la OEA en materia de ciberseguridad, implementando programas de capacitación, asistencia técnica y promoción de políticas públicas. Además, la OEA ha facilitado la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) en la región, fortaleciendo la capacidad de respuesta ante incidentes cibernéticos (OEA, 2023).

La OEA también ha impulsado la ciberdiplomacia mediante la creación de espacios de diálogo y cooperación entre los Estados miembros, promoviendo el intercambio de información y mejores prácticas en ciberseguridad. Estas iniciativas buscan establecer un enfoque común para enfrentar las amenazas cibernéticas y fortalecer la seguridad en el hemisferio occidental (Real Instituto Elcano, 2023).

Por otro lado, la ONU ha abordado la ciberseguridad y la ciberdiplomacia a través de diversas iniciativas y foros. Desde 1998, la Asamblea General ha adoptado resoluciones sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, subrayando la importancia de la cooperación entre los Estados para prevenir el uso malintencionado de las TIC (United Nations, 2015).

En 2004, se estableció el Grupo de Expertos Gubernamentales (GGE) para examinar las amenazas cibernéticas y proponer medidas para abordarlas. Este grupo ha producido varios

informes que destacan la aplicabilidad del derecho internacional en el ciberespacio y la necesidad de normas de comportamiento responsable de los Estados (United Nations, 2015).

Además, la ONU ha promovido la ciberdiplomacia mediante la creación de plataformas de diálogo, como el Foro de Gobernanza de Internet (IGF), que reúne a gobiernos, sector privado, sociedad civil y comunidad técnica para discutir políticas relacionadas con el ciberespacio. Estas iniciativas buscan fomentar un enfoque inclusivo y multilateral en la gobernanza de Internet y la ciberseguridad (United Nations, 2015).

2.1.2. Historia de la Caja Costarricense del Seguro Social (CCSS)

La Caja Costarricense del Seguro Social (CCSS) es una de las instituciones más trascendentales en la historia de Costa Rica. Desde su creación en 1941, ha sido el pilar fundamental del sistema de salud y seguridad social del país, garantizando el acceso equitativo a la atención médica para toda la población. Su desarrollo ha estado marcado por diversas reformas políticas, sociales y económicas, consolidándose como un modelo de referencia en Latinoamérica.

A lo largo de más de 80 años, la Caja Costarricense de Seguro Social (CCSS) ha evolucionado desde un sistema limitado de seguridad social hasta una red nacional de hospitales, clínicas y centros de atención primaria que brinda cobertura universal a los costarricenses. Este proceso ha sido acompañado por importantes avances en el financiamiento, la infraestructura hospitalaria y la integración de tecnologías en la prestación de servicios de salud.

2.1.2.1 Antecedentes Históricos de la Institución

Antes de la fundación de la Caja Costarricense de Seguro Social (CCSS), Costa Rica contaba con un sistema de salud fragmentado, caracterizado por la prestación de servicios médicos limitados a quienes podían costearlos. A inicios del siglo XX, la atención médica estaba dominada por hospitales de caridad y médicos privados, lo que generaba grandes desigualdades en el acceso a la salud (Solís, 2021).

El crecimiento de la economía cafetalera y la expansión de las plantaciones bananeras a finales del siglo XIX y principios del XX no se tradujeron en mejoras significativas para la clase trabajadora. La falta de derechos laborales y las precarias condiciones sanitarias derivaron en un aumento de enfermedades infecciosas, alta mortalidad infantil y bajas expectativas de vida (Fernández & Acuña, 2019).

Ante este panorama, comenzaron a surgir movimientos sociales y políticos que impulsaban la creación de un sistema de seguridad social. La presión de organizaciones sindicales, grupos políticos progresistas y médicos reformistas llevó a que el Estado costarricense considerara la posibilidad de establecer un modelo de seguro social similar al de algunos países europeos, como Alemania y el Reino Unido (Gutiérrez, 2020).

En 1941, en el contexto de un gobierno reformista liderado por Rafael Ángel Calderón Guardia, se aprobó la Ley de Creación de la Caja Costarricense del Seguro Social. Este hecho marcó el inicio de un sistema de protección social con una visión universalista y solidaria, basado en la contribución tripartita del Estado, los empleadores y los trabajadores (CCSS, 2023).

2.1.2.2 Contexto Político de su Creación

La creación de la Caja Costarricense de Seguro Social (CCSS) ocurrió en un contexto político y social de profundas transformaciones en Costa Rica. Durante el gobierno de Calderón Guardia (1940-1944), el país vivió un proceso de reformas impulsadas en alianza con la Iglesia Católica y el Partido Comunista de Costa Rica, que promovían la justicia social y la protección laboral (González, 2018).

Entre las reformas más importantes de esta época se encuentran:

1. El Código de Trabajo de 1943, que estableció derechos laborales fundamentales, como la jornada laboral de 8 horas, el derecho a la sindicalización y la protección contra el despido injustificado.
2. La creación de la Universidad de Costa Rica (UCR), como un esfuerzo por mejorar la educación y formar profesionales para el desarrollo del país.

3. El establecimiento de la Caja Costarricense de Seguro Social (CCSS), que introdujo el concepto de seguridad social y atención médica como un derecho fundamental.

La creación de la Caja Costarricense de Seguro Social (CCSS) no estuvo exenta de oposición. Grupos empresariales y sectores conservadores argumentaban que el modelo propuesto era inviable económicamente y que afectaría la competitividad de las empresas. Sin embargo, la creciente presión social y el respaldo de la comunidad internacional permitieron que el proyecto avanzara (Jiménez, 2017).

Durante las décadas de 1950 y 1960, la Caja Costarricense de Seguro Social (CCSS) comenzó a expandir su cobertura y servicios. Inicialmente, solo cubría a trabajadores asalariados urbanos, pero con el tiempo se amplió a sectores rurales y trabajadores independientes. En 1973, bajo el gobierno de José Figueres Ferrer, se impulsó la universalización de la seguridad social, convirtiendo a Costa Rica en uno de los primeros países de América Latina en garantizar atención médica para toda su población (Barboza, 2022).

2.1.2.3 Actualidad de la Caja Costarricense de Seguro Social (CCSS)

Hoy en día, la Caja Costarricense de Seguro Social (CCSS) es la única institución con incidencia directa en el sistema de salud costarricense, brindando atención médica a más de 5 millones de habitantes a través de una red de hospitales, clínicas y centros de atención primaria (OPS, 2023).

El sistema de salud de la Caja Costarricense de Seguro Social (CCSS) se organiza en tres niveles:

1. Atención primaria: Proporcionada por los Equipos Básicos de Atención Integral en Salud (EBAIS), encargados de la prevención y tratamiento de enfermedades comunes en comunidades.
2. Atención secundaria: Compuesta por clínicas y hospitales regionales que manejan casos de mayor complejidad.
3. Atención terciaria: Representada por hospitales nacionales especializados, como el Hospital México, el Hospital San Juan de Dios y el Hospital Nacional de Niños.

A pesar de sus logros, la Caja Costarricense de Seguro Social (CCSS) enfrenta importantes desafíos en la actualidad:

1. Envejecimiento poblacional: El aumento de la esperanza de vida ha generado una mayor demanda de servicios médicos y de pensiones, poniendo presión sobre la sostenibilidad del sistema.
2. Financiamiento y sostenibilidad: La Caja Costarricense de Seguro Social (CCSS) ha experimentado problemas financieros debido a la evasión de cuotas, el crecimiento de la deuda del Estado y el aumento de costos operativos.
3. Digitalización y ciberseguridad: La modernización del sistema de salud ha traído consigo riesgos asociados a la digitalización. En 2022, la Caja Costarricense de Seguro Social (CCSS) sufrió un ciberataque por parte del grupo de ransomware Conti, afectando gravemente sus sistemas administrativos y de atención médica (MICITT, 2022).

A pesar de estos desafíos, la Caja Costarricense de Seguro Social (CCSS) sigue siendo un modelo de referencia en América Latina. Su enfoque en prevención, acceso universal y atención integral ha permitido que Costa Rica mantenga altos estándares de salud pública, reflejados en indicadores como la esperanza de vida y la reducción de la mortalidad infantil (OPS, 2023).

2.1.3 Cronología de Ciberataques en Costa Rica

La seguridad cibernética en Costa Rica ha pasado por una transformación considerable en las últimas dos décadas. Lo que antes se consideraba una preocupación secundaria, asociada principalmente a la protección de datos personales y el resguardo de infraestructuras informáticas básicas, ha evolucionado hasta convertirse en un componente esencial de la seguridad nacional.

Con el crecimiento acelerado de la digitalización en sectores clave como salud, finanzas, comercio y servicios gubernamentales, la infraestructura tecnológica costarricense ha quedado expuesta a riesgos cada vez más sofisticados. La interconectividad global y la creciente dependencia de plataformas digitales han convertido a Costa Rica en un objetivo recurrente de ataques cibernéticos, evidenciando la vulnerabilidad del país ante actores malintencionados, tanto estatales como no estatales.

Desde ataques de phishing y denegación de servicio (DDoS) hasta incidentes de ransomware a gran escala, Costa Rica ha enfrentado desafíos significativos que han puesto en peligro la estabilidad de servicios esenciales. El ataque perpetrado contra la Caja Costarricense del Seguro Social (CCSS) en 2022 marcó un punto de inflexión en la historia de la ciberseguridad nacional, obligando a una revisión profunda de las estrategias y políticas de protección digital.

Este apartado presenta una cronología detallada de los ciberataques más relevantes en Costa Rica, agrupados en tres secciones principales:

1. Ciberataques antes de 2018, que evidencian las primeras amenazas significativas y las respuestas iniciales del Estado.
2. El ataque masivo a la Caja Costarricense de Seguro Social (CCSS) en 2022, el evento más crítico en la historia de la ciberseguridad costarricense, con impacto directo en la prestación de servicios de salud.
3. Los cambios en políticas y estrategias de ciberseguridad desde 2018, muestran cómo el país ha evolucionado en la gestión de amenazas cibernéticas y en la implementación de mecanismos de defensa digital.

A través de este análisis, se busca comprender la evolución de los riesgos cibernéticos en Costa Rica y la respuesta del Estado ante una realidad en la que la ciberseguridad es un pilar fundamental de la estabilidad nacional.

2.1.3.1 Ciberataques más relevantes antes de 2018

Antes de 2018, Costa Rica experimentó varios ataques cibernéticos que, si bien no generaron crisis de gran magnitud, sí evidenciaron vulnerabilidades críticas en los sistemas informáticos del país. Estos incidentes marcaron el inicio de una preocupación creciente por la ciberseguridad y evidenciaron la necesidad de fortalecer los protocolos de defensa digital en el ámbito estatal y privado.

A medida que el uso de plataformas en línea se expandía en sectores clave como la administración tributaria, la banca y los servicios gubernamentales, el país comenzó a enfrentar

una nueva clase de amenazas digitales, incluyendo ataques de denegación de servicio (DDoS), intentos de intrusión en redes bancarias y campañas de phishing dirigidas a ciudadanos y funcionarios públicos.

Uno de los primeros ciberataques de alto perfil en Costa Rica ocurrió en 2012, cuando los servidores del Ministerio de Hacienda fueron afectados por un ataque de denegación de servicio distribuido (DDoS). Este tipo de ataque consiste en el envío masivo de solicitudes a un servidor hasta sobrecargarlo y provocar la caída de los servicios en línea. Como resultado, las plataformas de declaración y pago de impuestos quedaron inhabilitadas por varias horas, afectando a miles de contribuyentes que dependían de estos sistemas para cumplir con sus obligaciones fiscales (Chacón, 2013).

A pesar de que el impacto fue temporal y los sistemas fueron restaurados en pocas horas, este incidente reveló deficiencias en la seguridad de las plataformas críticas del Estado. Además, puso en evidencia la falta de protocolos de respuesta inmediata ante incidentes cibernéticos, lo que generó un debate sobre la necesidad de mejorar la infraestructura de seguridad digital en las instituciones gubernamentales.

Por otro lado, el sector financiero fue uno de los más afectados por intentos de ciberataques en el periodo previo a 2018. Entre 2016 y 2017, se reportaron múltiples intentos de intrusión en sistemas bancarios, particularmente mediante ataques de phishing dirigidos a clientes y funcionarios de entidades como el Banco Nacional de Costa Rica (BNCR) y el Banco de Costa Rica (BCR) (Morales, 2018).

El phishing es una técnica de ingeniería social utilizada por ciberdelincuentes para engañar a los usuarios y obtener credenciales de acceso o información bancaria mediante correos electrónicos fraudulentos. En 2017, el Banco de Costa Rica (BCR) detectó una campaña masiva de correos electrónicos falsos que contenían enlaces maliciosos diseñados para robar información de los clientes y realizar transacciones fraudulentas. Como resultado de este ataque, varios clientes sufrieron pérdidas económicas significativas y el banco se vio obligado a reforzar sus protocolos de autenticación, implementando verificación en dos pasos y alertas de seguridad más estrictas (Rodríguez, 2017).

Además, en 2016, se detectaron intentos de acceso no autorizado a sistemas de procesamiento de pagos, lo que obligó a las instituciones financieras a mejorar sus infraestructuras de detección y respuesta ante ataques cibernéticos. Estos incidentes fueron una señal de advertencia sobre la creciente sofisticación de los ciberdelincuentes y la necesidad de una mayor inversión en tecnologías de ciberseguridad, capacitación del personal y educación a los usuarios para prevenir ataques futuros.

Entre 2015 y 2017, diversas entidades estatales costarricenses enfrentaron intentos de acceso no autorizado a sus sistemas y vulneraciones en sus páginas web oficiales. Los sitios web del Gobierno fueron objeto de ataques que buscaban explotar debilidades en la infraestructura tecnológica estatal, lo que llevó a la necesidad de establecer protocolos más estrictos de protección de la información pública.

Uno de los incidentes más preocupantes se registró en 2016, cuando grupos de hackers intentaron ingresar a los sistemas de varias instituciones gubernamentales, incluyendo ministerios y entidades encargadas de la seguridad nacional. Si bien estos intentos de acceso no lograron comprometer información clasificada, el Gobierno reconoció la necesidad de fortalecer sus defensas digitales y aumentar la vigilancia sobre posibles amenazas futuras (MICITT, 2017).

Ante este panorama, en 2017, el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) impulsó la creación de la Dirección de Gobernanza Digital, una entidad encargada de supervisar y coordinar los esfuerzos de seguridad informática en el sector público. Este organismo tenía como objetivo fortalecer la ciberseguridad en instituciones estatales, desarrollar estrategias de prevención y respuesta ante incidentes, y promover la capacitación de funcionarios en temas de protección digital (MICITT, 2017).

Los incidentes de ciberseguridad en Costa Rica antes de 2018 reflejan una tendencia creciente de amenazas cibernéticas, que afectaron tanto al sector público como al privado. Los ataques a entidades gubernamentales, bancos y plataformas de servicios en línea expusieron importantes deficiencias en la infraestructura de ciberseguridad del país y pusieron en evidencia la necesidad de desarrollar estrategias más robustas de protección digital.

A pesar de los esfuerzos por mejorar la seguridad informática en este periodo, la falta de preparación y recursos especializados en ciberseguridad continuó siendo un desafío significativo. Esto se hizo aún más evidente en años posteriores, cuando Costa Rica enfrentó ataques cibernéticos de mayor magnitud, incluyendo el ciberataque masivo contra la Caja Costarricense del Seguro Social (CCSS) en 2022, un evento que marcó un antes y un después en la seguridad digital del país.

El análisis de estos incidentes previos permite comprender cómo la ciberseguridad ha evolucionado en Costa Rica y cómo el país ha tenido que adaptar sus políticas y estrategias de defensa digital ante un entorno cada vez más amenazante y sofisticado.

2.1.3.2 Impacto del ataque a la Caja Costarricense del Seguro Social en 2022

Uno de los ciberataques más devastadores en la historia de Costa Rica ocurrió en mayo de 2022, cuando el grupo de ransomware Conti, de origen ruso, lanzó un ataque masivo contra múltiples instituciones gubernamentales, incluyendo la Caja Costarricense del Seguro Social (CCSS). Este evento puso en evidencia las vulnerabilidades de la infraestructura digital del país y provocó una crisis sin precedentes en la gestión de los servicios públicos esenciales.

En el caso de la Caja Costarricense de Seguro Social (CCSS), el impacto fue particularmente grave, ya que sus sistemas informáticos quedaron paralizados, afectando la prestación de servicios de salud a nivel nacional.

Hospitales, clínicas y centros médicos dependían de plataformas digitales para el manejo de expedientes médicos, citas y registros administrativos, por lo que la interrupción generó un colapso en la atención sanitaria y dejó a miles de costarricenses sin acceso oportuno a tratamientos médicos.

El ataque a la Caja Costarricense de Seguro Social (CCSS) se llevó a cabo mediante el uso de ransomware, un software malicioso diseñado para cifrar archivos críticos y exigir un rescate económico a cambio de la clave de desencriptación. Este tipo de ataque ha sido empleado en múltiples ocasiones a nivel internacional contra infraestructuras críticas, y en el caso de Costa Rica, sus consecuencias fueron particularmente severas.

Entre los principales sistemas afectados estuvieron los expedientes médicos electrónicos, los sistemas administrativos y de citas, así como diversas plataformas internas de la institución. La inoperatividad de estos sistemas obligó a los centros de salud a volver a procesos manuales, lo que generó retrasos significativos en la atención médica y una sobrecarga en el personal sanitario. Además, el grupo Conti exigió un rescate millonario, amenazando con divulgar información confidencial si no se cumplía con el pago. Sin embargo, el gobierno costarricense adoptó una postura firme al negarse a negociar con los atacantes, optando en su lugar por restaurar los sistemas con el apoyo de expertos en ciberseguridad nacionales e internacionales.

El impacto del ciberataque fue devastador en múltiples niveles. En primer lugar, el colapso del sistema de citas y registros médicos generó la suspensión de consultas, cirugías y tratamientos esenciales, afectando directamente la salud de los pacientes. Según un informe de la Caja Costarricense de Seguro Social (CCSS), se estima que durante las primeras semanas posteriores al ataque, más de 34.000 citas médicas fueron canceladas debido a la imposibilidad de acceso a los sistemas digitales (CCSS, 2022). Además, los hospitales y clínicas, que dependían de plataformas electrónicas para la asignación de recursos y la gestión de emergencias, experimentaron una notable reducción en su capacidad de respuesta, lo que agravó la crisis en la prestación de los servicios de salud (La Nación, 2022).

Otro aspecto crítico fue la exposición de datos sensibles, ya que se filtraron documentos internos con información confidencial sobre pacientes y empleados de la Caja Costarricense de Seguro Social (CCSS). Según el MICITT, el grupo de ciberdelincuentes responsable del ataque habría extraído al menos 1TB de datos, incluyendo expedientes clínicos, información financiera y credenciales de acceso a los sistemas institucionales (MICITT, 2022). Esta situación generó preocupaciones sobre la privacidad y la protección de datos personales, lo que llevó a la Agencia de Protección de Datos de los Habitantes (PRODHAB) a iniciar una investigación sobre el posible incumplimiento de normativas de seguridad informática.

A nivel financiero, las pérdidas económicas derivadas de este ataque fueron significativas, con un costo estimado de recuperación superior a los 30 millones de dólares, cifra confirmada en un informe de la Contraloría General de la República (CGR, 2023). Este monto incluyó no solo la inversión en infraestructura de ciberseguridad y la adquisición de nuevas

plataformas tecnológicas, sino también el impacto económico derivado de la paralización de los servicios de salud y los costos operativos adicionales generados por la crisis (Forbes Centroamérica, 2022).

Ante la magnitud del ataque, el gobierno costarricense declaró estado de emergencia nacional, siendo la primera vez que un incidente de esta naturaleza recibía tal clasificación en el país. En un discurso oficial, el presidente Rodrigo Chaves calificó la situación como un "ataque directo a la estabilidad del país" y justificó la declaratoria de emergencia como una medida necesaria para asignar recursos extraordinarios que permitieran mitigar los daños y fortalecer las estrategias de ciberseguridad (Casa Presidencial, 2022). Como parte de la respuesta gubernamental, se implementaron diversas acciones para contener la crisis, entre ellas la intervención del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y el Instituto Costarricense de Electricidad (ICE), que desplegaron un equipo de expertos en ciberseguridad para restaurar los sistemas afectados y evaluar las vulnerabilidades en la infraestructura tecnológica del país (MICITT, 2022).

Además, Costa Rica recurrió a la cooperación internacional, solicitando apoyo de agencias especializadas como el FBI, Microsoft e Interpol. Estas entidades brindaron asesoramiento sobre el grupo Conti, apoyaron en la restauración de servidores y colaboraron en la investigación para identificar posibles responsables y evitar futuros ataques similares.

El ataque también impulsó un fortalecimiento de la Unidad Nacional de Ciberseguridad (UNCIBER), que recibió recursos adicionales para mejorar el monitoreo de amenazas, la respuesta a incidentes y la capacitación de funcionarios en seguridad digital. Además, se inició un proceso de revisión de políticas y normativas en materia de ciberseguridad, con el objetivo de establecer marcos regulatorios más sólidos y eficaces para proteger las infraestructuras críticas del país. Como resultado de esta crisis, se evidenció la necesidad de invertir en infraestructuras tecnológicas resilientes, mejorar la cooperación entre el sector público y privado, y promover una cultura de concienciación y formación en ciberseguridad.

El ciberataque a la Caja Costarricense de Seguro Social (CCSS) en 2022 marcó un antes y un después en la ciberseguridad costarricense. Más allá de los daños inmediatos, este evento

llevó a una reconfiguración de las estrategias de seguridad digital del país, demostrando la importancia de la ciberdiplomacia, la cooperación internacional y la inversión en ciberdefensa como pilares fundamentales para la protección de infraestructuras críticas en la era digital.

2.1.3.3 Cambios en políticas y estrategias de ciberseguridad desde 2018

Desde 2018, Costa Rica ha experimentado una transformación significativa en sus estrategias de ciberseguridad, impulsada por la creciente digitalización de los servicios públicos y privados, así como por el incremento en la frecuencia y sofisticación de los ciberataques. En particular, el ataque de ransomware dirigido a la Caja Costarricense de Seguro Social (CCSS) en 2022 evidenció vulnerabilidades críticas en la infraestructura digital del Estado y enfatizó la necesidad de fortalecer los marcos normativos y operativos en materia de seguridad informática. Como respuesta a estos desafíos, el gobierno costarricense ha desarrollado e implementado diversas políticas y estrategias con el propósito de mitigar los riesgos cibernéticos, mejorar la capacidad de respuesta ante incidentes y fortalecer la cooperación internacional en la materia (MICITT, 2022; OEA, 2023).

Uno de los principales avances en materia de ciberseguridad en Costa Rica fue la formulación e implementación de la Estrategia Nacional de Ciberseguridad 2018-2022, la cual constituyó un marco normativo integral orientado a la protección de infraestructuras críticas, la prevención de amenazas cibernéticas y el fortalecimiento de capacidades en seguridad digital. Dicha estrategia, elaborada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) con el apoyo de organismos internacionales como la Organización de los Estados Americanos (OEA), estableció los siguientes ejes de acción (MICITT, 2018):

1. Mejorar la protección de infraestructuras críticas mediante auditorías de seguridad.
2. Fortalecer la capacitación y concienciación en ciberseguridad a nivel público y privado.
3. Actualizar el marco normativo para garantizar una respuesta efectiva ante incidentes cibernéticos.
4. Promover la cooperación internacional a través de alianzas estratégicas para el intercambio de información y asistencia técnica (OEA, 2019).

Estos ejes permitieron la consolidación de un enfoque estructurado para la seguridad digital en el país, fomentando la resiliencia frente a amenazas emergentes en el ciberespacio.

En 2019, con el objetivo de fortalecer la capacidad del país para hacer frente a las crecientes amenazas en el ciberespacio, se creó la Unidad Nacional de Ciberseguridad (UNCIBER), adscrita al MICITT. Esta entidad fue concebida como un organismo encargado de coordinar la detección, análisis y mitigación de incidentes de seguridad informática en el ámbito gubernamental y en sectores estratégicos (MICITT, 2019).

Entre las funciones principales de UNCIBER se destacan el monitoreo de incidentes cibernéticos en las instituciones estatales, la coordinación de respuestas ante ataques informáticos y la colaboración con agencias de seguridad internacionales, lo que permitió el acceso a herramientas y conocimientos avanzados en ciberseguridad (Cordero, 2021). No obstante, el ciberataque perpetrado contra la Caja Costarricense de Seguro Social (CCSS) en 2022 evidenció la insuficiencia de los recursos y capacidades de UNCIBER para hacer frente a amenazas de gran escala, lo que motivó la necesidad de fortalecer su estructura y alcance operativo (Chacón, 2022).

Con el propósito de dotar al Estado de herramientas jurídicas más eficaces para combatir la ciberdelincuencia, en 2020 se promulgó una reforma a la Ley de Delitos Informáticos, la cual estableció sanciones más rigurosas para delitos relacionados con ataques a infraestructuras críticas, el robo de información sensible y la propagación de malware (Asamblea Legislativa de Costa Rica, 2020).

Entre las disposiciones más relevantes de esta reforma destacan el endurecimiento de penas para los delitos informáticos que afecten el funcionamiento de instituciones del Estado y empresas del sector privado, y la implementación de mecanismos de cooperación internacional que faciliten la persecución penal de ciberdelincuentes y la extradición de individuos responsables de ataques cibernéticos (MICITT, 2021).

En 2023, a raíz del impacto del ataque del grupo Conti en el país, se propusieron nuevas modificaciones al marco legal, orientadas a agilizar la persecución penal de los delitos

informáticos y fortalecer la colaboración entre el sector público y organismos internacionales de ciberseguridad (Rodríguez, 2023).

Ante la creciente sofisticación de las amenazas cibernéticas y la necesidad de contar con un organismo especializado en la prevención y respuesta ante incidentes de seguridad informática, en 2022 se estableció el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR). Dicho centro opera como una entidad de monitoreo y reacción ante ciberataques, proporcionando asistencia técnica a instituciones gubernamentales y empresas del sector privado (MICITT, 2022). Entre sus principales funciones destacan la detección y análisis de amenazas cibernéticas, la emisión de alertas y capacitaciones en ciberseguridad, y la coordinación de respuestas ante incidentes de seguridad, facilitando la recuperación de los servicios afectados de manera eficiente (Gutiérrez, 2023).

A pesar de los avances logrados en materia de ciberseguridad, Costa Rica aún enfrenta desafíos significativos en este ámbito. Entre los principales obstáculos se pueden señalar las deficiencias en la infraestructura de ciberseguridad, lo que limita la capacidad de detección y respuesta ante ataques sofisticados (Solano, 2023), la falta de personal especializado, lo que dificulta la implementación de estrategias efectivas para la protección de los sistemas informáticos (OEA, 2023), y la creciente complejidad de las amenazas cibernéticas, lo que demanda una actualización constante de los protocolos de seguridad y las tecnologías utilizadas (Mora, 2023).

En respuesta a estos desafíos, el gobierno costarricense ha planteado la actualización de la Estrategia Nacional de Ciberseguridad para el período 2023-2027, con el objetivo de consolidar una infraestructura de seguridad digital más robusta y adaptada a las necesidades actuales del país (MICITT, 2023).

2.1.4. Desarrollo de la Ciberdiplomacia en Costa Rica

La digitalización de los servicios públicos y privados en Costa Rica ha traído consigo grandes avances tecnológicos, pero también ha expuesto al país a una creciente cantidad de amenazas cibernéticas. En este contexto, la ciberdiplomacia ha emergido como un eje

fundamental dentro de la política exterior y de seguridad del Estado costarricense, en un esfuerzo por fortalecer la protección de sus infraestructuras digitales y garantizar una respuesta coordinada ante ciberataques.

La ciberdiplomacia, entendida como la aplicación de estrategias diplomáticas para la gestión de riesgos cibernéticos, ha sido crucial para Costa Rica, especialmente tras los ataques sufridos en los últimos años, incluyendo el devastador ataque del grupo Conti en 2022. Ante la creciente sofisticación de las amenazas digitales, el país ha adoptado un enfoque proactivo en la cooperación internacional, suscribiendo acuerdos bilaterales y multilaterales, participando en foros globales de ciberseguridad y fortaleciendo el rol del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) en la formulación e implementación de políticas cibernéticas.

2.1.4.1 Participación de Costa Rica en foros internacionales de ciberseguridad

Desde finales de la década de 2010, Costa Rica ha incrementado significativamente su presencia en foros internacionales enfocados en la ciberseguridad, con el objetivo de fortalecer sus capacidades de prevención, respuesta y recuperación ante incidentes cibernéticos. En este sentido, el país ha desarrollado alianzas estratégicas con organismos multilaterales que lideran la gestión de la ciberseguridad a nivel global.

Uno de los espacios más relevantes en los que Costa Rica ha tenido una participación activa es la Organización de los Estados Americanos (OEA). A través de su adhesión al Comité Interamericano contra el Terrorismo (CICTE) y su Programa de Ciberseguridad, el país ha trabajado en la implementación de marcos regulatorios y estrategias de fortalecimiento de la seguridad digital en el sector público y privado. En este contexto, Costa Rica ha recibido asistencia técnica y capacitación en materia de ciberseguridad, enfocándose en la protección de infraestructuras críticas y en la formulación de planes nacionales de respuesta ante ataques cibernéticos (OEA, 2021).

Otro organismo clave en el que Costa Rica ha consolidado su participación es la Unión Internacional de Telecomunicaciones (UIT), entidad especializada de la Organización de las

Naciones Unidas (ONU) que promueve el desarrollo de estándares internacionales en ciberseguridad. La colaboración con la UIT ha permitido a Costa Rica mejorar la regulación de su sector digital, así como acceder a herramientas de evaluación de riesgos cibernéticos y programas de fortalecimiento de la ciberresiliencia (UIT, 2022).

Asimismo, Costa Rica ha sido parte del Foro Global sobre Ciberexperticia (GFCE) desde 2019. Este organismo promueve el fortalecimiento de capacidades de ciberseguridad en países en desarrollo, permitiendo a Costa Rica acceder a asistencia técnica y participar en iniciativas de formación para funcionarios públicos y expertos en seguridad digital. La vinculación con este foro ha sido fundamental para mejorar la capacidad de prevención y respuesta del país frente a amenazas cibernéticas emergentes (GFCE, 2020).

2.1.4.2 Acuerdos bilaterales y multilaterales para la cooperación en ciberdefensa

El compromiso de Costa Rica con la ciberseguridad se ha visto reflejado en la firma de acuerdos bilaterales y multilaterales para el fortalecimiento de su infraestructura de ciberdefensa. Estos acuerdos han sido clave para dotar al país de herramientas tecnológicas avanzadas, mejorar la cooperación en investigaciones de ciberdelitos y fortalecer la resiliencia de las instituciones estatales frente a ataques digitales.

A nivel bilateral, Costa Rica ha consolidado una estrecha relación con Estados Unidos, nación con la que mantiene acuerdos de cooperación en seguridad digital. En mayo de 2022, tras el ciberataque del grupo Conti, el gobierno costarricense recibió apoyo técnico del Buró Federal de Investigaciones (FBI) y del Departamento de Seguridad Nacional de EE.UU., los cuales proporcionaron asistencia en el análisis del ataque, la recuperación de sistemas comprometidos y la implementación de mejores prácticas en ciberseguridad (Embajada de EE.UU. en Costa Rica, 2022).

Otro socio clave en el fortalecimiento de la ciberdefensa costarricense ha sido España, a través del Instituto Nacional de Ciberseguridad de España (INCIBE). La cooperación con INCIBE ha permitido la capacitación de especialistas costarricenses en la identificación y

mitigación de riesgos cibernéticos, así como en el desarrollo de estrategias de ciberseguridad orientadas a la protección de infraestructuras críticas (MICITT, 2021).

En el ámbito multilateral, Costa Rica ha sido signataria del Convenio de Budapest sobre Ciberdelincuencia, promovido por el Consejo de Europa. Este tratado, adoptado en 2018 por el país, ha sido fundamental para mejorar las capacidades del Estado costarricense en la persecución de ciberdelincuentes, al facilitar la cooperación con otras naciones en la investigación y judicialización de delitos informáticos (Consejo de Europa, 2020).

Además, en 2023, Costa Rica suscribió un acuerdo con la OEA para la implementación de programas de fortalecimiento de la ciberseguridad en sectores estratégicos como la banca y las telecomunicaciones. Este acuerdo ha permitido la ejecución de auditorías de seguridad y la capacitación de funcionarios públicos en la gestión de incidentes cibernéticos (OEA, 2023).

2.1.4.3 Papel del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) en la política cibernética del país

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) ha desempeñado un papel central en la formulación e implementación de políticas de ciberseguridad en Costa Rica, liderando esfuerzos para mejorar la capacidad de prevención y respuesta ante ciberamenazas.

Uno de los logros más significativos del MICITT ha sido la creación de la Estrategia Nacional de Ciberseguridad 2018-2022, la cual estableció un marco integral para la protección del ciberespacio costarricense. Esta estrategia incluyó medidas como la implementación de auditorías de seguridad en instituciones gubernamentales, la promoción de la cultura de ciberseguridad en el sector privado y la cooperación internacional para el fortalecimiento de capacidades técnicas (MICITT, 2018). Tras el ataque de Conti en 2022, el MICITT ha trabajado en la actualización de esta estrategia para el período 2023-2027, incorporando un enfoque más robusto en la detección temprana de amenazas y la recuperación de sistemas tras incidentes cibernéticos (MICITT, 2023).

Además, el MICITT ha impulsado la creación de la Unidad Nacional de Ciberseguridad (UNCIBER), entidad encargada de la gestión de incidentes de seguridad digital y la coordinación con organismos nacionales e internacionales en la prevención de ciberataques. UNCIBER ha sido fundamental en la detección y mitigación de amenazas dirigidas a instituciones públicas, permitiendo mejorar la capacidad de respuesta del país frente a incidentes de alto impacto (Cordero, 2021).

A pesar de estos avances, Costa Rica sigue enfrentando importantes desafíos en materia de ciberseguridad, incluyendo la necesidad de incrementar el presupuesto destinado a la protección de infraestructuras críticas, fortalecer la colaboración interinstitucional y mejorar la formación de especialistas en seguridad digital. Para abordar estos retos, el MICITT continúa promoviendo la cooperación internacional y la actualización de marcos normativos que permitan consolidar la resiliencia cibernética del país en los próximos años (MICITT, 2023).

2.2 Marco Conceptual.

El marco conceptual constituye la base teórica que orienta el desarrollo de la investigación, proporcionando definiciones clave y modelos explicativos que permiten comprender el fenómeno estudiado. En el contexto de la ciberdiplomacia y la ciberseguridad, es esencial delimitar los conceptos fundamentales que sustentan el análisis, estableciendo una relación entre las teorías de las relaciones internacionales, los marcos regulatorios y las estrategias de respuesta ante amenazas digitales.

Este apartado se estructura en torno a tres ejes principales. En primer lugar, se aborda la ciberdiplomacia, explorando su evolución, dimensiones y ejemplos internacionales que ilustran su aplicación en la gestión de conflictos cibernéticos y la cooperación global en seguridad digital. Posteriormente, se examina el concepto de ciberseguridad, su relación con la seguridad nacional, la protección de infraestructuras críticas y las estrategias de mitigación y respuesta ante ciberataques. Finalmente, se analiza el Reglamento General del Sistema Nacional de Planificación, estableciendo su relevancia en la formulación de políticas de ciberseguridad en Costa Rica.

La importancia del marco conceptual radica en su capacidad para unificar distintos enfoques teóricos y normativos, permitiendo una comprensión integral de la influencia de la ciberdiplomacia en la respuesta del Estado costarricense ante ciberataques. A través de la revisión de conceptos y principios clave, este capítulo establece las bases para el análisis posterior de la investigación.

2.2.1. Ciberdiplomacia

La creciente digitalización de los Estados ha planteado nuevos desafíos en las relaciones internacionales, como la seguridad cibernética, la soberanía digital y la necesidad de cooperación global para la regulación del ciberespacio. En este contexto surge la ciberdiplomacia, un concepto que integra la diplomacia tradicional con estrategias específicas para enfrentar amenazas cibernéticas, aprovechar oportunidades tecnológicas y fortalecer la gobernanza digital a nivel internacional.

2.2.1.1 Definición general y evolución del concepto

La ciberdiplomacia puede definirse como el conjunto de estrategias y acciones diplomáticas que los Estados y organizaciones internacionales emplean para abordar cuestiones relacionadas con la ciberseguridad, la gobernanza de internet y la cooperación digital a nivel global (Nye, 2018). Se trata de un campo emergente dentro de la diplomacia que busca gestionar conflictos y promover acuerdos en el ciberespacio, facilitando la cooperación entre actores estatales y no estatales para la regulación y protección de infraestructuras digitales críticas.

El concepto de ciberdiplomacia ha evolucionado significativamente en las últimas dos décadas. Inicialmente, se enfocaba en la regulación del uso de internet y la promoción del acceso equitativo a la tecnología. Sin embargo, con el incremento de ciberataques a infraestructuras estratégicas y la proliferación de actores estatales y no estatales involucrados en operaciones cibernéticas ofensivas, el enfoque ha cambiado hacia la protección de la seguridad digital y la formulación de marcos regulatorios internacionales (Tikk & Kerttunen, 2020).

Desde la primera Cumbre Mundial sobre la Sociedad de la Información organizada por la ONU en 2003 y 2005, hasta la reciente adopción de principios de comportamiento responsable

en el ciberespacio por parte de la Asamblea General de la ONU en 2021, la ciberdiplomacia ha pasado de ser un aspecto secundario en la agenda internacional a convertirse en un eje prioritario para la seguridad global y la estabilidad de los sistemas digitales (ONU, 2021).

2.2.1.2 Dimensiones: diplomacia reactiva, preventiva y de cooperación

La ciberdiplomacia puede abordarse desde tres dimensiones clave, cada una con un enfoque específico para enfrentar los desafíos del ciberespacio:

1. Diplomacia reactiva: Se orienta a la gestión de incidentes cibernéticos una vez que han ocurrido. En este marco, los Estados pueden negociar la atribución de ataques, establecer medidas diplomáticas de represalia o sanción, y cooperar en la recuperación de sistemas afectados. Un ejemplo de ello fue la respuesta internacional al ataque de ransomware WannaCry en 2017, que impulsó esfuerzos coordinados para mitigar sus efectos y fortalecer la cooperación en ciberseguridad (NCSC, 2018).
2. Diplomacia preventiva: Se enfoca en la creación de normas y acuerdos internacionales para reducir la probabilidad de ciberataques y garantizar la estabilidad en el ciberespacio. Esto incluye la adopción de marcos legales, la firma de tratados sobre el uso responsable de las tecnologías digitales y el desarrollo de capacidades de ciberseguridad en países con menor infraestructura tecnológica. Un ejemplo representativo es el Convenio de Budapest sobre Ciberdelincuencia de 2001, que estableció estándares para la cooperación global en la lucha contra delitos informáticos (Consejo de Europa, 2020).
3. Diplomacia de cooperación: Promueve la colaboración entre países, organizaciones internacionales y el sector privado para fortalecer la gobernanza del ciberespacio y mejorar la seguridad digital. Dentro de este enfoque, se priorizan iniciativas de intercambio de información, asistencia técnica y programas de formación en ciberseguridad. Un caso destacado es el Foro Global sobre Ciber Experticia (GFCE), que facilita la cooperación entre Estados en el fortalecimiento de capacidades en ciberseguridad, especialmente en países en desarrollo (GFCE, 2021).

2.2.1.3 Ejemplos internacionales de ciberdiplomacia en acción

La ciberdiplomacia ha sido utilizada en múltiples escenarios internacionales para gestionar crisis cibernéticas y promover la cooperación global en seguridad digital. Estos casos representan ejemplos concretos de cómo los Estados y organizaciones han recurrido a mecanismos diplomáticos para abordar desafíos en el ciberespacio:

1. Acuerdo entre EE.UU. y China sobre ciberespionaje (2015): El aumento de los ataques cibernéticos entre Estados Unidos y China generó tensiones significativas, especialmente en el ámbito económico. Empresas estadounidenses acusaban a actores vinculados al gobierno chino de robar información estratégica y propiedad intelectual, lo que motivó negociaciones bilaterales. El acuerdo de 2015 estableció el compromiso de ambas naciones de no respaldar el ciberespionaje económico, lo que representó un esfuerzo sin precedentes para regular el comportamiento estatal en el ciberespacio. Aunque su implementación ha sido objeto de debate, el acuerdo sentó un precedente en la diplomacia cibernética al demostrar que es posible alcanzar entendimientos en esta materia (Segal, 2016).
2. Iniciativa de la UE sobre ciberseguridad y sanciones (2019): Ante el aumento de ciberataques dirigidos a infraestructuras críticas y procesos democráticos dentro de la Unión Europea, se estableció un marco legal para imponer sanciones a individuos, empresas y entidades responsables de estos ataques. Esta iniciativa busca disuadir futuras agresiones en el ciberespacio al establecer consecuencias concretas para los actores malintencionados. Además, refuerza la cooperación entre los Estados miembros y establece un mecanismo de respuesta unificado frente a las amenazas digitales, consolidando a la UE como un actor relevante en la gobernanza del ciberespacio (Comisión Europea, 2019).
3. Grupo de Expertos Gubernamentales de la ONU en el Ciberespacio (2021): La falta de normativas claras sobre el comportamiento estatal en el ciberespacio ha sido un desafío constante en las relaciones internacionales. En respuesta, la ONU ha promovido el diálogo entre países a través de su Grupo de Expertos Gubernamentales (GGE), cuyo objetivo es desarrollar principios para el uso responsable de las tecnologías digitales. En

2021, este grupo logró consensos clave sobre la necesidad de respetar los derechos humanos en el ciberespacio y de prevenir el uso de tecnologías digitales con fines hostiles. Estos avances han sido fundamentales para sentar las bases de un marco regulador internacional en materia de ciberseguridad (ONU, 2021).

4. Ciberdiplomacia en América Latina: El Marco de Ciberseguridad de la OEA: La creciente amenaza de ataques cibernéticos en América Latina ha impulsado la cooperación regional en materia de ciberseguridad. En este contexto, la Organización de los Estados Americanos (OEA) ha liderado esfuerzos para fortalecer las capacidades de los países miembros a través del Marco de Ciberseguridad. Esta iniciativa busca mejorar la resiliencia digital de la región mediante el intercambio de información, la capacitación de profesionales y la implementación de estándares comunes. Costa Rica ha sido un actor clave en estos esfuerzos, especialmente tras haber enfrentado ataques de alto impacto en su infraestructura digital, lo que ha reforzado su compromiso con la cooperación internacional en ciberseguridad (OEA, 2022).

Los casos expuestos demuestran que la ciberdiplomacia se ha convertido en un mecanismo fundamental para abordar los desafíos del ciberespacio a nivel global y regional. Desde acuerdos bilaterales hasta iniciativas multilaterales, los Estados han reconocido la necesidad de establecer normativas y mecanismos de cooperación para mitigar los riesgos asociados a los ciberataques y garantizar la estabilidad digital.

Asimismo, el papel de organizaciones internacionales como la ONU, la OEA y la UE ha sido clave para promover marcos regulatorios y estrategias de respuesta ante amenazas cibernéticas. Sin embargo, a pesar de estos avances, persisten desafíos como la falta de consenso sobre atribución de ataques, la rápida evolución de las tácticas cibernéticas y las brechas de capacidad entre los países.

En este contexto, la ciberdiplomacia no solo es una herramienta reactiva para gestionar crisis, sino también una estrategia preventiva para fomentar la confianza y la cooperación entre Estados. La consolidación de estos esfuerzos será determinante para el desarrollo de un ciberespacio más seguro y estable en el futuro.

2.2.2. Ciberseguridad

La creciente dependencia de la tecnología digital en todos los sectores de la sociedad ha convertido a la ciberseguridad en un pilar fundamental para la protección de la información, la infraestructura crítica y la estabilidad de los Estados. En un mundo interconectado, las amenazas cibernéticas han evolucionado, desde ataques de denegación de servicio (DDoS) hasta operaciones avanzadas de espionaje y sabotaje patrocinadas por Estados. La ciberseguridad, en este sentido, no solo es un componente técnico, sino también un asunto de seguridad nacional y gobernanza internacional.

2.2.2.1 Concepto y su relación con la seguridad nacional

La ciberseguridad se define como el conjunto de medidas, políticas y tecnologías diseñadas para proteger sistemas, redes y datos de accesos no autorizados, ataques maliciosos y otras amenazas en el ciberespacio (ISO/IEC 27032, 2012). Se trata de un enfoque multidimensional que involucra tanto a los sectores públicos como privados, con el objetivo de garantizar la integridad, disponibilidad y confidencialidad de la información.

En el contexto de la seguridad nacional, la ciberseguridad se ha convertido en un elemento esencial. Las infraestructuras estratégicas, como redes eléctricas, sistemas de transporte, telecomunicaciones y plataformas gubernamentales, dependen de sistemas digitales interconectados. Un ataque exitoso contra estos sistemas puede generar caos económico, afectar la prestación de servicios esenciales e incluso poner en riesgo la soberanía de un país. Según Nye (2017), las amenazas cibernéticas han cambiado la naturaleza de la seguridad nacional, ampliando el concepto de defensa más allá del ámbito militar y obligando a los Estados a desarrollar estrategias integrales para protegerse en el ciberespacio.

Estados Unidos, la Unión Europea y organismos como la Organización del Tratado del Atlántico Norte (OTAN) han identificado a la ciberseguridad como una prioridad estratégica. En América Latina, la Organización de los Estados Americanos (OEA) ha promovido la creación de marcos regulatorios y equipos de respuesta a incidentes para fortalecer la seguridad digital en la región (OEA, 2021).

2.2.2.2 Infraestructuras críticas y su protección

Las infraestructuras críticas son aquellos sistemas y activos físicos o virtuales cuya interrupción o destrucción tendría un impacto significativo en la seguridad, la economía o la salud pública de un país. Estas incluyen sectores como la energía, el agua, el transporte, la banca y la salud, todos ellos dependientes de sistemas digitales y, por ende, vulnerables a ciberataques (CISA, 2022).

El ataque a infraestructuras críticas es una táctica recurrente en la guerra cibernética y el ciberterrorismo. Un ejemplo paradigmático es el ataque con el malware Stuxnet en 2010, que afectó plantas nucleares en Irán y evidenció el potencial destructivo de las operaciones cibernéticas (Zetter, 2014). De manera similar, el ataque del ransomware WannaCry en 2017 paralizó hospitales y entidades gubernamentales en más de 150 países, demostrando la vulnerabilidad de sectores esenciales frente a ataques cibernéticos de gran escala (Europol, 2018).

Para proteger estas infraestructuras, los Estados han implementado diversas estrategias, entre ellas:

1. Regulación y normativas específicas: Países como Estados Unidos han desarrollado leyes como la Ley de Modernización de la Ciberseguridad de 2014, que establece requisitos de seguridad para infraestructuras críticas. Es de suma importancia contar con regulación y normativas específicas que obliguen a operadores de infraestructuras críticas a implementar medidas de seguridad adecuadas. Por ejemplo, la Ley de Modernización de la Ciberseguridad de 2014 en Estados Unidos estableció estándares obligatorios para la protección de estos sistemas, garantizando una respuesta coordinada y efectiva ante amenazas digitales.
2. Equipos de respuesta a incidentes: Muchos países han creado Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT), estos equipos son responsables de monitorear, detectar y reaccionar ante ataques en tiempo real, minimizando el impacto de las amenazas. La rápida intervención de los CSIRT ha sido clave en casos como la contención del ataque WannaCry, donde la acción coordinada de estos centros a nivel

internacional permitió mitigar la propagación del ransomware y reducir las pérdidas económicas (Europol, 2018).

3. Cooperación público-privada: dado que muchas infraestructuras críticas son operadas por empresas privadas. La falta de colaboración entre el sector gubernamental y las compañías encargadas de estos sistemas podría generar brechas de seguridad difíciles de mitigar. Modelos como el de la Unión Europea han promovido el intercambio de información y la coordinación de esfuerzos entre ambos sectores, lo que ha permitido mejorar la resiliencia frente a ciberataques (ENISA, 2021).

Costa Rica ha avanzado en la protección de sus infraestructuras críticas con la implementación del Centro de Respuesta de Seguridad Informática (CSIRT-CR), que busca coordinar acciones para la detección y mitigación de ciberataques a nivel nacional (MICITT, 2022).

2.2.2.3 Estrategias de mitigación y respuesta ante ciberataques

Los ciberataques han evolucionado en complejidad y alcance, por lo que los Estados y organizaciones deben adoptar estrategias de mitigación y respuesta para reducir su impacto. Estas estrategias pueden clasificarse en tres niveles: prevención, detección y respuesta.

1. Prevención: Consiste en medidas proactivas para evitar ataques antes de que ocurran. Incluye:
    - Implementación de marcos de seguridad basados en estándares internacionales, como la norma ISO 27001.
    - Concienciación y formación en ciberseguridad para empleados y ciudadanos.
    - Aplicación de arquitecturas de seguridad avanzadas, como el modelo de confianza cero (Zero Trust), que restringe el acceso a sistemas incluso dentro de la red interna de una organización (Forrester, 2020).
2. Detección: Se basa en el monitoreo constante de redes y sistemas para identificar anomalías que puedan indicar la presencia de amenazas. Algunas de las herramientas utilizadas son:

- Sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS).
- Análisis de inteligencia de amenazas, que permite anticipar y neutralizar ataques mediante información obtenida de incidentes previos.
- Uso de inteligencia artificial y machine learning para la identificación de patrones anómalos en el tráfico de datos (Gartner, 2021).

3. Respuesta: Incluye las acciones implementadas tras un ataque para contener sus efectos y restaurar los sistemas afectados. Algunas estrategias incluyen:
    - Planes de continuidad del negocio, que permiten garantizar la operatividad de los servicios esenciales tras un ciberataque.
    - Restauración de sistemas a partir de copias de seguridad seguras y descentralizadas.
    - Cooperación internacional, como el intercambio de información sobre amenazas en foros especializados como el Foro Global sobre Ciberexperticia (GFCE) o el Convenio de Budapest para la persecución de ciberdelincuentes.

En el caso de Costa Rica, el ataque del ransomware Conti en 2022 evidenció la importancia de estas estrategias. La paralización de los sistemas de la Caja Costarricense del Seguro Social (CCSS) y otras entidades gubernamentales obligó al gobierno a reforzar sus medidas de ciberseguridad, incluyendo la modernización del CSIRT-CR y la actualización de su Estrategia Nacional de Ciberseguridad (MICITT, 2023).

La ciberseguridad, por lo tanto, no solo es una cuestión técnica, sino también un desafío político, económico y social. La evolución de las amenazas cibernéticas exige una respuesta integral que combine regulación, cooperación internacional y el desarrollo de capacidades en ciberdefensa para garantizar la estabilidad y seguridad del entorno digital.

2.2.3. Reglamento General del Sistema Nacional de Planificación

El Reglamento General del Sistema Nacional de Planificación constituye el marco normativo fundamental que rige la planificación del desarrollo en Costa Rica. Su objetivo principal es establecer los lineamientos, procedimientos y mecanismos para la formulación,

ejecución, seguimiento y evaluación de planes, programas y proyectos dentro de la administración pública. En este contexto, la planificación es un proceso esencial para la asignación eficiente de recursos, la definición de políticas estratégicas y la consecución de los objetivos de desarrollo nacional.

Este reglamento es administrado por el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), entidad encargada de coordinar y supervisar el funcionamiento del Sistema Nacional de Planificación. Dicho sistema articula la planificación a nivel sectorial, regional y territorial, garantizando que las políticas públicas sean coherentes con los objetivos nacionales de desarrollo y con las disposiciones de organismos internacionales con los que Costa Rica mantiene compromisos estratégicos.

2.2.3.1 Principios y objetivos del Reglamento

El Reglamento General del Sistema Nacional de Planificación se fundamenta en una serie de principios que buscan garantizar la eficiencia y sostenibilidad del proceso de planificación en el país. Estos principios permiten establecer un marco coherente y funcional para la toma de decisiones estratégicas, asegurando que los procesos sean inclusivos, coordinados y transparentes. Entre ellos destacan:

1. Integralidad: La planificación debe considerar todas las dimensiones del desarrollo, incluyendo los aspectos económicos, sociales, ambientales y tecnológicos. Este enfoque holístico permite abordar los desafíos de manera estructural, asegurando que las políticas implementadas no generen impactos negativos en otras áreas del desarrollo.
2. Participación: Se promueve la inclusión de diversos actores en el proceso de planificación, desde entidades gubernamentales hasta sectores privados y la sociedad civil. La participación garantiza una mayor legitimidad en la toma de decisiones y fomenta la corresponsabilidad en la implementación de las estrategias nacionales.
3. Coordinación interinstitucional: Se busca la armonización de esfuerzos entre instituciones del Estado para evitar duplicidades y optimizar recursos. La falta de coordinación puede generar sobrecostos y desarticulación en la ejecución de políticas públicas, por lo que este principio fortalece la eficiencia del sistema de planificación.

4. Transparencia y rendición de cuentas: La planificación debe garantizar el acceso a la información pública y la evaluación constante de los resultados. Esto permite mejorar la confianza en las instituciones, así como asegurar que los planes y programas sean ejecutados de acuerdo con los objetivos establecidos.

Por otro lado, los objetivos del reglamento establecen las bases para la planificación estratégica y operativa en el país, garantizando que las acciones del Estado se alineen con las necesidades del desarrollo nacional. Entre sus objetivos principales, el reglamento establece la necesidad de:

1. Formular planes estratégicos nacionales alineados con las políticas de desarrollo sostenible y los compromisos internacionales de Costa Rica. La planificación debe responder a las metas de desarrollo sostenible establecidas en acuerdos internacionales como la Agenda 2030 de Naciones Unidas, asegurando que las estrategias nacionales contribuyan a estos objetivos globales.
2. Fomentar la descentralización de la planificación mediante la participación de gobiernos locales y regionales. La desconcentración de la toma de decisiones permite que las políticas públicas sean más eficaces al adaptarse a las necesidades específicas de cada territorio, fortaleciendo la gobernanza local y la equidad en la distribución de recursos.
3. Establecer mecanismos de monitoreo y evaluación para garantizar el cumplimiento de los planes y programas públicos. La implementación de herramientas de seguimiento y control permite detectar posibles desviaciones en la ejecución de las políticas y hacer ajustes oportunos para maximizar su impacto.
4. Modernizar la gestión pública a través de herramientas digitales y sistemas de información integrados. La transformación digital es clave para mejorar la eficiencia del sector público, optimizando procesos administrativos y facilitando la accesibilidad a los servicios para la ciudadanía.

En conjunto, estos principios y objetivos buscan fortalecer la capacidad del Estado para planificar y ejecutar políticas de manera eficiente, garantizando un desarrollo equilibrado y sostenible en Costa Rica.

2.2.3.2 Estructura y aplicación del Reglamento en la planificación nacional

El reglamento define una estructura organizativa clara para la implementación del Sistema Nacional de Planificación, la cual involucra distintos niveles de gobierno y sectores estratégicos. Dentro de esta estructura, el MIDEPLAN juega un rol central al coordinar y asesorar a las instituciones en la formulación de sus planes institucionales, sectoriales y territoriales.

A nivel operativo, el reglamento establece una jerarquía de instrumentos de planificación, que incluyen:

1. Plan Nacional de Desarrollo e Inversión Pública (PNDIP): Define las prioridades del gobierno en cada período y orienta la asignación de recursos.
2. Planes estratégicos sectoriales: Aplicados en áreas clave como educación, salud, infraestructura y seguridad.
3. Planes operativos institucionales (POI): Desarrollados por cada entidad del sector público para traducir los lineamientos estratégicos en acciones concretas.

Estos instrumentos de planificación garantizan la alineación de las políticas públicas con las necesidades del país y facilitan la implementación de proyectos de alto impacto.

2.2.3.3 Vinculación del Reglamento con la ciberseguridad y la ciberdiplomacia

En el contexto de la ciberseguridad y la ciberdiplomacia, el Reglamento General del Sistema Nacional de Planificación adquiere una relevancia particular, ya que permite integrar la seguridad digital en la planificación del Estado. La creciente digitalización de los servicios públicos y la vulnerabilidad ante amenazas cibernéticas han llevado a que el reglamento contemple la ciberseguridad como un eje transversal en la formulación de planes nacionales.

En este sentido, el reglamento establece la necesidad de fortalecer la gobernanza digital mediante estrategias como:

1. La incorporación de la ciberseguridad en los planes de modernización del sector público.

2. La asignación de recursos específicos para la protección de infraestructuras críticas y sistemas de información gubernamentales.
3. La cooperación internacional para el fortalecimiento de capacidades en ciberseguridad y respuesta ante incidentes.
4. La articulación de políticas entre el MICITT, el MIDEPLAN y otras entidades responsables de la transformación digital del país.

Un ejemplo concreto de la aplicación de estos lineamientos es la inclusión de la Estrategia Nacional de Ciberseguridad 2018-2022 dentro del Plan Nacional de Desarrollo, lo que permitió establecer prioridades en la protección del ciberespacio costarricense y promover la cooperación con organismos internacionales como la OEA y el BID.

2.2.3.4 Retos y desafíos en la implementación del Reglamento

A pesar de los avances en la planificación nacional, la aplicación efectiva del reglamento enfrenta diversos desafíos. Entre los principales se encuentran:

1. Limitaciones presupuestarias: La ejecución de planes estratégicos depende en gran medida de la disponibilidad de recursos financieros, lo que en algunos casos ha retrasado proyectos clave.
2. Burocracia y falta de articulación interinstitucional: A pesar de los esfuerzos por mejorar la coordinación entre entidades, todavía existen barreras administrativas que dificultan la implementación de políticas transversales.
3. Adaptación a nuevas amenazas digitales: La rápida evolución de las amenazas cibernéticas exige que la planificación estatal sea flexible y se actualice constantemente para responder a los desafíos emergentes.

Por tanto, el Reglamento General del Sistema Nacional de Planificación es una herramienta esencial para la formulación y ejecución de políticas públicas en Costa Rica. Su aplicación en el ámbito de la ciberseguridad y la ciberdiplomacia permite garantizar que el país cuente con estrategias claras para enfrentar las amenazas digitales y fortalecer su capacidad de respuesta ante incidentes cibernéticos. Sin embargo, su implementación efectiva requiere superar

desafíos estructurales y promover una mayor coordinación entre las entidades responsables de la seguridad digital en el país.

2.2.4. Infraestructuras Críticas en el Contexto Costarricense.

Las infraestructuras críticas son aquellas instalaciones, sistemas y servicios esenciales para el funcionamiento de un país, cuya interrupción o afectación podría generar graves consecuencias en la seguridad, economía y bienestar social. Según la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE), dentro de las infraestructuras críticas de Costa Rica se incluyen sectores como el energético, el financiero, las telecomunicaciones y la salud, siendo este último de especial relevancia debido a su impacto directo en la población (CNE, 2022).

2.2.4.1 La Caja Costarricense de Seguro Social (CCSS) como infraestructura crítica

En el contexto costarricense, la Caja Costarricense de Seguro Social (CCSS) es la institución más importante del sistema de salud, encargada de la administración de hospitales, clínicas y centros de atención primaria en todo el país. Su papel como infraestructura crítica radica en su responsabilidad de garantizar el acceso a servicios médicos, gestionar bases de datos con información de millones de ciudadanos y coordinar respuestas ante emergencias sanitarias (OPS, 2023).

Debido a su dependencia de sistemas digitales para la gestión de expedientes médicos, programación de citas, facturación y administración de recursos, la Caja Costarricense de Seguro Social (CCSS) se ha convertido en un objetivo vulnerable a los ciberataques. En mayo de 2022, la institución sufrió uno de los incidentes de seguridad más graves en la historia del país cuando el grupo de ransomware Conti ejecutó un ataque que paralizó múltiples servicios hospitalarios y comprometió información confidencial de pacientes y empleados (MICITT, 2022).

El ciberataque perpetrado contra la Caja Costarricense de Seguro Social (CCSS) puso de manifiesto importantes debilidades en la infraestructura tecnológica de una de las instituciones más relevantes del sistema de salud nacional. Este incidente reveló las limitaciones de las estrategias existentes de ciberseguridad dentro del sector salud, así como la urgencia de

implementar mecanismos más robustos y actualizados. Ante la magnitud de los daños causados, el gobierno costarricense optó por declarar un estado de emergencia nacional, una medida que facilitó la asignación extraordinaria de recursos destinados tanto a la recuperación de los sistemas comprometidos como al diseño de acciones preventivas para mitigar el riesgo de nuevos ciberataques (Gobierno de Costa Rica, 2022).

2.2.4.2 Riesgos cibernéticos que enfrentan los servicios de salud

Los servicios de salud en Costa Rica enfrentan diversos riesgos cibernéticos que pueden comprometer tanto la operatividad de los sistemas hospitalarios como la privacidad de los pacientes. Algunos de los principales riesgos incluyen:

1. Ransomware y bloqueo de sistemas: Como se evidenció en el ataque del grupo Conti, el uso de malware para cifrar archivos y exigir pagos como rescate representa una de las amenazas más críticas para las instituciones de salud (Europol, 2022). Este tipo de ataques puede dejar hospitales inoperativos, retrasando cirugías y tratamientos esenciales.
2. Robo y filtración de datos sensibles: La Caja Costarricense de Seguro Social (CCSS) almacena información altamente confidencial sobre diagnósticos, tratamientos y datos personales de los ciudadanos. Un ataque dirigido a sus bases de datos puede derivar en filtraciones que expongan a la población a riesgos como el robo de identidad o la venta de información en la darknet (ENISA, 2021).
3. Ataques de denegación de servicio (DDoS): Estos ataques buscan saturar los servidores de las instituciones de salud, impidiendo el acceso a plataformas digitales esenciales, como los sistemas de gestión hospitalaria y expedientes electrónicos (CISA, 2022).
4. Manipulación de dispositivos médicos conectados: Con el avance de la digitalización, muchos dispositivos médicos, como marcapasos y bombas de insulina, están conectados a redes hospitalarias. Un ataque cibernético dirigido a estos dispositivos podría poner en riesgo la vida de los pacientes (WHO, 2022).

Para mitigar estos riesgos, se han implementado estrategias como la creación del Centro de Respuesta de Seguridad Informática de Costa Rica (CSIRT-CR), encargado de monitorear amenazas y coordinar acciones de ciberseguridad en el país (MICITT, 2022). Asimismo, la Caja

Costarricense de Seguro Social (CCSS) ha adoptado protocolos de seguridad más estrictos, incluyendo el refuerzo en la autenticación de accesos y la segmentación de redes internas para reducir la propagación de malware en caso de incidentes (CCSS, 2023).

En este contexto, la ciberdiplomacia también juega un papel clave en la protección de infraestructuras críticas, facilitando la cooperación internacional para el intercambio de información sobre amenazas emergentes y mejores prácticas en ciberseguridad. La adhesión de Costa Rica a iniciativas como el Marco de Ciberseguridad de la OEA y la colaboración con organismos como el Centro de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) refuerzan las capacidades nacionales para enfrentar los desafíos digitales en el sector salud (OEA, 2022).

2.3 Marco Referencial

El marco referencial de esta investigación proporciona el sustento teórico necesario para analizar la influencia de la ciberdiplomacia en la respuesta del Estado costarricense ante ciberataques. A través de la revisión de teorías de las relaciones internacionales y conceptos geopolíticos, se busca comprender cómo los Estados utilizan la ciberseguridad como una herramienta de poder, cómo se construyen normas en el ciberespacio y de qué manera se institucionaliza la cooperación internacional en materia de ciberseguridad.

Para ello, este apartado se estructura en tres secciones principales. En primer lugar, se aborda el realismo como una perspectiva teórica para entender la ciberseguridad dentro del sistema internacional anárquico, analizando cómo los Estados utilizan los ciberataques como herramientas de desestabilización y dominio geopolítico. Luego, desde una perspectiva constructivista, se examina la construcción de normas en el ciberespacio, destacando el papel de la cooperación internacional y la institucionalización de la ciberdiplomacia a través de organismos multilaterales como la ONU y la OEA. Finalmente, se estudia la geopolítica del ciberespacio, explorando la competencia por el dominio digital entre potencias como Estados Unidos, China y Rusia, así como sus implicaciones para países en desarrollo como Costa Rica.

Este marco referencial no solo permite establecer un marco analítico sólido para la investigación, sino que también contextualiza la importancia de la ciberdiplomacia como un mecanismo clave para la seguridad nacional y la estabilidad global en un entorno digital cada vez más interconectado y vulnerable a amenazas cibernéticas.

2.3.1. El Realismo y la Ciberseguridad como herramienta de poder

La ciberseguridad se ha convertido en un componente central de la seguridad nacional de los Estados en un contexto internacional marcado por la anarquía, donde la acumulación de poder y la protección de la soberanía son primordiales. Desde la perspectiva del realismo en las relaciones internacionales, los Estados priorizan la seguridad y el fortalecimiento de sus capacidades tecnológicas como medios de defensa y disuasión ante amenazas externas (Morgenthau, 1948). La proliferación de ciberataques y su impacto en la estabilidad global han convertido al ciberespacio en un nuevo campo de competencia geopolítica, en el cual los Estados emplean estrategias tanto ofensivas como defensivas para consolidar su hegemonía y contrarrestar la influencia de actores rivales (Waltz, 1979).

Dado que el realismo considera que los Estados son los principales actores del sistema internacional, la ciberseguridad se percibe como una extensión del poder estatal. En este sentido, el desarrollo de capacidades ofensivas en el ciberespacio no solo responde a la necesidad de defensa, sino también a la posibilidad de proyectar influencia y establecer un balance de poder favorable (Singer & Friedman, 2014). Así, el uso de ciberataques con fines estratégicos se ha convertido en una herramienta recurrente dentro de la competencia internacional, permitiendo la obtención de información, la interrupción de infraestructuras críticas y la desestabilización de adversarios sin necesidad de confrontaciones convencionales.

2.3.1.1 La seguridad en el sistema anárquico: el Estado como actor central.

El realismo enfatiza que el sistema internacional es anárquico, es decir, carece de una autoridad central que regule las relaciones entre Estados. En este contexto, la seguridad se convierte en la máxima prioridad y los Estados buscan maximizar su poder para evitar amenazas externas (Waltz, 1979). Esta lógica ha llevado a los Estados a adoptar estrategias defensivas y

ofensivas en distintos ámbitos, incluyendo el ciberespacio, donde las amenazas pueden provenir tanto de otros Estados como de actores no estatales, o grupos criminales y hacktivistas (Singer & Friedman, 2014). La falta de regulación global en el ciberespacio ha permitido que los Estados desarrollen capacidades cibernéticas con fines tanto de protección como de ataque, generando una carrera armamentista digital similar a la observada en la guerra convencional durante el siglo XX (Kello, 2017).

Tradicionalmente, la seguridad ha estado vinculada a capacidades militares convencionales, pero en la era digital, la ciberseguridad ha adquirido un rol crucial dentro de la estrategia de defensa estatal. La digitalización de infraestructuras críticas, como el sector energético, las telecomunicaciones y la banca, ha hecho que la protección del ciberespacio sea una prioridad para la seguridad nacional. De acuerdo con Nye (2011), los ciberataques pueden debilitar significativamente la estabilidad política y económica de un país, afectando su capacidad para proyectar poder en el ámbito internacional. Esta vulnerabilidad ha llevado a los Estados a reforzar sus estrategias de ciberseguridad mediante el desarrollo de marcos regulatorios, sistemas de monitoreo avanzados y la cooperación internacional en defensa digital.

El fortalecimiento de las capacidades cibernéticas se ha convertido en un componente esencial de la política de seguridad nacional. En este sentido, los Estados han desarrollado agencias especializadas en ciberseguridad y han establecido marcos regulatorios estrictos para proteger sus infraestructuras digitales. Ejemplos de ello incluyen la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) en Estados Unidos, el Centro Nacional de Ciberseguridad en el Reino Unido y la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Estas instituciones tienen como objetivo mejorar la resiliencia digital, coordinar respuestas ante incidentes cibernéticos y fomentar la cooperación entre sectores público y privado (NATO, 2021).

Un ejemplo clave de la cooperación internacional en ciberdefensa es la Organización del Tratado del Atlántico Norte (OTAN), que ha priorizado la resiliencia digital como un elemento fundamental de la seguridad colectiva. En 2016, la OTAN declaró el ciberespacio como un dominio operativo de guerra, lo que significa que un ataque cibernético contra un Estado

miembro podría activar la cláusula de defensa colectiva del Artículo 5 del tratado, el cual establece que:

> "Las Partes acuerdan que un ataque armado contra una o más de ellas en Europa o América del Norte se considerará un ataque contra todas ellas y, en consecuencia, acuerdan que, si tal ataque ocurre, cada una de ellas [...] asistirá a la Parte o Partes atacadas [...] tomando individualmente y de acuerdo con las demás Partes, las medidas que juzgue necesarias, incluido el uso de la fuerza armada" (OTAN, 1949, Art. 5).

Además, la OTAN ha establecido el Centro de Excelencia Cooperativa de Ciberdefensa en Estonia, donde se desarrollan estrategias para mejorar la seguridad digital de sus aliados y fortalecer la respuesta a posibles ciberataques.

La anarquía del sistema internacional y la ausencia de un marco regulador global han llevado a los Estados a reforzar sus posturas en materia de ciberseguridad. En este contexto, la ciberdefensa se ha convertido en un componente esencial de la política de seguridad nacional, no solo orientada a la protección de infraestructuras críticas, sino también al resguardo de la estabilidad política y económica en un mundo cada vez más interconectado. A medida que la competencia en el ciberespacio se intensifica, es previsible que los Estados continúen invirtiendo en el desarrollo de capacidades cibernéticas tanto defensivas como ofensivas, lo que contribuye a consolidar el ciberespacio como un nuevo campo de disputa dentro de la geopolítica contemporánea.

2.3.1.2 Los ciberataques como estrategia de desestabilización y dominio geopolítico.

El uso de ciberataques como estrategia de desestabilización ha demostrado ser altamente efectivo en el escenario internacional. Desde la perspectiva realista, los Estados recurren a estas tácticas para afectar la economía, infraestructura y estabilidad política de sus rivales sin recurrir a confrontaciones directas. Estos ataques permiten a los Estados proyectar poder de manera encubierta, evitando la atribución inmediata y las represalias directas, lo que los convierte en herramientas estratégicas dentro del panorama geopolítico contemporáneo (Lindsay, 2015).

Un ejemplo claro es la presunta interferencia rusa en las elecciones presidenciales de EE.UU. en 2016, donde se emplearon ciberataques para manipular la opinión pública y debilitar la confianza en las instituciones democráticas (Rid, 2020). A través de campañas de desinformación, robo de datos y ataques a la infraestructura electoral, actores vinculados al gobierno ruso intentaron influir en el proceso democrático estadounidense. Este caso refleja cómo el ciberespacio se ha convertido en un nuevo frente de la competencia entre potencias, en el que la guerra de la información y la manipulación de narrativas desempeñan un papel clave (Buchanan, 2020).

Asimismo, el ataque a la red eléctrica de Ucrania en 2015 mostró cómo un ciberataque puede paralizar sectores estratégicos y enviar un mensaje geopolítico de advertencia a otras naciones (Zetter, 2014). Este ataque, atribuido al grupo Sandworm, dejó sin electricidad a más de 200,000 personas y evidenció la vulnerabilidad de las infraestructuras críticas ante amenazas cibernéticas. La capacidad de los Estados para llevar a cabo ataques de este tipo refuerza la idea de que la guerra moderna no se libra únicamente con armas convencionales, sino también a través de la disrupción digital y el sabotaje de servicios esenciales.

A lo largo de la última década, los ciberataques han pasado de ser amenazas aisladas a convertirse en herramientas clave en la guerra híbrida, donde los conflictos no se libran únicamente en el campo de batalla, sino también en el ámbito digital. La guerra híbrida combina tácticas convencionales con operaciones cibernéticas, desinformación y presión económica para debilitar a un adversario sin desencadenar una confrontación militar abierta (Kello, 2017).

Estados como China, Rusia y Estados Unidos han desarrollado capacidades cibernéticas avanzadas con fines de inteligencia, sabotaje y desinformación, incrementando la complejidad de las dinámicas geopolíticas. China, por ejemplo, ha sido señalada por su uso de ciberespionaje para obtener información estratégica de gobiernos y empresas en Occidente. El caso del hackeo a la Oficina de Administración de Personal de EE.UU. en 2015, atribuido a actores chinos, expuso los datos personales de más de 22 millones de empleados gubernamentales, subrayando la importancia de la ciberseguridad en la protección de la soberanía estatal (Sanger, 2018).

El uso estratégico de los ciberataques por parte de los Estados refleja la evolución de la seguridad internacional en la era digital. A medida que las naciones dependen cada vez más de las tecnologías de la información, la capacidad para defenderse y atacar en el ciberespacio se ha convertido en un elemento esencial de la política de poder global. En este contexto, el realismo sigue siendo una teoría clave para comprender la dinámica de competencia y conflicto en el ámbito de la ciberseguridad.

2.3.1.3 Ejemplos de ciberataques en el contexto del realismo: Stuxnet y la guerra cibernética.

Uno de los ejemplos más emblemáticos de guerra cibernética bajo la óptica del realismo es el caso del malware Stuxnet, descubierto en 2010. Este ciberataque, atribuido a EE.UU. e Israel, tenía como objetivo sabotear el programa nuclear iraní mediante la alteración de las centrifugadoras utilizadas para el enriquecimiento de uranio (Singer & Friedman, 2014). La sofisticación de Stuxnet demostró la capacidad de los Estados para emplear herramientas cibernéticas con fines estratégicos, sin necesidad de una intervención militar convencional. Stuxnet fue diseñado con una precisión quirúrgica, logrando infiltrarse en los sistemas de control industrial de la planta de Natanz sin ser detectado durante meses, lo que evidenció la capacidad de los Estados para ejecutar ataques prolongados y altamente especializados (Langner, 2011).

Este ataque también puso de manifiesto la creciente militarización del ciberespacio y el uso de ciberarmas como un medio para alcanzar objetivos políticos y geopolíticos. Stuxnet no solo ralentizó el desarrollo del programa nuclear iraní, sino que también envió un mensaje claro sobre la vulnerabilidad de las infraestructuras estratégicas ante la guerra cibernética. Este incidente marcó un punto de inflexión en la seguridad internacional, ya que demostró cómo una operación cibernética podía sustituir una intervención militar convencional, redefiniendo las estrategias de defensa y ataque en el ámbito global (Zetter, 2014).

El caso de Stuxnet evidencia cómo la ciberseguridad se ha convertido en un campo de batalla donde los Estados buscan mantener su hegemonía y prevenir el desarrollo de capacidades hostiles en naciones rivales. Posteriormente, otros ataques como el NotPetya en 2017, atribuido a Rusia, demostraron cómo el uso de malware puede generar consecuencias devastadoras a nivel

económico y político. NotPetya, inicialmente disfrazado como un ransomware, se propagó rápidamente a través de sistemas interconectados, causando interrupciones en infraestructuras críticas y pérdidas económicas estimadas en más de 10 mil millones de dólares a nivel mundial (Greenberg, 2019).

En el ámbito de la guerra cibernética, NotPetya es considerado uno de los ciberataques más destructivos registrados, ya que paralizó bancos, aerolíneas, empresas multinacionales y redes gubernamentales en Ucrania, con impactos colaterales en diversas partes del mundo. Su rápida expansión evidenció la interconectividad global y la vulnerabilidad de los sistemas informáticos ante ataques diseñados para causar caos a gran escala (Buchanan, 2020).

Otro caso relevante es el ataque a Sony Pictures en 2014, atribuido a Corea del Norte, en represalia por la producción de una película satírica sobre su líder, Kim Jong-un. Este ataque no solo resultó en la filtración de información confidencial y la paralización temporal de la compañía, sino que también representó un intento de censura internacional a través del uso del ciberespionaje y el sabotaje digital. Este evento demostró cómo los ciberataques pueden ser utilizados no solo como herramientas militares, sino también como instrumentos de presión política y propaganda (Healey, 2016).

En este contexto, el realismo explica cómo la competencia por la seguridad y el poder sigue siendo un factor determinante en la formulación de estrategias cibernéticas a nivel global. La capacidad de los Estados para llevar a cabo ataques cibernéticos sofisticados y su disposición a utilizarlos como herramientas de coerción, sabotaje y represalia refuerzan la idea de que el ciberespacio se ha convertido en un nuevo campo de batalla en la lucha por la hegemonía internacional. La constante evolución de las amenazas cibernéticas y la creciente dependencia de las infraestructuras digitales sugieren que la guerra cibernética continuará desempeñando un papel clave en la geopolítica del siglo XXI.

2.3.2. El Constructivismo y la Construcción de Normas en el Ciberespacio

El constructivismo en las relaciones internacionales enfatiza el papel de las ideas, normas e identidad en la configuración del comportamiento de los Estados y otros actores del sistema

internacional (Wendt, 1999). En el contexto de la ciberseguridad, esta perspectiva permite analizar cómo se crean, consolidan y transforman las normas que rigen el ciberespacio.

A diferencia del realismo, que ve la seguridad como un juego de poder entre actores estatales, o del liberalismo, que se centra en la cooperación y las instituciones, el constructivismo sostiene que la seguridad digital y las respuestas a las amenazas cibernéticas son socialmente construidas y dependen del consenso internacional sobre lo que constituye una amenaza y cómo debe abordarse (Finnemore & Sikkink, 1998).

A medida que el ciberespacio se ha convertido en un escenario fundamental para la economía, la seguridad nacional y la política internacional, la construcción de normas ha cobrado una importancia estratégica sin precedentes (Dunn Cavelty, 2012).

2.3.2.1 El papel de las ideas y normas en la seguridad digital.

Las ideas y normas desempeñan un papel fundamental en la seguridad digital, ya que determinan cómo los Estados y otros actores perciben las amenazas cibernéticas y cómo reaccionan ante ellas (Tikk, Kerttunen & Vihul, 2014). Finnemore y Sikkink (1998) proponen un modelo de construcción de normas que se aplica a la ciberseguridad:

1. Emergencia de normas: Se genera un consenso inicial sobre la importancia de un tema, promovido por expertos y organizaciones.
2. Cascada de normas: A medida que más actores adoptan la norma, esta gana legitimidad y se convierte en un estándar de comportamiento esperado.
3. Internalización de normas: La norma se consolida en leyes y políticas nacionales, volviéndose parte del marco institucional de los Estados.

En el ciberespacio, este proceso se refleja en la creación de principios de comportamiento responsable, como el respeto a la soberanía digital, la protección de infraestructuras críticas y la prohibición de ciberataques contra servicios esenciales (Schmitt, 2017).

Sin embargo, las normas en seguridad digital no son estáticas, sino que evolucionan conforme cambia la percepción de las amenazas y las capacidades tecnológicas (Adler, 2013).

Un ejemplo de esta evolución es la creciente aceptación de la atribución de ciberataques a actores estatales, algo que hace una década era impensable debido a la dificultad de rastrear con precisión la autoría de los ataques (Nye, 2017).

Desde una perspectiva constructivista, la seguridad cibernética no es simplemente una cuestión técnica, sino una construcción social. Las percepciones sobre qué constituye un ciberataque grave y qué tipo de respuesta es legítima dependen del discurso internacional y de la interpretación de los Estados (Dunn Cavelty, 2012).

Por ejemplo, algunos países consideran los ataques a sus sistemas de salud o financieros como actos de guerra cibernética, mientras que otros los clasifican como delitos comunes o acciones de espionaje (Tikk et al., 2014). Esta diferencia de enfoques ha impedido la creación de un consenso global sobre la definición de ciberterrorismo o ciberguerra (Schmitt, 2017).

2.3.2.2 La cooperación internacional en ciberseguridad: acuerdos y tratados.

A medida que el ciberespacio se ha convertido en un área clave para la seguridad global, los Estados han buscado cooperación internacional para enfrentar amenazas cibernéticas comunes. Sin embargo, la falta de consenso sobre definiciones y principios básicos ha dificultado la adopción de tratados vinculantes en ciberseguridad (Nye, 2017).

Algunos acuerdos y tratados internacionales relevantes en materia de ciberseguridad incluyen:

1. Convenio de Budapest sobre Ciberdelincuencia (2001): Se trata del primer tratado internacional sobre delitos informáticos, cuyo objetivo es armonizar las legislaciones nacionales para mejorar la cooperación judicial y policial en la lucha contra el cibercrimen (Council of Europe, 2001). Su importancia radica en que establece definiciones legales estandarizadas para crímenes cibernéticos, como el acceso ilícito a sistemas, la falsificación informática y el fraude digital. Este convenio ha servido como referencia para numerosos países, incluidos varios de América Latina, a pesar de que Costa Rica no es firmante. Su inclusión en este análisis responde a su papel en la creación de una normativa internacional común, promoviendo la cooperación entre Estados en materia de persecución de delitos informáticos.

2. Resoluciones de la ONU sobre Ciberseguridad: Desde 2004, la Asamblea General de la ONU ha aprobado múltiples resoluciones dirigidas a fortalecer la cooperación internacional en ciberseguridad, enfocándose en la prevención del uso del ciberespacio con fines criminales, terroristas o bélicos (ONU, 2015). Estas resoluciones reflejan el papel de las normas y la construcción de consensos internacionales, elementos clave dentro del constructivismo. Aunque no son vinculantes, establecen principios de comportamiento responsable que guían las políticas nacionales e internacionales en ciberseguridad. Su inclusión en este análisis es fundamental para entender cómo los Estados han intentado regular el ciberespacio sin afectar la soberanía digital, promoviendo una gobernanza más estructurada.
3. Marco de Normas de la ONU sobre el Comportamiento Estatal en el Ciberespacio (2015): Este marco representa uno de los intentos más avanzados para establecer principios de comportamiento en el ciberespacio, especialmente en relación con la protección de infraestructuras críticas y la limitación del uso ofensivo de herramientas cibernéticas (Schmitt, 2017). La importancia de este documento radica en que reconoce la necesidad de evitar ciberataques a sectores esenciales como salud, energía y telecomunicaciones, estableciendo un punto de referencia para la diplomacia cibernética. Se menciona en este análisis debido a su influencia en la formulación de políticas nacionales de ciberseguridad y su relación con el concepto constructivista de internalización de normas.
4. Acuerdos bilaterales y regionales: Los acuerdos bilaterales y regionales, como los firmados entre Estados Unidos y China, buscan limitar la ciberguerra y el espionaje digital, reflejando una evolución en la forma en que los Estados abordan la ciberseguridad a nivel diplomático (Nye, 2017). Estos acuerdos son fundamentales porque demuestran cómo la cooperación en ciberseguridad no solo se da en foros multilaterales, sino también en negociaciones directas entre Estados. Su inclusión responde a la necesidad de entender cómo las normas en ciberseguridad se consolidan tanto en ámbitos globales como en acuerdos específicos entre potencias tecnológicas.

Si bien estos acuerdos han sentado bases importantes, aún no existe un tratado global sobre ciberseguridad, en parte debido a la desconfianza entre Estados y la dificultad de aplicar mecanismos de verificación efectivos (Tikk et al., 2014).

2.3.2.3 Institucionalización de la ciberdiplomacia: la ONU, la OEA y otras iniciativas multilaterales.

La creciente interdependencia digital entre los Estados y la proliferación de amenazas cibernéticas han llevado a la necesidad de fortalecer la ciberdiplomacia como un mecanismo fundamental en la gobernanza del ciberespacio. La institucionalización de la ciberdiplomacia a nivel internacional ha sido impulsada por organismos multilaterales como la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA) y diversas iniciativas regionales que buscan establecer normas comunes, fomentar la cooperación y reducir los riesgos asociados a conflictos en el ámbito cibernético (Tikk & Kerttunen, 2020).

A diferencia de otros ámbitos de la diplomacia tradicional, la ciberdiplomacia requiere la participación no solo de los Estados, sino también de organizaciones internacionales, empresas tecnológicas y la sociedad civil, ya que las amenazas cibernéticas no reconocen fronteras y pueden afectar infraestructuras críticas en distintos países simultáneamente (Maurer, 2018). En este sentido, las instituciones multilaterales han desempeñado un papel clave en la creación de marcos normativos, la facilitación de diálogos internacionales y la promoción de buenas prácticas en ciberseguridad.

La ONU ha sido una de las principales plataformas para la discusión de normativas sobre ciberseguridad y la promoción de la cooperación internacional en el ciberespacio. En 2004, la Asamblea General de la ONU estableció el Grupo de Expertos Gubernamentales sobre Ciberseguridad (GGE, por sus siglas en inglés) con el objetivo de analizar las amenazas cibernéticas y formular principios para la seguridad internacional en el ciberespacio (ONU, 2015). Este grupo ha sido fundamental en la creación de normas de comportamiento responsable de los Estados, incluyendo el principio de no atacar infraestructuras críticas y la necesidad de fortalecer la cooperación internacional en la lucha contra el cibercrimen (Schmitt, 2017).

Además, la ONU ha promovido la inclusión de la ciberseguridad en su agenda de paz y seguridad internacional, dado que los ciberataques pueden constituir amenazas a la estabilidad global. En 2021, el Comité de las Naciones Unidas sobre Uso Pacífico del Ciberespacio propuso un nuevo marco de gobernanza digital, destacando la necesidad de normas vinculantes y mecanismos de verificación para reducir el riesgo de conflictos en el ámbito cibernético (ONU, 2021).

Asimismo, la ONU ha trabajado en la promoción de tratados internacionales que regulen el uso del ciberespacio con fines militares. Si bien aún no existe un convenio global específico, el Derecho Internacional Humanitario (DIH) se ha comenzado a aplicar a los conflictos cibernéticos, estableciendo limitaciones en el uso de ataques cibernéticos en escenarios bélicos (Tikk & Kerttunen, 2020).

En el contexto regional, la Organización de los Estados Americanos (OEA) ha desempeñado un papel central en el desarrollo de la ciberdiplomacia en América Latina y el Caribe. A través del Comité Interamericano contra el Terrorismo (CICTE) y su Programa de Seguridad Cibernética, la OEA ha promovido iniciativas de cooperación entre sus Estados miembros para fortalecer la protección de infraestructuras críticas, compartir información sobre amenazas y fomentar la capacitación en ciberseguridad (OEA, 2019).

Uno de los principales logros de la OEA ha sido la adopción de la Estrategia de Ciberseguridad de las Américas, que proporciona lineamientos para el desarrollo de políticas nacionales de ciberseguridad, mecanismos de respuesta a incidentes y estrategias de concientización sobre los riesgos digitales (OEA, 2018). Esta estrategia ha sido clave para que países como Costa Rica fortalezcan sus capacidades en el ámbito de la ciberseguridad, especialmente tras el ataque de 2022 a la Caja Costarricense del Seguro Social (CCSS).

Además, la OEA ha impulsado la creación de equipos nacionales de respuesta a incidentes de seguridad informática (CSIRTs), los cuales facilitan la coordinación entre países frente a amenazas transnacionales. Estos equipos han permitido mejorar la capacidad de respuesta ante ataques cibernéticos y fomentar el intercambio de información técnica y operativa entre Estados miembros (OEA, 2020).

Además de la ONU y la OEA, existen otras iniciativas multilaterales que han contribuido a la institucionalización de la ciberdiplomacia a nivel global. Algunas de las más relevantes incluyen:

1. **Foro Global sobre Ciberexperiencia (Global Forum on Cyber Expertise - GFCE)**:

El Foro Global sobre Ciberexperiencia (GFCE) es una iniciativa que busca fortalecer las capacidades globales en materia de ciberseguridad a través del intercambio de conocimientos y experiencias entre distintos actores. A diferencia de otros foros centrados en la regulación y las estrategias gubernamentales, el GFCE adopta un enfoque basado en la cooperación multisectorial, reuniendo a gobiernos, el sector privado, organizaciones internacionales y la sociedad civil para compartir buenas prácticas y promover la capacitación en seguridad digital (GFCE, 2020).

La importancia del GFCE radica en su papel como un puente entre países desarrollados y en desarrollo en términos de ciberseguridad. Muchas naciones carecen de la infraestructura y el conocimiento técnico necesario para responder eficazmente a amenazas cibernéticas, por lo que el foro facilita la transferencia de conocimientos y el desarrollo de capacidades en regiones vulnerables (GFCE, 2021). Además, esta plataforma fomenta la creación de redes de cooperación internacional y la asistencia técnica en la implementación de marcos de seguridad cibernética, lo que contribuye a un ecosistema digital más seguro y resiliente a nivel global.

2. **Grupo de los 20 (G20) y la Ciberseguridad en la Economía Global:**

El Grupo de los 20 (G20) ha incorporado la ciberseguridad en su agenda debido al impacto que los ataques cibernéticos pueden tener en la economía global y en la estabilidad de los mercados financieros. Desde 2017, el G20 ha reconocido que la seguridad digital es un pilar esencial para la resiliencia económica y ha instado a sus miembros a fortalecer la cooperación en este ámbito (G20, 2018).

Uno de los principales enfoques del G20 en materia de ciberseguridad es la protección de infraestructuras críticas y la seguridad del sector financiero. En un mundo cada vez más interconectado, los ataques cibernéticos dirigidos a bancos, bolsas de valores y sistemas de pago

pueden generar efectos dominó con consecuencias catastróficas para la economía global (FSB, 2020). Por ello, el G20 ha promovido iniciativas como:

1. El establecimiento de estándares de ciberseguridad para el sector financiero, con la participación de organismos como el Fondo Monetario Internacional (FMI) y el Consejo de Estabilidad Financiera (FSB).
2. La promoción de cooperación internacional en la gestión de crisis cibernéticas para minimizar el impacto de ciberataques en los mercados globales.
3. El desarrollo de estrategias conjuntas para mitigar el cibercrimen financiero, especialmente en el contexto del crecimiento de las criptomonedas y la digitalización de los servicios financieros (G20, 2021).

El rol del G20 en ciberdiplomacia se justifica en su capacidad de generar consensos entre las principales economías del mundo, estableciendo compromisos que pueden traducirse en políticas nacionales y acuerdos multilaterales que fortalezcan la ciberseguridad global.

3. OTAN y la Ciberdefensa: Un Nuevo Escenario en la Seguridad Internacional:

La Organización del Tratado del Atlántico Norte (OTAN) ha sido un actor clave en la institucionalización de la ciberdefensa dentro del ámbito de la seguridad internacional. Aunque tradicionalmente se ha enfocado en amenazas militares convencionales, la OTAN ha reconocido que los ataques cibernéticos pueden representar un riesgo estratégico para la seguridad de sus Estados miembros y, desde 2014, ha declarado que los ciberataques pueden activar el Artículo 5 del Tratado del Atlántico Norte, el cual establece que un ataque contra un miembro de la alianza es considerado un ataque contra todos (NATO, 2019).

Uno de los hitos más importantes en la estrategia de ciberdefensa de la OTAN fue la creación del Centro de Excelencia en Ciberdefensa Cooperativa (CCDCOE) en Estonia, en 2008. Este centro se ha convertido en un referente global en la investigación y desarrollo de estrategias de defensa cibernética, proporcionando entrenamiento y ejercicios como Locked Shields, el cual es considerado el simulacro de guerra cibernética más grande del mundo (NATO CCDCOE, 2020).

La OTAN también ha promovido la cooperación en materia de ciberseguridad entre sus miembros a través de iniciativas como:

1. El Plan de Acción en Ciberdefensa de la OTAN, que establece directrices para la mejora de la resiliencia cibernética de los países miembros.
2. La colaboración con la Unión Europea (UE) en estrategias de ciberdefensa compartida, dado que ambas organizaciones enfrentan amenazas comunes en el ciberespacio.
3. La incorporación de la ciberseguridad en sus doctrinas militares, estableciendo el ciberespacio como un dominio operativo, al mismo nivel que la tierra, el mar y el aire (NATO, 2019).

El papel de la OTAN en la ciberdiplomacia es crucial porque demuestra cómo la seguridad cibernética ha trascendido el ámbito puramente técnico para convertirse en un tema estratégico en la política internacional y la defensa colectiva.

4. **Convención de Budapest sobre Ciberdelincuencia**:

La Convención de Budapest sobre Ciberdelincuencia, adoptada en 2001 y promovida por el Consejo de Europa, es el primer tratado internacional que aborda el cibercrimen y la cooperación transnacional en su persecución. Su importancia radica en que establece un marco legal común para que los países tipifiquen delitos informáticos, mejoren la cooperación en la recolección de evidencia digital y fortalezcan sus capacidades de persecución penal en casos de delitos cibernéticos (Council of Europe, 2001).

A pesar de haber sido impulsada por el Consejo de Europa, la Convención de Budapest ha sido firmada y ratificada por países de distintas regiones del mundo, convirtiéndose en un referente global en la legislación sobre cibercrimen. Su impacto se refleja en:

1. La adopción de normas legales armonizadas en más de 60 países, facilitando la cooperación en investigaciones transfronterizas.
2. La promoción de mecanismos de asistencia legal mutua (MLA) para agilizar la entrega de información entre Estados en la lucha contra el cibercrimen.

3. La actualización constante de sus disposiciones, a través de protocolos adicionales que abordan temas emergentes como la ciberdelincuencia transnacional y la protección de datos personales (Council of Europe, 2022).

Dado que los delitos informáticos no tienen fronteras, la Convención de Budapest representa un esfuerzo pionero en la institucionalización de la ciberdiplomacia al facilitar la cooperación internacional en la lucha contra el cibercrimen. Sin embargo, su alcance se ha visto limitado por la negativa de algunos países a adherirse, como China y Rusia, quienes han promovido sus propios marcos alternativos de gobernanza digital (Tikk & Kerttunen, 2020).

La institucionalización de la ciberdiplomacia a través de organismos multilaterales refleja un esfuerzo global por regular y coordinar la seguridad en el ciberespacio, en un contexto donde las amenazas cibernéticas son cada vez más sofisticadas y transnacionales. La ONU ha liderado iniciativas clave en la construcción de normas y marcos de gobernanza, mientras que la OEA ha jugado un papel fundamental en la cooperación regional en América Latina.

Asimismo, organismos como la OTAN, el G20 y el GFCE han contribuido a fortalecer la cooperación internacional, promoviendo mecanismos de seguridad cibernética tanto en ámbitos militares como económicos. La consolidación de la ciberdiplomacia como una herramienta fundamental en las relaciones internacionales demuestra que la seguridad digital no puede abordarse de manera unilateral, sino que requiere un esfuerzo coordinado entre Estados, empresas tecnológicas y la sociedad civil para garantizar la estabilidad del ciberespacio.

2.3.3 La Geopolítica del Ciberespacio.

El ciberespacio se ha consolidado en las últimas décadas como un nuevo escenario de disputa geopolítica, donde los Estados compiten no solo por el acceso y control de la información, sino también por la definición de las normas que rigen este entorno digital. En un contexto internacional marcado por la anarquía y la ausencia de un órgano regulador global en ciberseguridad, los Estados más poderosos han comenzado a posicionarse estratégicamente para garantizar su soberanía digital y proteger sus intereses económicos, militares y políticos (Kello, 2017).

La geopolítica del ciberespacio implica, por tanto, una disputa por el control de la infraestructura digital, el flujo de datos, las plataformas de comunicación y los espacios virtuales donde se almacena, procesa y distribuye información. Esta competencia trasciende el ámbito tecnológico, afectando aspectos claves de la soberanía nacional, la seguridad internacional y los derechos humanos (Nye, 2017).

2.3.3.1 La competencia por el dominio digital: Estados Unidos, China y Rusia.

Los principales actores de la geopolítica del ciberespacio son Estados Unidos, China y Rusia, quienes desde hace más de una década lideran los debates y conflictos relacionados con la gobernanza digital y la ciberseguridad global. Cada uno de estos países ha desarrollado estrategias específicas para extender su influencia en el ciberespacio y proteger sus intereses nacionales frente a amenazas reales y potenciales.

Estados Unidos, tradicionalmente, ha promovido una visión del ciberespacio basada en la libre circulación de la información, considerando el acceso abierto a internet como un elemento central de su modelo democrático y de su liderazgo económico y tecnológico. A través de la influencia de gigantes tecnológicos como Google, Amazon, Microsoft y Meta (Facebook), Estados Unidos ha dominado gran parte del tráfico global de datos, lo que le ha conferido una posición privilegiada en la arquitectura de internet (Segal, 2016). No obstante, frente al aumento de ciberataques por parte de actores estatales y no estatales, Estados Unidos ha reforzado sus capacidades de ciberdefensa y ha adoptado una política más agresiva en la identificación y disuasión de amenazas cibernéticas (Nye, 2017).

Por su parte, China ha promovido el modelo de la soberanía cibernética, según el cual cada Estado tiene derecho a controlar y regular el ciberespacio dentro de sus fronteras. Bajo este enfoque, el gobierno chino ejerce un control estricto sobre el contenido en línea, restringe el acceso a plataformas extranjeras y supervisa la actividad digital de sus ciudadanos a través de herramientas de censura y vigilancia como el "Gran Cortafuegos" (Segal, 2018). Además, China ha incrementado su capacidad de desarrollar tecnologías propias, como las redes 5G y las plataformas de inteligencia artificial, reduciendo su dependencia de infraestructuras digitales

extranjeras y ampliando su influencia en regiones como África y América Latina mediante proyectos de cooperación tecnológica.

Rusia, por su parte, ha adoptado una postura híbrida, combinando la promoción de la soberanía cibernética con acciones ofensivas en el ciberespacio, como ciberataques dirigidos a infraestructuras críticas y campañas de desinformación. Según Rid (2020), Rusia ha utilizado el ciberespacio como un espacio de "guerra política", desplegando operaciones de hackeo y filtración de información, como las evidenciadas durante las elecciones presidenciales en Estados Unidos en 2016. La estrategia rusa busca, por un lado, proteger su espacio digital interno y, por otro, debilitar a sus rivales estratégicos mediante operaciones de influencia.

2.3.3.2 Modelos de gobernanza digital: soberanía cibernética vs. libre circulación de datos.

En el debate sobre la gobernanza global del ciberespacio se enfrentan dos modelos principales:

1. La soberanía cibernética, defendida por China, Rusia y otros países, promueve el derecho de cada Estado a regular y controlar internet dentro de sus fronteras, con base en su soberanía nacional y seguridad interna (Segal, 2018). Este modelo defiende la creación de infraestructuras digitales propias, el control de contenidos y la restricción de plataformas extranjeras, justificando estas medidas como mecanismos para evitar el cibercrimen, el terrorismo digital y la injerencia extranjera. Sin embargo, sus críticos argumentan que esta visión limita la libertad de expresión y el acceso a la información, generando "ciberfronteras" que fragmentan el espacio digital global (Deibert, 2019).
2. La libre circulación de datos, respaldada por Estados Unidos, la Unión Europea y otros aliados, postula que internet debe ser un espacio abierto, sin restricciones indebidas, donde los datos fluyan libremente a través de las fronteras. Este modelo enfatiza la interoperabilidad de los sistemas, la cooperación internacional en ciberseguridad y la protección de los derechos digitales (Chertoff & Simon, 2018). No obstante, la creciente amenaza de ciberataques y la preocupación por la soberanía de los datos han llevado incluso a defensores de este modelo a proponer mayores controles y regulaciones, especialmente en lo relativo a la privacidad y la seguridad nacional.

2.3.3.3 Implicaciones para Costa Rica: inserción en la geopolítica del ciberespacio.

Costa Rica, como un Estado pequeño y altamente dependiente de las tecnologías digitales para la administración pública, la economía y los servicios esenciales, enfrenta importantes desafíos en su inserción en la geopolítica del ciberespacio. El ciberataque sufrido por la Caja Costarricense del Seguro Social (CCSS) en 2022 y los ataques al Ministerio de Hacienda evidenciaron la vulnerabilidad del país ante actores externos, así como la necesidad urgente de fortalecer su capacidad de ciberdefensa (MICITT, 2022).

A nivel internacional, Costa Rica debe navegar entre dos modelos contrapuestos: por un lado, la presión por mantener un ciberespacio abierto, compatible con su modelo democrático y de respeto a los derechos humanos; por otro, la necesidad de adoptar ciertas medidas de soberanía digital para protegerse de ciberamenazas que ponen en riesgo su estabilidad interna. En este contexto, la adhesión a acuerdos internacionales, como el Convenio de Budapest sobre Ciberdelincuencia, y la participación en foros multilaterales como la OEA y la ONU, son estrategias fundamentales para fortalecer su postura en la gobernanza del ciberespacio (OEA, 2020).

Además, Costa Rica se enfrenta al desafío de no quedar rezagada frente a las grandes potencias tecnológicas. La dependencia de servicios en la nube, proveedores internacionales de telecomunicaciones y plataformas digitales, coloca al país en una posición de vulnerabilidad frente a decisiones tomadas por actores globales. Por ello, desarrollar una estrategia nacional de ciberseguridad robusta, acompañada de una política activa de ciberdiplomacia, resulta imprescindible para equilibrar su seguridad digital con el respeto a los principios democráticos y los derechos fundamentales.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 Enfoque de la investigación

Para la presente investigación, se ha seleccionado un enfoque cualitativo, dado que el propósito principal es analizar la influencia de la ciberdiplomacia en la capacidad de respuesta del Estado costarricense frente a ciberataques, específicamente en el caso de los incidentes que afectaron a la Caja Costarricense de Seguro Social (CCSS). Según Hernández, Fernández y Baptista (2014), el enfoque cualitativo se enfoca en explorar los significados, experiencias y dinámicas sociales que subyacen a un fenómeno, lo que resulta adecuado para abordar un tema complejo como la interacción entre diplomacia, ciberseguridad y cooperación internacional (p. 2).

La elección del enfoque cualitativo se fundamenta en los objetivos de esta investigación, que buscan comprender a profundidad las estrategias diplomáticas adoptadas por el Estado costarricense y cómo estas han influido en su respuesta ante las amenazas cibernéticas. En este sentido, no se pretende medir ni probar hipótesis a través de datos numéricos, sino interpretar y analizar información a partir de fuentes documentales y testimonios clave. El enfoque cualitativo permite una aproximación más contextual y detallada, lo que es esencial para entender el impacto de las relaciones diplomáticas en la gestión de cibercrisis.

Este enfoque también facilita el uso de técnicas como el análisis de contenido y las entrevistas semi estructuradas con expertos en ciberseguridad y diplomacia. A través de estas metodologías, se espera extraer conclusiones significativas sobre los logros y desafíos de las políticas de ciberseguridad en Costa Rica, así como identificar áreas de mejora en la cooperación internacional.

Sin embargo, se reconoce que el enfoque cualitativo puede tener ciertas limitaciones, como la subjetividad en la interpretación de datos y la dificultad para generalizar los resultados. A pesar de ello, se considera que esta metodología es la más adecuada para alcanzar los objetivos propuestos, ya que ofrece una visión profunda y comprensiva del fenómeno investigado.

3.2 Método de la investigación

La presente investigación adopta un enfoque cualitativo para analizar la influencia de la ciberdiplomacia en la respuesta del Estado costarricense a los ciberataques sufridos por la Caja Costarricense de Seguro Social (CCSS) durante el período 2018-2023. Este enfoque es el más adecuado porque permite explorar en profundidad las experiencias, percepciones y significados que los actores involucrados atribuyen a las dinámicas de cooperación internacional en el ámbito de la ciberseguridad. Según Hernández, Fernández y Baptista (2014), el enfoque cualitativo se caracteriza por buscar una comprensión contextualizada de los fenómenos desde la perspectiva de los participantes, utilizando datos no numéricos y aplicando métodos flexibles en la recolección de información.

El diseño fenomenológico ha sido seleccionado porque la investigación busca comprender las experiencias subjetivas de los actores involucrados en la gestión de ciberataques, con un énfasis particular en cómo interpretan el papel de la ciberdiplomacia en la protección de infraestructuras críticas. Según Creswell y Poth (2018), el enfoque fenomenológico permite explorar cómo los individuos viven un fenómeno en su contexto específico y proporciona una descripción detallada de las experiencias compartidas. En este caso, se analizarán las perspectivas de funcionarios públicos, expertos en ciberseguridad y diplomáticos que participaron en las estrategias de respuesta a los ciberataques.

Este enfoque es adecuado porque no se pretende establecer correlaciones estadísticas ni medir fenómenos, sino interpretar los significados y percepciones de los participantes. Así, se logrará una comprensión profunda del impacto de la cooperación internacional y de las alianzas diplomáticas en la mejora de las políticas de ciberseguridad en Costa Rica.

La recolección de datos se basará en dos técnicas principales:

1. Entrevistas a profundidad: Se realizarán entrevistas semiestructuradas a expertos en ciberseguridad involucrados en la gestión de ciberataques. Esta técnica permitirá explorar las percepciones, motivaciones y desafíos que enfrentaron durante la implementación de

las estrategias de respuesta. Las entrevistas semi estructuradas proporcionan flexibilidad para que los entrevistados expresen sus opiniones en profundidad (Kvale, 2007).

2. Análisis documental: Se recopilarán documentos oficiales como el informe del MICITT (2022), reportes de la Organización de los Estados Americanos (OEA), normativas nacionales en ciberseguridad, y acuerdos internacionales que hayan impactado la estrategia costarricense de ciberdefensa. Esta técnica ayudará a contextualizar las experiencias de los participantes y a vincular las políticas diplomáticas con los resultados obtenidos en la ciberseguridad.

El proceso de investigación se dividirá en cuatro fases:

1. Fase exploratoria: En esta etapa se identificarán las fuentes documentales relevantes y se seleccionarán los participantes para las entrevistas.
2. Fase de recolección de datos: Se aplicarán entrevistas semiestructuradas y se revisarán los documentos recopilados. Esta fase permitirá captar las experiencias subjetivas de los participantes y obtener información contextual relevante.
3. Fase de análisis: Los datos recolectados serán organizados y codificados mediante un análisis temático, identificando patrones y categorías emergentes. Según Braun y Clarke (2006), el análisis temático es útil en investigaciones cualitativas porque permite encontrar conexiones significativas en los testimonios de los participantes.
4. Fase de redacción: En esta fase se integrarán los hallazgos obtenidos en un estudio de caso sobre los ciberataques a la Caja Costarricense de Seguro Social (CCSS), vinculando las experiencias de los actores con las políticas implementadas y proponiendo recomendaciones para mejorar las estrategias de ciberseguridad mediante la diplomacia.

El enfoque fenomenológico se justifica porque permite explorar las experiencias individuales y colectivas de los actores involucrados en la ciberseguridad costarricense, proporcionando una visión profunda y contextual del fenómeno. Al interpretar las percepciones y vivencias de los participantes, se obtendrán hallazgos cualitativos relevantes que contribuirán al conocimiento sobre las dinámicas entre la ciberdiplomacia y la ciberdefensa. Además, la investigación contribuirá al desarrollo de políticas más eficaces para proteger las infraestructuras críticas, basándose en las experiencias previas y las recomendaciones de los participantes.

Este diseño cualitativo y fenomenológico permite comprender cómo la ciberdiplomacia ha influido en la respuesta estatal a los ciberataques, desde las perspectivas de los actores involucrados. Al centrarse en un caso real y en las experiencias subjetivas de los participantes, la investigación proporcionará conocimientos valiosos para mejorar las políticas de ciberseguridad en Costa Rica y promover una cooperación internacional más efectiva. Además, los hallazgos podrán ser útiles para otros países de la región que enfrenten desafíos similares en la protección de sus infraestructuras críticas.

3.3 Fuentes de información

Las fuentes de información constituyen el fundamento del proceso investigativo, ya que proporcionan los datos necesarios para analizar y comprender el fenómeno en estudio. En este contexto, se entiende por fuente de información cualquier recurso que permita satisfacer las necesidades informativas del investigador, facilitando la recopilación de datos relevantes (Arias, 2019). Estas fuentes incluyen tanto los participantes del estudio como documentos y registros relevantes, divididos en **fuentes primarias** y **secundarias**. La selección adecuada de estas fuentes es fundamental para responder al problema planteado, cumplir con los objetivos propuestos y asegurar la validez de los resultados obtenidos (Hernández, Fernández y Baptista, 2014). A continuación, se detallan las características de la muestra de investigación y las fuentes utilizadas.

3.3.1 Muestra de la investigación

Dado el enfoque cualitativo de esta investigación, se utilizará una muestra no probabilística por conveniencia y criterios. Esta estrategia permite seleccionar participantes que posean experiencia y conocimientos específicos relacionados con la ciberdiplomacia y la ciberseguridad en Costa Rica, asegurando una comprensión profunda del tema (Flick, 2015). La muestra estará compuesta por actores clave involucrados en la gestión de los ciberataques a la Caja Costarricense de Seguro Social (CCSS) y en la cooperación internacional en ciberseguridad.

Se ha delimitado la población objetivo a tres grupos principales: funcionarios del MICITT, quienes lideran la formulación de políticas de ciberseguridad; representantes de la Caja Costarricense de Seguro Social (CCSS), que participaron en la gestión de los ciberataques sufridos entre 2018 y 2023; y miembros de la OEA, quienes colaboraron en iniciativas de cooperación para fortalecer las capacidades del país en esta materia.

Para la selección de los participantes, se establecieron criterios de inclusión que exigen una experiencia mínima de dos años en gestión de ciberseguridad o diplomacia digital. Además, se excluyen aquellos actores sin relación directa con las respuestas a los ciberataques o cuyas experiencias estén desactualizadas (anteriores a 2018). Esta delimitación garantiza que la información recopilada sea relevante y pertinente para el objetivo del estudio.

3.3.2 Fuentes primarias

Las fuentes primarias constituyen el núcleo de la recolección de datos en esta investigación, ya que proporcionan información directa y específica del fenómeno analizado. En este caso, se obtendrán datos mediante entrevistas semiestructuradas a funcionarios del MICITT, representantes de la Caja Costarricense de Seguro Social (CCSS) y colaboradores de la OEA. Las entrevistas permiten explorar percepciones, estrategias y experiencias relacionadas con la gestión de ciberataques y la cooperación internacional en ciberseguridad, ofreciendo una perspectiva profunda y contextualizada (Taylor, Bogdan y DeVault, 2016).

Además, se revisarán documentos internos y registros oficiales del MICITT, la Caja Costarricense de Seguro Social (CCSS) y otras instituciones estatales para comprender las medidas adoptadas y los desafíos enfrentados durante las crisis cibernéticas. Estas fuentes brindan evidencia directa de las acciones emprendidas y facilitan la evaluación de la eficacia de las estrategias implementadas.

3.3.3 Fuentes secundarias

Las fuentes secundarias complementan los datos primarios, proporcionando contexto y facilitando la triangulación de información para lograr una interpretación más amplia y sólida de los hallazgos. Entre las fuentes secundarias se incluyen artículos académicos y tesis que abordan

temas de ciberdiplomacia, ciberseguridad y gestión de crisis digitales en la región. Estos estudios permiten comparar las experiencias de Costa Rica con otros contextos internacionales y regionales, enriqueciendo el análisis (Hernández et al., 2014).

También se emplearán informes de organizaciones internacionales, como los documentos de la OEA, que aportan información sobre las iniciativas de cooperación en ciberseguridad. De igual manera, se consultarán libros y textos normativos relevantes para fundamentar el marco teórico con enfoques de las relaciones internacionales, como el constructivismo y el realismo. Finalmente, los reportajes periodísticos que cubrieron los ciberataques a la Caja Costarricense de Seguro Social (CCSS) proporcionan datos adicionales sobre el impacto social y las repercusiones económicas de estos eventos, ofreciendo una perspectiva más completa del fenómeno.

3.4 Población y muestra

La población en una investigación representa el grupo de personas, entidades u objetos sobre los cuales se busca obtener información relevante para responder a los objetivos planteados. En este sentido, Arias et al. (2016) afirman que:

> "La población de estudio es un conjunto de casos, definido, limitado y accesible, que formará el referente para la elección de la muestra, y que cumple con una serie de criterios predeterminados. Es necesario aclarar que cuando se habla de población de estudio, el término no se refiere exclusivamente a seres humanos sino que también puede corresponder a animales, muestras biológicas, expedientes, hospitales, objetos, familias, organizaciones, etc." (p. 202).

De acuerdo con lo anterior, la población de esta investigación está conformada por los actores involucrados en la gestión de ciberataques en Costa Rica durante el periodo 2018-2023, con especial atención en los ataques sufridos por la Caja Costarricense de Seguro Social (CCSS). Esta población incluye tanto a funcionarios públicos como a representantes de organizaciones internacionales y expertos en ciberseguridad. La relevancia de estos actores radica en que, a partir de sus experiencias y conocimientos, es posible analizar la efectividad de la combinación entre diplomacia y ciberseguridad en la respuesta del Estado costarricense ante los ciberataques.

En investigaciones cualitativas, como la presente, se emplea un muestreo intencional o criterial, en el que se seleccionan casos específicos que puedan aportar información valiosa para comprender el fenómeno de estudio (Hernández, Fernández y Baptista, 2014). El objetivo no es lograr una muestra estadísticamente representativa, sino seleccionar actores clave que permitan un análisis profundo de la problemática. En este caso, la muestra estará compuesta por:

1. Funcionarios del servicio exterior costarricense con experiencia en relaciones diplomáticas y representación del país en el extranjero, particularmente en temas vinculados a la ciberseguridad y cooperación internacional.
2. Expertos en gobernanza digital y formulación de políticas públicas en ciberseguridad, con trayectoria en el sector público y la sociedad civil.
3. Especialistas en ciberseguridad en el sector financiero, con conocimiento sobre la protección de infraestructuras críticas y la gestión de riesgos ante ciberataques.

La elección de esta muestra permitirá obtener información detallada y relevante sobre las estrategias utilizadas por el Estado costarricense para gestionar ciberataques mediante la cooperación internacional. La combinación de voces institucionales y académicas proporcionará una perspectiva integral sobre los logros, desafíos y aprendizajes del proceso. Como señalan Hernández et al. (2014), en estudios cualitativos se prioriza la profundidad y la riqueza de los datos obtenidos, en lugar de la generalización estadística, buscando comprender el fenómeno desde las experiencias de los actores clave.

Tabla 1.

Entrevistado	**Puesto**	**Razón**
No. 1 Jazmín Esquivel Vega	Consejera y Cónsul en el Consulado General de Costa Rica en Atlanta, Georgia.	Brinda una visión diplomática sobre la cooperación internacional en ciberseguridad y la importancia de la ciberdiplomacia en la respuesta ante ataques cibernéticos.

No. 2 Paula Brenes Ramírez	Presidenta de la Fundación YoD y exdirectora de Gobernanza Digital en el MICITT.	Ofrece información clave sobre la formulación de estrategias nacionales de ciberseguridad y el papel del MICITT en la gestión del ciberataque a la CCSS.
No. 3 Yuliana Leitón Álvarez	Especialista en Ciberseguridad en el Banco Nacional de Costa Rica.	Aporta una perspectiva técnica sobre las estrategias de ciberseguridad implementadas en el sector financiero y su relación con las acciones tomadas tras el ciberataque a la CCSS.

Fuente: Elaboración propia.

3.5 Unidad de análisis

La respuesta del Estado costarricense ante los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS) durante el período 2018-2023.

3.6 Instrumentos

Para garantizar la obtención de información relevante que permita cumplir con los objetivos de la investigación, se emplearán diversos instrumentos metodológicos. Estos proporcionarán una base sólida para el análisis cualitativo, permitiendo recoger datos desde diferentes perspectivas.

3.6.1 Revisión bibliográfica

La revisión bibliográfica es fundamental para recopilar información secundaria que contextualice el fenómeno investigado. Esta fase incluirá el análisis de documentos académicos, informes institucionales, normativas nacionales e internacionales y estudios previos relacionados con la ciberdiplomacia y ciberseguridad en Costa Rica. La revisión permitirá identificar marcos conceptuales y teóricos relevantes, así como los avances en políticas públicas en la materia (Hernández, Fernández & Baptista, 2014).

3.6.2 Cuestionario

Se diseñará un cuestionario estructurado para recopilar información directa de los actores involucrados. Este instrumento facilitará la obtención de datos estandarizados y permitirá comparar respuestas de diferentes participantes. Las preguntas estarán orientadas a identificar percepciones sobre las políticas de ciberseguridad y el impacto de la ciberdiplomacia en la respuesta estatal. Los cuestionarios serán aplicados principalmente a expertos en ciberseguridad, funcionarios públicos y miembros de instituciones clave en el manejo de incidentes cibernéticos.

3.6.3 Entrevista a profundidad

Este instrumento permitirá explorar a fondo las opiniones, experiencias y perspectivas de los participantes. Las entrevistas se realizarán con actores clave, como funcionarios del MICITT y qla Caja Costarricense de Seguro Social (CCSS). Al ser semi-estructuradas, ofrecerán flexibilidad para que los entrevistados profundicen en temas relevantes, proporcionando información cualitativa que no puede ser obtenida mediante cuestionarios (Taylor, Bogdan & DeVault, 2016).

3.6.4 Grupo focal

Se utilizarán grupos focales para recolectar datos mediante la interacción entre varios participantes. Los grupos estarán conformados por expertos en ciberseguridad, representantes del sector privado y funcionarios gubernamentales, lo que permitirá conocer diversas perspectivas y enriquecer el análisis. Este método ayudará a identificar consensos y discrepancias en torno a la cooperación internacional y la diplomacia en la gestión de incidentes cibernéticos. La dinámica de discusión grupal permitirá explorar ideas colectivas y emergentes que no surgen fácilmente en entrevistas individuales (Krueger & Casey, 2015).

Estos instrumentos se integrarán en el proceso de análisis de datos, facilitando la triangulación de la información recopilada para asegurar la validez y confiabilidad de los resultados obtenidos. Cada método aportará elementos distintos que permitirán construir una comprensión profunda del fenómeno estudiado y generar conclusiones sólidas.

3.7 Recolección y procesamiento de datos

La recolección de datos es una etapa fundamental en toda investigación, ya que permite obtener la información necesaria para analizar el fenómeno de estudio y responder a los objetivos planteados. Según la Universidad del Desarrollo (s.f.), "El o los instrumentos de recolección de información deben estar vinculados y alineados con la selección del diseño de investigación y la muestra apropiados al problema de investigación propuesto. La selección de estos instrumentos presenta un plan detallado del procedimiento que conduce al investigador a cumplir con los objetivos específicos" (p. 1).

En el marco de esta investigación cualitativa sobre la influencia de la ciberdiplomacia en la respuesta del Estado costarricense ante los ciberataques dirigidos a la Caja Costarricense de Seguro Social (CCSS), se han definido las siguientes fases para la recolección y procesamiento de los datos:

1. Selección del tema
2. Ejecución de la investigación
3. Recolección de datos bibliográficos
4. Entrevistas a profundidad
5. Aplicación de cuestionarios y grupos focales
6. Procesamiento y análisis de la información recopilada
7. Conclusiones y recomendaciones

La combinación de fuentes primarias y secundarias, junto con el uso de múltiples instrumentos de recolección de datos, permitió una comprensión integral del fenómeno investigado. El proceso de análisis garantizó que las conclusiones reflejaran de manera fiel las experiencias y perspectivas de los actores clave, proporcionando una base sólida para la elaboración de recomendaciones.

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE DATOS.

El presente capítulo expone el análisis y la interpretación de los datos obtenidos en función de los objetivos específicos planteados en esta investigación. Se analizan tanto las estrategias de ciberdiplomacia adoptadas por el Estado costarricense para enfrentar los ciberataques a la Caja Costarricense del Seguro Social (CCSS), como la relevancia y efectividad de dichas estrategias en el marco de la cooperación internacional. La información ha sido recopilada a partir de fuentes documentales oficiales, tales como informes del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), informes de la Caja Costarricense de Seguro Social (CCSS), así como entrevistas a actores clave vinculados con la respuesta del Estado costarricense frente al ciberataque de 2022.

4.1 Principales estrategias de ciberdiplomacia costarricense para la aplicación de la ciberseguridad.

El análisis de las estrategias de ciberdiplomacia implementadas por el Estado costarricense entre 2018 y 2023 en el contexto de la ciberseguridad revela la importancia de la cooperación internacional y el desarrollo de políticas nacionales para fortalecer la respuesta ante amenazas cibernéticas. De acuerdo con la entrevista realizada a Paula Brenes, exdirectora de Gobernanza Digital en el MICITT, el ataque a la Caja Costarricense de Seguro Social (CCSS) en 2022 no puede considerarse un evento aislado, sino parte de una serie de incidentes que afectaron a diversas instituciones del Estado costarricense. En sus palabras:

> "Tal vez como para poner en contexto, no deberías ver el ataque al Seguro Social como un hecho aislado, sino que el ciberataque sufrido en el 2022 corresponde a una serie de acciones que inician en un cambio de administración pública del Presidente de la República. Entonces, no fue un ataque a la Caja Costarricense del Seguro Social, fue un ataque al país. Estamos hablando de 27 instituciones, casi al mismo tiempo" (Brenes, 2025).

Esta visión más amplia del problema llevó al gobierno costarricense a declarar el estado de emergencia nacional, facilitando la implementación de estrategias de contención y mitigación,

así como la movilización de recursos nacionales e internacionales. Entre las principales acciones desarrolladas en este contexto se encuentra la elaboración del Plan de Atención a la Emergencia Nacional, documento que recopiló los esfuerzos institucionales para responder a la crisis cibernética y que, según Brenes, está disponible en la Comisión Nacional de Emergencias.

La colaboración internacional fue un componente clave en estas estrategias, permitiendo el acceso a conocimientos técnicos, herramientas de seguridad avanzadas y asesoramiento en la formulación de políticas públicas. Brenes enfatizó que varios países ofrecieron apoyo a Costa Rica durante la crisis, aunque posteriormente la cooperación internacional se concentró en un único país, lo que subraya la necesidad de establecer marcos claros de actuación en situaciones de emergencia. Al respecto, señaló:

> "Al ser Costa Rica un país que no tiene ejército, debería tener más estructurada la atención de los incidentes, y así lo determina la Contraloría de la República cuando hace el estudio del ciberataque. [...] El mayor riesgo es improvisar, porque después le sale muy costoso al país este tema. Creo que la seguridad nacional no puede estar dedicada exclusivamente al acompañamiento internacional, porque eso nos hace perder soberanía" (Brenes, 2025).

Esta declaración destaca la tensión entre la necesidad de asistencia internacional y la preservación de la autonomía estatal en la gestión de la ciberseguridad. La entrevista también reveló que, tras el ciberataque, se impulsaron reformas en materia de seguridad digital, incluyendo la actualización del Código Nacional de Tecnologías Digitales y la introducción de normas técnicas específicas sobre ciberseguridad. Asimismo, la Contraloría General de la República emitió directrices para mejorar la regulación y la respuesta a incidentes, subrayando la necesidad de fortalecer la institucionalidad del Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT), cuya existencia se basa en un decreto y no en una ley formal.

Otra de las estrategias clave mencionadas en la entrevista fue la necesidad de un enfoque más preventivo en materia de ciberseguridad, que no solo contemple la respuesta a incidentes, sino que también fortalezca el desarrollo tecnológico seguro y la capacitación de los usuarios. Brenes afirmó:

> "Más del 90% de los ataques entran por un error humano a las instituciones. Si te focalizas solamente en el ataque, no estás viendo la causa real de la caída de lo que pasó en la Caja o en cualquiera de estas instituciones grandes. [...] La causa raíz principal de lo vivido en Costa Rica es el desarrollo de la tecnología que Costa Rica tiene, la protección de datos, la privacidad, la forma en que desarrollamos la tecnología" (Brenes, 2025).

Este enfoque preventivo implica la adopción de mejores prácticas en el desarrollo de software, la segmentación de redes, la gestión de accesos y la promoción del doble factor de autenticación como medidas fundamentales para reducir la vulnerabilidad de las instituciones costarricenses ante ataques cibernéticos.

En términos diplomáticos, Brenes destacó que la Cancillería debería desempeñar un rol más activo en la negociación de acuerdos internacionales en materia de ciberseguridad, asegurando que estos beneficien a Costa Rica sin comprometer la protección de datos sensibles. Subrayó que la aceptación indiscriminada de apoyo internacional podría conllevar riesgos en términos de vigilancia y privacidad, por lo que es fundamental que la diplomacia costarricense cuente con especialistas capacitados para evaluar y negociar estos acuerdos de manera estratégica.

Finalmente, la estrategia de ciberdiplomacia adoptada por Costa Rica entre 2018 y 2023 ha estado marcada por la cooperación internacional, el fortalecimiento de marcos regulatorios y la implementación de mejores prácticas en el ámbito de la ciberseguridad. Sin embargo, la experiencia del ciberataque a la CCSS ha dejado lecciones importantes sobre la necesidad de estructurar de manera más eficiente la atención de incidentes, fortalecer la autonomía en la toma de decisiones de seguridad y promover una cultura de ciberseguridad que integre tanto a instituciones como a la ciudadanía.

4.2 Actores internacionales y su impacto en la ciberdiplomacia costarricense durante los ciberataques de la Caja Costarricense de Seguro Social (CCSS)

El ataque cibernético contra la Caja Costarricense de Seguro Social (CCSS) en 2022 evidenció la importancia de la cooperación internacional en la respuesta a incidentes de

seguridad digital. Diversos actores internacionales desempeñaron un papel crucial en la mitigación de los efectos del ataque y en la recuperación de los sistemas afectados. Según los informes de auditoría interna de la Caja Costarricense del Seguro Social (CCSS):

> "La intervención de organismos multilaterales, agencias gubernamentales extranjeras y empresas privadas fue determinante para fortalecer la ciberseguridad del país y reducir la vulnerabilidad ante futuras amenazas" (CCSS, 2022, Informe AD-ATIC-039-2022).

Uno de los actores internacionales más relevantes fue la Organización de los Estados Americanos (OEA), que a través de su Programa de Ciberseguridad brindó asistencia técnica a Costa Rica. La OEA facilitó el intercambio de información sobre amenazas, proporcionando recomendaciones para la mejora de la respuesta gubernamental. Además, la Caja Costarricense del Seguro Social (CCSS) participó en la identificación de vulnerabilidades críticas en la infraestructura digital de la CCSS y en la implementación de protocolos de seguridad más rigurosos. Como se menciona en los informes:

> "La OEA desempeñó un papel clave en la detección y mitigación de amenazas, brindando asesoría especializada en la formulación de estrategias de ciberseguridad y promoviendo la colaboración entre el sector público y privado para reforzar la protección de la infraestructura digital" (OEA, 2022, Informe AS-ATIC-090-2023).

Por otro lado, el Buró Federal de Investigaciones (FBI) de los Estados Unidos también tuvo un papel significativo en la investigación del ataque. Según los informes internos de la Caja Costarricense del Seguro Social (CCSS):

> "El FBI aportó conocimientos especializados en análisis forense digital, lo que permitió rastrear el origen del ataque y comprender las técnicas utilizadas por los ciberdelincuentes. Además, contribuyó con herramientas avanzadas para la detección de amenazas y el fortalecimiento de capacidades nacionales en ciberseguridad" (CCSS, 2022, Informe AD-ATIC-067-2022).

Otro actor relevante fue la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA, por sus siglas en inglés), la cual es una entidad gubernamental

encargada de proteger las infraestructuras críticas del país frente a amenazas cibernéticas. Su labor incluye la prevención, detección y respuesta ante incidentes de seguridad digital, así como la colaboración con gobiernos y organizaciones a nivel internacional para fortalecer las capacidades de ciberseguridad. En el contexto del ataque a la CCSS, su participación fue fundamental para mitigar los daños y reforzar la resiliencia del sistema costarricense. En los informes se menciona que:

> "La CISA proporcionó herramientas de detección y mitigación de amenazas, además de capacitar al personal costarricense en la respuesta a incidentes cibernéticos. Este acompañamiento facilitó la restauración de servicios críticos y la implementación de medidas de seguridad más robustas" (CISA, 2022, Informe AS-AATIC-174-2022).

En el ámbito privado, empresas tecnológicas como Microsoft y Cisco también contribuyeron significativamente a la respuesta ante el ciberataque. Microsoft colaboró con el análisis de vulnerabilidades en los sistemas afectados y recomendó soluciones para fortalecer la protección de la infraestructura digital de la Caja Costarricense del Seguro Social (CCSS). Cisco, por su parte, apoyó con la implementación de soluciones de seguridad de red y monitoreo de amenazas, lo que permitió una respuesta más efectiva ante posibles nuevos ataques. Como se señala en los informes:

> "La colaboración con empresas privadas permitió acelerar la recuperación de los sistemas afectados y fortalecer la protección contra futuras amenazas. Microsoft y Cisco brindaron apoyo en la identificación de vulnerabilidades y en la implementación de soluciones de seguridad avanzadas" (CCSS, 2022, Informe AS-AATIC-093-2022).

Los informes de auditoría interna de la Caja Costarricense del Seguro Social (CCSS) destacan la importancia de estas colaboraciones en la gestión del ciberataque y en la prevención de futuros incidentes. Además, subrayan la necesidad de continuar fortaleciendo la cooperación internacional para mejorar las capacidades nacionales en ciberseguridad y garantizar la protección de infraestructuras críticas. Según el informe:

"El fortalecimiento de la cooperación internacional debe ser una prioridad para garantizar la protección de las infraestructuras críticas del país. La integración de actores internacionales en la estrategia de ciberseguridad ha demostrado ser un factor clave en la mitigación de amenazas" (CCSS, 2022, Informe AS-ATIC-006-2023).

La respuesta al ciberataque contra la Caja Costarricense del Seguro Social (CCSS) en 2022 demostró el valor de la diplomacia cibernética y la cooperación internacional en la seguridad digital. La participación de la OEA, el FBI, la CISA y empresas tecnológicas permitió una reacción coordinada y efectiva, facilitando la mitigación del impacto del ataque y el fortalecimiento de la infraestructura de ciberseguridad en Costa Rica. La experiencia adquirida refuerza la importancia de seguir fomentando alianzas internacionales en materia de ciberseguridad para enfrentar amenazas cada vez más sofisticadas.

Este caso evidenció la colaboración entre distintos actores en el ámbito de la ciberseguridad, incluyendo dos agencias gubernamentales de Estados Unidos (el FBI y la CISA), un organismo internacional (la OEA) y dos empresas privadas de tecnología de origen estadounidense. La combinación de estos esfuerzos permitió una respuesta más estructurada y efectiva, resaltando el papel clave de la cooperación público-privada e internacional en la gestión de crisis cibernéticas.

4.3 Importancia de la diplomacia en la cooperación internacional ante ciberataques a la Caja Costarricense de Seguro Social (CCSS).

La respuesta diplomática ante los ciberataques a infraestructuras críticas es hoy un componente fundamental en la política exterior y de seguridad nacional de los Estados. Tal como lo ha planteado la literatura, la ciberdiplomacia no se limita a la negociación de tratados o a la creación de normas internacionales, sino que se convierte en una herramienta clave para obtener cooperación técnica, asistencia financiera, y respaldo político en momentos de crisis (Lewis, 2018; Nye, 2017).

En el caso de Costa Rica, el ataque cibernético dirigido a la Caja Costarricense del Seguro Social (CCSS) en 2022 no solo puso a prueba las capacidades internas de ciberdefensa,

sino también la habilidad diplomática del Estado para articular una respuesta internacional efectiva.

Desde esta perspectiva, la entrevista realizada a la licenciada en Relaciones Internacionales con énfasis en comercio exterior, Jazmín Esquivel, quien a su vez se desempeña como funcionaria del Ministerio de Relaciones Exteriores y Culto, permite evidenciar los desafíos, vacíos y logros que enfrenta Costa Rica en materia de ciberdiplomacia.

Esquivel reconoce que el desarrollo de una diplomacia cibernética formal y proactiva aún es incipiente en el país, señalando que "Costa Rica todavía está dando sus primeros pasos realmente en temas de ciberdiplomacia, temas digitales. Es algo en lo que todavía estamos aprendiendo las mejores prácticas de Estados que tienen más tiempo en esto" (Esquivel, comunicación personal, 2025).

Este reconocimiento es significativo, ya que sitúa a Costa Rica dentro de la categoría de Estados en desarrollo digital, aquellos que, aunque han avanzado en la digitalización de sus servicios, carecen de capacidades robustas para responder a ciberamenazas complejas (Bechara & Schuch, 2021). A diferencia de potencias como Estados Unidos, Rusia o China, cuya diplomacia digital está consolidada y alineada con estrategias nacionales de ciberdefensa, Costa Rica carece de una política específica de ciberdiplomacia integrada a su política exterior, lo que limita su capacidad de actuar de manera preventiva frente a amenazas transnacionales.

Uno de los aspectos más relevantes señalados por Esquivel es que las alianzas estratégicas que Costa Rica logra establecer, como las mantenidas con Estados Unidos e Israel, se activan principalmente de manera reactiva y no como parte de una política continua y estructurada. La funcionaria menciona que, aunque estos países han mostrado disposición para cooperar, el tema de ciberseguridad no está aún formalmente institucionalizado en todas las relaciones bilaterales, sino que se gestiona "de manera personalizada, dependiendo de cada relación" (Esquivel, 2025).

Esta observación coincide con lo que autores como Nye (2017) han llamado ciberdiplomacia reactiva, es decir, aquella que se activa únicamente ante situaciones de crisis, en

lugar de desarrollarse como una estrategia constante de cooperación internacional. Para un país como Costa Rica, que carece de capacidades ofensivas y defensivas avanzadas, la falta de una ciberdiplomacia proactiva representa un riesgo significativo frente a futuras amenazas cibernéticas.

Por otro lado, Esquivel reconoce que, pese a estas limitaciones, el aparato diplomático costarricense cuenta con algunas herramientas institucionales que podrían aprovecharse mejor para facilitar la cooperación internacional en ciberseguridad. Menciona, por ejemplo, los contactos establecidos por las embajadas costarricenses y las misiones permanentes en la ONU y la OEA, a las cuales podría recurrirse con mayor agilidad para solicitar asistencia internacional en casos de crisis. No obstante, la entrevistada señala que estos canales no están plenamente articulados ni preparados para una respuesta rápida y sistematizada en caso de un nuevo ciberataque. En sus palabras:

> "Yo siento que si llegáramos a tener otro ciberataque al nivel del que hubo en la Caja Costarricense del Seguro Social (CCSS), en lugar de ser algo un poco como más proactivo que nosotros vinimos preparando, nuestra diplomacia reaccionaría de una forma un poco más coyuntural, tocando puertas de nuestros socios y decirles, mira nos pasó esto, puedes ayudarnos" (Esquivel, 2025).

Este punto refleja claramente una carencia en la estrategia nacional de respuesta diplomática a cibercrisis, ya que las alianzas no están formalizadas mediante protocolos o acuerdos previos. Tal situación contrasta con el enfoque de países como Estonia, que desde los ataques de 2007 han construido una estrategia nacional de ciberdiplomacia, integrando a la Cancillería como un actor clave en la coordinación de respuestas internacionales (Ottis, 2008).

Asimismo, Esquivel propone una visión clara del rol que debería tener el Ministerio de Relaciones Exteriores en la ciberseguridad nacional. Sostiene que la Cancillería no debe asumir un rol técnico, sino actuar como un "tentáculo" que conecte a las instituciones nacionales con los recursos internacionales, afirmando:

> "El Ministerio debería de ser como este tentáculo entre Costa Rica y el exterior, que las instancias que manejan temas tecnológicos en Costa Rica expresen abiertamente que necesitan respaldo en tal tema de ciberseguridad" (Esquivel, 2025).

Esta visión se alinea con las teorías recientes sobre gobernanza de la ciberseguridad, que sostienen que la diplomacia debe actuar como un puente entre la política interna y las redes globales de seguridad digital (Segal, 2016). Por tanto, Costa Rica necesita formalizar este papel mediante la creación de protocolos específicos, oficinas de ciberdiplomacia o secciones especializadas dentro de la Cancillería.

Finalmente, Esquivel aporta recomendaciones clave para el fortalecimiento de la ciberdiplomacia costarricense, las cuales son vitales para superar los desafíos mencionados. Entre ellas destacan:

1. Capacitar al funcionariado público en la importancia y manejo de infraestructura crítica digital, con el fin de elevar la conciencia sobre la importancia de la ciberseguridad.
2. Establecer una cartera clara de socios estratégicos y crear grupos de trabajo específicos para ciberseguridad, con canales directos de comunicación y cooperación en tiempo real.
3. Posicionar a Costa Rica internacionalmente como un actor comprometido y competente en ciberseguridad, para ganar credibilidad y atraer cooperación.

Estas propuestas no solo buscan mejorar la respuesta a futuras crisis, sino también insertar a Costa Rica de manera más sólida en las redes diplomáticas globales de ciberseguridad. Este enfoque podría facilitar la transición del país hacia una ciberdiplomacia más proactiva y preventiva, en alineación con las mejores prácticas internacionales.

Por tanto, el análisis de la entrevista revela que la diplomacia ha sido y seguirá siendo un componente crucial en la capacidad de Costa Rica para enfrentar ciberataques complejos como el sufrido por la Caja Costarricense de Seguro Social (CCSS), aunque es urgente avanzar hacia una institucionalización de la ciberdiplomacia como política pública nacional.

4.4 Evaluación de la eficacia de la ciberdiplomacia en la respuesta a los ciberataques contra la Caja Costarricense del Seguro Social (CCSS).

El ataque cibernético sufrido por la Caja Costarricense de Seguro Social (CCSS) en 2022 representó un parteaguas en la historia de la ciberseguridad costarricense. Este incidente puso en evidencia no solo la vulnerabilidad de la infraestructura digital del país, sino también la necesidad de desarrollar mecanismos diplomáticos y de cooperación internacional más efectivos. En el contexto global actual, la seguridad cibernética no puede abordarse de manera aislada, ya que los ataques suelen trascender fronteras y estar asociados con actores estatales y no estatales de distintas jurisdicciones.

A través de la entrevista realizada a Yuliana Leitón Álvarez, especialista en ciberseguridad y auditora del Banco Nacional de Costa Rica, se obtuvo un testimonio clave sobre la gestión diplomática del Estado costarricense en la respuesta al ciberataque, identificando logros, obstáculos y áreas de mejora. Su experiencia permite realizar un análisis detallado de la manera en que se articularon las estrategias de ciberdiplomacia, tanto en términos de cooperación técnica como en la activación de alianzas internacionales.

Uno de los puntos centrales expuestos por la entrevistada es que Costa Rica no contaba con un plan estratégico definido para responder a un ataque cibernético de gran magnitud, lo que llevó a que las decisiones fueran tomadas de manera improvisada y reactiva. Según sus palabras:

> "El problema fue que no había una respuesta estructurada. La Caja Costarricense del Seguro Social no tenía un plan claro de contingencia para un ciberataque de esta magnitud. Esto llevó a que se tomaran decisiones reactivas en lugar de preventivas, lo que agravó el impacto y retrasó la recuperación de los sistemas comprometidos. La falta de comunicación entre las entidades afectadas y los organismos de seguridad internacional hizo que se perdiera tiempo valioso en los primeros días del ataque." (Leitón, 2025).

El testimonio de Leitón es coherente con los hallazgos del informe del MICITT (2022), en el cual se señala que las instituciones del Estado carecían de protocolos específicos para

manejar incidentes de ransomware a gran escala. Esta situación no es exclusiva de Costa Rica, sino que ha sido identificada en otros países que han enfrentado ataques similares sin contar con estructuras robustas de ciberseguridad.

Por ejemplo, el ataque de ransomware WannaCry en 2017, que afectó a más de 150 países, evidenció fallas similares en la coordinación gubernamental de varios Estados, lo que llevó a respuestas lentas y fragmentadas (NATO, 2020). Sin embargo, países con estrategias de ciberdiplomacia bien establecidas, como Estonia, lograron activar rápidamente sus protocolos de cooperación internacional, minimizando el impacto del ataque y restaurando servicios en menor tiempo (Ottis, 2008).

En el caso costarricense, si bien la Cancillería y el MICITT lograron contactar a organismos internacionales y recibir asistencia técnica, la ausencia de una estructura formal de ciberdiplomacia dificultó la canalización eficiente de esta ayuda. Leitón señala que:

> "Las entidades internacionales como el FBI y la OEA brindaron apoyo, pero el problema es que no había una línea de comunicación clara entre el gobierno, las empresas afectadas y estos organismos. Se perdió tiempo valioso en la coordinación de esfuerzos. En algunos casos, la información no fluía con la rapidez que se necesitaba, lo que hizo que ciertas soluciones tardaran en aplicarse. Esto evidencia la falta de un marco diplomático claro para gestionar este tipo de crisis de manera más eficiente." (Leitón, 2025).

La entrevistada enfatiza que la falta de claridad en los canales de comunicación interinstitucional generó retrasos en la implementación de soluciones técnicas. Este punto es crucial, ya que evidencia que la diplomacia cibernética no solo implica acceder a ayuda internacional, sino también tener la capacidad de integrarla de manera eficiente dentro del aparato estatal. En este sentido, la falta de un equipo especializado dentro de la Cancillería o del MICITT hizo que la gestión de la crisis dependiera de esfuerzos individuales en lugar de una estrategia previamente definida.

Otro aspecto relevante señalado en la entrevista es la participación de actores privados en la recuperación de la infraestructura digital afectada. Empresas tecnológicas como Microsoft, Cisco y CrowdStrike ofrecieron asistencia técnica, sin embargo, su intervención se dio de manera descoordinada, ya que no existían protocolos formales para la colaboración entre el Estado y el sector privado en situaciones de crisis cibernética. Sobre este tema, Leitón menciona:

> "El sector privado jugó un papel importante en la recuperación, pero hubo falta de coordinación en cómo y cuándo aplicar las soluciones. Muchas de estas empresas estaban dispuestas a ayudar, pero sin una estructura clara dentro del Estado que guiara estas colaboraciones, hubo momentos en que las soluciones tardaron más de lo necesario en implementarse." (Leitón, 2025).

Este punto es clave, ya que confirma un problema recurrente en países con estructuras débiles de ciberdiplomacia: la falta de integración entre gobiernos, sector privado y organismos internacionales. Modelos exitosos como el de la Unión Europea han demostrado que la cooperación público-privada en ciberseguridad es un factor determinante para la efectividad de la respuesta ante incidentes digitales (European Commission, 2020).

Otro elemento crucial mencionado por la entrevistada es la falta de institucionalización de la ciberdiplomacia en Costa Rica. Según su testimonio:

> "No hay un departamento específico que maneje estos temas dentro de la Cancillería. Todo se maneja de manera informal y reactiva, lo que hace que la coordinación sea más lenta. Se necesita un equipo que pueda encargarse exclusivamente de estos temas, con personal capacitado que entienda la dinámica de la ciberseguridad y que tenga acceso a contactos estratégicos en otros países y organismos internacionales." (Leitón, 2025).

Este punto resalta una de las principales debilidades estructurales del país en términos de ciberseguridad: la falta de una unidad especializada en ciberdiplomacia. Países con estructuras más avanzadas en esta materia, como Estados Unidos, Estonia y Alemania, han desarrollado

departamentos específicos dentro de sus ministerios de relaciones exteriores dedicados a la ciberseguridad y la cooperación internacional en este ámbito (Segal, 2016).

En este sentido, Costa Rica se enfrenta al reto de transitar de un enfoque reactivo a una estrategia preventiva y estructurada, donde las relaciones diplomáticas en ciberseguridad no se activen únicamente en momentos de crisis, sino que formen parte de un modelo continuo de cooperación. Leitón sugiere algunas acciones concretas para fortalecer esta área:

> "Debería de haber una cartera de socios en los que se pueda detectar propiamente su rol y que tengamos canales de comunicación directos, que exista alguna especie de grupo de trabajo. No podemos seguir dependiendo de reacciones improvisadas, necesitamos una estrategia clara y estructurada para que, cuando ocurra otro incidente de este tipo, sepamos exactamente qué hacer y con quién comunicarnos." (Leitón, 2025).

En este contexto, se hace evidente la necesidad de crear protocolos estandarizados de cooperación internacional, establecer un equipo especializado en ciberdiplomacia dentro de la Cancillería y desarrollar una política nacional de ciberseguridad que integre la dimensión diplomática.

El caso del ataque a la Caja Costarricense de Seguro Social (CCSS) deja importantes lecciones para el país. Si bien Costa Rica logró acceder a cooperación internacional para mitigar los efectos del ataque, la falta de una estructura formal y de planificación previa redujo la efectividad de esta ayuda. A futuro, el país debe avanzar hacia un modelo de ciberdiplomacia proactiva, basado en alianzas estratégicas sólidas, una mejor coordinación interinstitucional y una integración efectiva con el sector privado.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La ciberdiplomacia ha sido un factor determinante en la capacidad del Estado costarricense para atender los ataques informáticos a la Caja Costarricense del Seguro Social (CCSS) durante el período 2018-2023. A lo largo del estudio, se identificaron diversos aspectos relacionados con el papel de la diplomacia en la cooperación internacional, la asistencia técnica, la formulación de políticas de ciberseguridad y la gestión de crisis. La evidencia recopilada demuestra que, aunque Costa Rica ha logrado establecer lazos estratégicos con actores internacionales clave, persisten deficiencias estructurales que han limitado la efectividad de estas estrategias en la práctica.

Uno de los hallazgos más significativos es que Costa Rica ha abordado la ciberdiplomacia desde un enfoque predominantemente reactivo. Si bien el país ha sido capaz de movilizar apoyo internacional en momentos de crisis, como se evidenció tras el ataque a la Caja Costarricense de Seguro Social (CCSS) en 2022, este respaldo no ha sido suficiente para garantizar una recuperación ágil ni una mejora sustancial en la capacidad de prevención de futuros ataques. La falta de una estrategia diplomática formal en ciberseguridad ha dificultado la consolidación de alianzas estratégicas a largo plazo y ha generado incertidumbre en la gestión de incidentes cibernéticos a nivel estatal.

El análisis de las estrategias de ciberdiplomacia implementadas por el Estado costarricense evidencia que, si bien se han dado avances en la cooperación con organismos como la Organización de los Estados Americanos (OEA), el FBI y agencias de ciberseguridad extranjeras, estos esfuerzos han sido fragmentados y carecen de continuidad. La inexistencia de una estructura diplomática especializada en ciberseguridad ha impedido la creación de un marco estable que garantice el desarrollo de capacidades nacionales de forma progresiva. La ausencia de protocolos claros y de un equipo técnico-diplomático encargado de gestionar relaciones internacionales en materia de seguridad cibernética ha hecho que la respuesta a los ciberataques dependa de la improvisación y la gestión individual de cada institución afectada.

A nivel internacional, el estudio confirma que la ciberdiplomacia ha sido un recurso clave para los Estados que buscan fortalecer su seguridad digital mediante la cooperación con aliados estratégicos. Países con una estructura formal en ciberdiplomacia han logrado integrar estos esfuerzos en sus políticas exteriores, consolidando mecanismos de respuesta más eficientes. En el caso costarricense, la falta de una visión integral en la diplomacia digital ha generado una dependencia de terceros en momentos de crisis, sin que esto se traduzca en una reducción de la vulnerabilidad del país ante ataques futuros.

La identificación de los actores internacionales clave en la gestión del ataque a la Caja Costarricense de Seguro Social (CCSS) permitió comprender el papel que desempeñan organismos multilaterales, agencias de inteligencia y empresas del sector privado en la respuesta ante incidentes de ciberseguridad. A pesar de la valiosa asistencia brindada por entidades como la OEA y el FBI, la falta de coordinación interna dentro del aparato estatal costarricense redujo la efectividad de esta ayuda. En varias ocasiones, las soluciones técnicas proporcionadas por aliados internacionales fueron implementadas con retraso debido a la carencia de mecanismos administrativos adecuados para facilitar su integración.

La participación del sector privado en la gestión de la crisis cibernética fue otro aspecto relevante identificado en la investigación. Empresas como Microsoft y Cisco desempeñaron un papel crucial en la restauración de los sistemas de la Caja Costarricense de Seguro Social (CCSS), lo que resalta la importancia de establecer alianzas público-privadas en el ámbito de la ciberseguridad. Sin embargo, la falta de una estrategia gubernamental clara impidió que esta colaboración se llevara a cabo de manera ordenada y eficiente. La inexistencia de protocolos definidos para la integración del sector privado en la gestión de incidentes cibernéticos resultó en demoras y complicaciones innecesarias en la implementación de soluciones tecnológicas.

Un aspecto crítico identificado en el estudio es que Costa Rica carece de un marco normativo robusto que regule la ciberdiplomacia como un pilar fundamental de su política exterior. Mientras que países líderes en ciberseguridad han adoptado legislaciones específicas que formalizan la cooperación internacional en la gestión de amenazas digitales, Costa Rica aún no ha desarrollado una legislación integral en esta materia. La adhesión al Convenio de Budapest representa un avance en términos de ciberseguridad, pero no es suficiente para consolidar un

enfoque diplomático sólido que permita al país fortalecer sus capacidades de prevención, detección y respuesta ante ciberataques.

El estudio también reveló que la efectividad de las estrategias de ciberdiplomacia en Costa Rica ha sido limitada debido a la falta de inversión en formación y capacitación de funcionarios públicos en temas de ciberseguridad y relaciones internacionales digitales. A pesar de que la cooperación internacional ha permitido acceder a conocimientos técnicos avanzados, estos no han sido incorporados de manera sistemática en las instituciones del Estado. La falta de cuadros especializados en diplomacia digital ha dificultado la implementación de acuerdos de cooperación y ha generado una dependencia excesiva de actores externos en la formulación de estrategias de seguridad cibernética.

Otro factor determinante en la evaluación de la efectividad de la ciberdiplomacia en Costa Rica ha sido la fragmentación institucional en la gestión de incidentes cibernéticos. La inexistencia de una entidad centralizada que coordine la respuesta a ciberataques ha dado lugar a una toma de decisiones desarticulada y a la ausencia de un liderazgo claro en la materia. Esta fragmentación ha generado una serie de dificultades administrativas que han ralentizado la capacidad de respuesta del Estado ante crisis cibernéticas.

El análisis de la crisis de 2022 en la Caja Costarricense de Seguro Social (CCSS) evidenció que la ciberdiplomacia costarricense carece de una estructura formalizada y de protocolos establecidos para canalizar la asistencia internacional de manera eficiente. La respuesta al ataque fue gestionada a través de múltiples actores sin una coordinación clara, lo que derivó en retrasos y dificultades en la implementación de soluciones tecnológicas. Si bien la cooperación internacional fue un factor clave en la recuperación de los sistemas afectados, la falta de preparación interna limitó su impacto y redujo la efectividad de las medidas adoptadas.

El estudio también reveló que Costa Rica no cuenta con mecanismos de monitoreo y evaluación que permitan medir la efectividad de su ciberdiplomacia en la gestión de crisis. La ausencia de indicadores de desempeño y de un sistema de seguimiento impide determinar con precisión el impacto de las estrategias diplomáticas implementadas en el ámbito de la ciberseguridad. La falta de evaluación sistemática limita la capacidad del país para identificar

áreas de mejora y ajustar su política exterior digital en función de las lecciones aprendidas en eventos pasados.

A modo de cierre, la ciberdiplomacia ha sido un elemento determinante en la respuesta costarricense a los ciberataques, pero su efectividad ha estado condicionada por la falta de planificación estratégica, la ausencia de una estructura formal en Cancillería, la escasa capacitación de funcionarios y la fragmentación institucional.

5.2 Recomendaciones

La ciberdiplomacia en Costa Rica requiere un fortalecimiento estructural que garantice una respuesta más efectiva ante ciberataques futuros. Es fundamental que el país transite de un enfoque reactivo a uno preventivo, mediante la institucionalización de una estrategia de diplomacia digital que facilite la cooperación internacional y la gestión coordinada de incidentes cibernéticos. Para ello, se recomienda la creación de una unidad especializada en ciberdiplomacia dentro del Ministerio de Relaciones Exteriores y Culto (MREC), con personal capacitado en ciberseguridad y relaciones internacionales. Este equipo debe encargarse de gestionar acuerdos internacionales, participar en foros multilaterales y establecer protocolos de cooperación con otros Estados y organismos especializados en seguridad digital.

La falta de un marco normativo claro en materia de ciberdiplomacia ha limitado la capacidad de Costa Rica para consolidar alianzas estratégicas a largo plazo. Es necesario desarrollar un marco legal integral que formalice la cooperación internacional en ciberseguridad, incluyendo la adhesión a tratados multilaterales, acuerdos bilaterales de asistencia técnica y protocolos para la colaboración público-privada en la gestión de incidentes cibernéticos. Este marco normativo debe contemplar la creación de mecanismos de comunicación interinstitucional que faciliten la coordinación entre entidades nacionales e internacionales, permitiendo una respuesta más eficiente y estructurada ante ataques informáticos.

La respuesta costarricense ante el ataque a la Caja Costarricense de Seguro Social (CCSS) en 2022 evidenció la necesidad de contar con protocolos de comunicación más eficientes. Para ello, se recomienda la implementación de un protocolo interinstitucional de

respuesta a ciberataques, que defina las líneas de acción en casos de crisis y establezca los canales de comunicación entre instituciones estatales, organismos internacionales y actores privados. Este protocolo debe estar respaldado por simulacros y ejercicios de ciberseguridad que permitan evaluar la capacidad de respuesta del país y corregir debilidades en la gestión de crisis digitales.

El fortalecimiento de la ciberdiplomacia en Costa Rica no solo depende de la institucionalización de su marco legal y organizativo, sino también del desarrollo de capacidades técnicas en los funcionarios públicos encargados de gestionar estos temas. Se recomienda la creación de programas de formación en ciberseguridad y diplomacia digital de parte de la academia diplomática Manuel María de Peralta, dirigidos a diplomáticos, oficiales de seguridad y tomadores de decisión dentro del aparato estatal. Estas capacitaciones deben incluir módulos sobre gestión de crisis cibernéticas, negociación en incidentes de seguridad digital y cooperación internacional en materia de ciberdefensa.

El sector privado desempeña un papel crucial en la respuesta ante incidentes cibernéticos, pero la falta de una estrategia gubernamental clara ha dificultado la integración efectiva de las empresas tecnológicas en la gestión de crisis. Se recomienda la creación de una mesa de trabajo permanente entre el Estado y el sector privado, donde se definan estrategias conjuntas de prevención y respuesta ante ciberataques. Este mecanismo permitiría mejorar la colaboración público-privada y garantizar una coordinación más eficiente en la implementación de soluciones tecnológicas en momentos de crisis.

Para asegurar que las estrategias de ciberdiplomacia sean efectivas, es necesario implementar indicadores de evaluación que permitan medir su impacto en la seguridad digital del país. Se recomienda desarrollar mecanismos de monitoreo y evaluación que midan la efectividad de la cooperación internacional en ciberseguridad, asegurando que los acuerdos firmados y la asistencia recibida generen mejoras concretas en la protección de infraestructuras críticas y la gestión de incidentes cibernéticos.

El fortalecimiento de la cultura de ciberseguridad dentro de las instituciones estatales es otro aspecto clave para reducir la vulnerabilidad ante ataques informáticos. Se recomienda que

todas las entidades públicas adopten protocolos de seguridad cibernética obligatorios, incluyendo auditorías periódicas, simulacros de ataque y planes de contingencia específicos para incidentes de ransomware. Esto permitiría garantizar que los sistemas gubernamentales estén preparados para responder de manera efectiva a amenazas digitales y reducir el impacto de futuros ciberataques.

El desarrollo de una estrategia integral de ciberdiplomacia en Costa Rica debe ser un esfuerzo multisectorial que involucre tanto al Estado como a la academia y al sector privado. Se recomienda a la Universidad Internacional de las Américas que se incorporen en sus planes de estudio de Relaciones Internacionales cursos sobre ciberdiplomacia y ciberseguridad, con el fin de formar profesionales capacitados en la intersección entre seguridad digital y diplomacia. Además, se debe fomentar la investigación en estos temas mediante la promoción de estudios académicos sobre la cooperación internacional en ciberseguridad y su impacto en la gobernanza global del ciberespacio.

La investigación sobre ciberdiplomacia en Costa Rica aún tiene múltiples áreas por explorar, por lo que se recomienda que futuros estudios amplíen el análisis de la diplomacia digital en otros sectores estratégicos, como la infraestructura energética y los sistemas financieros. Además, sería valioso realizar estudios comparativos con otros países de América Latina para identificar buenas prácticas en la implementación de estrategias de ciberdiplomacia y evaluar su aplicabilidad en el contexto costarricense.

El país debe avanzar hacia una ciberdiplomacia proactiva que garantice una mayor resiliencia ante amenazas digitales y una mejor integración en el ecosistema global de seguridad cibernética. La implementación de estas recomendaciones permitirá a Costa Rica fortalecer su capacidad de respuesta ante ciberataques, consolidar alianzas estratégicas con actores internacionales y garantizar la protección de su infraestructura crítica en un mundo cada vez más interconectado.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2019). *El proyecto de investigación: Introducción a la metodología científica.* Editorial Episteme.

Arias, P. (2021). Diplomacia costarricense y ciberseguridad: Estrategias y desafíos. *Revista del Ministerio de Relaciones Exteriores, 45*(2), 67-89.

Azubuike, C. F. (2023). Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks.

Bartolome, M. C. (2021). *El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea y la Organización de Estados Americanos*. Recuperado de https://www.academia.edu

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28(2), 347-362.

Borghard, E., & Lonergan, S. (2021). The Logic of Coercion in Cyberspace. Security Studies, 30(2), 170-198.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Caja Costarricense de Seguro Social. (2022). *Evaluación de asistencia internacional en la respuesta al ataque cibernético*(Informe AS-AATIC-093-2022). CCSS.

Caja Costarricense de Seguro Social. (2022). *Evaluación de vulnerabilidades y respuesta al ciberataque* (Informe AD-ATIC-067-2022). CCSS.

Caja Costarricense de Seguro Social. (2022). *Informe de auditoría interna sobre el ciberataque a la CCSS* (Informe AD-ATIC-039-2022). CCSS.

Caja Costarricense de Seguro Social. (2023). *Informe de seguimiento sobre ciberseguridad y cooperación internacional*(Informe AS-ATIC-090-2023). CCSS.

Caja Costarricense de Seguro Social. (2023). *Auditoría de infraestructura digital y estrategias de seguridad post-ataque*(Informe AS-ATIC-006-2023). CCSS.

Caja Costarricense de Seguro Social. (2022). *Análisis forense y medidas de recuperación tras el ataque cibernético*(Informe AS-AATIC-174-2022). CCSS.

CCSS (2023). *Informe de seguridad digital y medidas implementadas tras el ataque de 2022*. Caja Costarricense de Seguro Social.

CETES. (2023). *Evaluación de la Estrategia Nacional de Ciberseguridad 2018-2023*. Heredia, Costa Rica: Universidad Nacional.

Chacón, F. (2013). *Ataques cibernéticos en Costa Rica: Evaluación y respuesta gubernamental*. Revista de Seguridad Digital, 5(2), 45-58.

Chertoff, M., & Simon, T. (2018). *The impact of the dark web on internet governance and cyber security*. Global Commission on Internet Governance.

CISA (2022). *Healthcare Cybersecurity: Risks and Best Practices*. Cybersecurity and Infrastructure Security Agency.

CNE (2022). *Infraestructuras críticas en Costa Rica: evaluación y estrategias de protección*. Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.

Consejo de Europa (2020). *Budapest Convention on Cybercrime*. Disponible en: https://www.coe.int

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. https://www.coe.int/en/web/cybercrime

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage Publications.

DAN, V., & PANDEY, M. (2020). Cyber-Security Threats In International Relation: The Implications of Cyber Threats on State Sovereignty, National Security, and International Cooperation, Focusing on Recent Cyber Incidents.

Deibert, R. (2019). *The road to digital unfreedom: Three painful truths about social media*. Journal of Democracy, 30(1), 25-39.

Denning, D. E. (1989). *Computers Under Attack: Intruders, Worms, and Viruses*. ACM Press.

ENISA (2021). *Cyber Threats to the Healthcare Sector*. European Union Agency for Cybersecurity.

European Commission. (2020). *Cyber Diplomacy in the European Union: A Joint Strategy.* Brussels: European Commission.

Europol (2022). *Ransomware Threat Landscape 2022: The Rise of Double Extortion Attacks*.

Flick, U. (2015). *An Introduction to Qualitative Research.* SAGE Publications.

G20. (2018). *G20 Leaders' Declaration: Building Consensus for Fair and Sustainable Development*.

GFCE. (2020). *Annual Report 2020*.

Global Forum on Cyber Expertise (2021). *Annual Report on Cyber Capacity Building*. Disponible en: https://www.thegfce.org

Gobierno de Costa Rica (2022). *Declaratoria de emergencia nacional por ciberataques: Decreto Ejecutivo N° 42542-MP*.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Guitton, C. (2020). Balancing the Risks of Cyber Operations. Journal of Strategic Studies, 43(1), 42-64.

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación.* McGraw-Hill Education.

ICE. (2019). *Cooperación en ciberseguridad: La experiencia de Costa Rica con la OEA*. San José, Costa Rica: Instituto Costarricense de Electricidad.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Krueger, R., & Casey, M. A. (2015). *Focus Groups: A Practical Guide for Applied Research*. SAGE.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer.

Kvale, S. (2007). *Doing Interviews*. Sage Publications.

La Nación. (2022, 4 de julio). *Hackeo a CCSS obligó a cancelar casi 80.000 citas médicas en un mes*. La Nación. Recuperado de https://www.nacion.com/el-pais/salud/hackeo-a-ccss-obligo-a-cancelar-casi-80000-citas/MVIQHOZ2WNFGVJXYIOXXPEWPDI/story/

Langner, R. (2011). *Stuxnet: Dissecting a Cyberwarfare Weapon*. IEEE Security & Privacy.

Lewis, J. (2018). *Cybersecurity and International Cooperation.* Washington, D.C.: Center for Strategic and International Studies (CSIS).

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

MICITT. (2017). Estrategia Nacional de Ciberseguridad de Costa Rica 2017-2021. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

MICITT. (2017). *Informe sobre gobernanza digital y estrategias de ciberseguridad en Costa Rica*. Ministerio de Ciencia, Tecnología y Telecomunicaciones.

MICITT. (2022). Estrategia Nacional de Ciberseguridad 2023-2027. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

MICITT. (2022). *Informe sobre la respuesta a los ciberataques a la Caja Costarricense del Seguro Social (CCSS)*. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

MICITT (2022). *Ciberseguridad en Costa Rica: acciones y estrategias frente a los ciberataques de 2022*. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

Morales, A. (2018). *Impacto de los ataques de phishing en la banca costarricense: Casos de estudio entre 2016 y 2017*. Revista Costarricense de Tecnología, 8(1), 22-37.

Morgenthau, H. (1948). *Politics Among Nations: The Struggle for Power and Peace*. A. A. Knopf.

Naciones Unidas (2021). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Disponible en: https://www.un.org

NATO. (2019). *Cyber Defence Policy of NATO*. https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2020). *Cyber Defence*. Recuperado de https://www.nato.int/cyberdefence

NATO. (2020). *NATO Cybersecurity Cooperation Report.* Brussels: NATO Press.

NATO (2021). *Cyber Defence Pledge: Progress Report*. North Atlantic Treaty Organization.

Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace*. International Security, 41(3), 44-71.

OEA. (2018). *Estrategia de Ciberseguridad de las Américas*.

OEA. (2019). *Informe sobre Seguridad Cibernética en las Américas*.

OEA. (2020). Informe de Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Organización de los Estados Americanos.

OEA. (2020). *Informe sobre la ciberseguridad en las Américas*. Organización de los Estados Americanos.

OEA. (2023). *Estrategia Interamericana de Ciberseguridad*. Recuperado de https://www.oas.org/es/seguridad/ciberseguridad

OEA (2022). *Marco de Ciberseguridad en América Latina y el Caribe: Avances y Desafíos*. Organización de los Estados Americanos.

ONU. (2015). *Resolutions on Cybersecurity and International Security*.

ONU. (2021). *The Future of Cybersecurity: UN Proposals for a Secure Digital World*.

OPS (2023). *Informe sobre la digitalización del sector salud en Costa Rica y su impacto en la prestación de servicios médicos*. Organización Panamericana de la Salud.

Organización de los Estados Americanos (2022). *Marco Interamericano de Ciberseguridad*. Disponible en: https://www.oas.org

Organización del Tratado del Atlántico Norte (OTAN). (1949). *Tratado del Atlántico Norte* (Tratado de Washington). Recuperado de https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence.

Pernik, P. (2018). *Cybersecurity and NATO's Cyber Defense Strategy*. NATO CCDCOE Publications.

Ramírez, M. (2021). Diplomacia digital en América Latina: Desafíos y oportunidades. *Revista de Relaciones Internacionales, 23*(2), 78-93.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.

Rid, T. (2020). *Cyber War Will Not Take Place*. Oxford University Press.

Rodríguez, J. (2017). *Fraudes electrónicos en Costa Rica: Un análisis del impacto en el sistema financiero nacional*. Banco de Costa Rica.

Sánchez, L. (2020). Ciberseguridad y diplomacia en Costa Rica: Retos y perspectivas. *Revista de Ciencias Políticas, 35*(1), 123-145.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Taylor, S. J., Bogdan, R., & DeVault, M. (2016). *Introduction to Qualitative Research Methods: A Guidebook and Resource.* John Wiley & Sons.

Taylor, S. J., Bogdan, R., & DeVault, M. (2016). *Introduction to Qualitative Research Methods: A Guidebook and Resource*. Wiley.

Tikk, E., & Kerttunen, M. (2020). *International Cyber Norms: Legal, Policy & Industry Perspectives*.

United Nations. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Naciones Unidas.

United Nations. (2022). *Report of the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security*. United Nations General Assembly.

United Nations. (2022). *UN Cybersecurity Working Group Report.* New York: UN Publications.

Unión Internacional de Telecomunicaciones. (2020). *Índice Global de Ciberseguridad 2020*. UIT.

Waltz, K. N. (1979). *Theory of International Politics*. Addison-Wesley.

WHO (2022). *Guidelines on Digital Health Security and Cyber Resilience in Healthcare Systems*. World Health Organization.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

ANEXOS

Anexo 1: Definición de términos utilizados en el estudio.

Acrónimo	Significado
CCSS	Caja Costarricense de Seguro Social
CISA	Cybersecurity and Infrastructure Security Agency (Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU.)
CICTE	Comité Interamericano contra el Terrorismo (OEA)
CNE	Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (Costa Rica)
CSIRT	Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)
ENISA	European Union Agency for Cybersecurity (Agencia de la Unión Europea para la Ciberseguridad)
FBI	Federal Bureau of Investigation (Buró Federal de Investigaciones de EE.UU.)
GFCE	Global Forum on Cyber Expertise (Foro Global sobre Ciberexperticia)
G20	Grupo de los Veinte (Foro de cooperación económica internacional)
ICE	Instituto Costarricense de Electricidad
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Costa Rica)
NATO/OTAN	North Atlantic Treaty Organization / Organización del Tratado del Atlántico Norte
OEA	Organización de los Estados Americanos
ONU	Organización de las Naciones Unidas
OPS	Organización Panamericana de la Salud
UE	Unión Europea
UN GGE	United Nations Group of Governmental Experts (Grupo de Expertos Gubernamentales de la ONU sobre Ciberseguridad)

WHO/OMS	World Health Organization / Organización Mundial de la Salud

Fuente: Elaboración propia.

Anexo 2: Cuestionario 1. Paula Brenes Ramírez, Presidenta de la Fundación YoD y exdirectora de Gobernanza Digital en el MICITT.

1. Desde su perspectiva, ¿cuáles fueron las principales acciones o estrategias que lideró el MICITT para enfrentar el ciberataque a la Caja Costarricense del Seguro Social (CCSS)?
2. ¿Cómo valora la efectividad de la cooperación internacional (por ejemplo, con otros Estados u organizaciones) que se gestionó desde el MICITT durante y después del ataque?
3. ¿Considera usted que la intervención diplomática internacional facilitó una respuesta técnica más efectiva al ciberataque? ¿Por qué?
4. ¿Qué mecanismos de colaboración con actores internacionales fueron más efectivos para contener o mitigar los efectos del ataque a la CCSS?
5. A partir de la experiencia del ataque a la CCSS, ¿qué debilidades en la infraestructura y la gestión de ciberseguridad fueron más evidentes?
6. Desde el MICITT, ¿se impulsaron nuevas políticas o reformas tras el ataque que hayan reforzado la capacidad de respuesta del Estado? ¿Cuáles?
7. ¿Qué lecciones aprendidas destacaría el MICITT para futuras situaciones similares y cómo considera que la diplomacia internacional puede contribuir a mejorar la respuesta estatal?

Anexo 3: Cuestionario 2. Jazmín Esquivel Vega, Consejera y Cónsul en el Consulado General de Costa Rica en Atlanta, Georgia.

1. Desde su experiencia en la Cancillería, ¿cómo valora el trabajo que ha realizado el Ministerio de Relaciones Exteriores para fortalecer la diplomacia digital y responder efectivamente a ciberataques que pueda recibir el Estado en el futuro?
2. Desde su experiencia profesional, considera que la ciberseguridad es un tema recurrente en la diplomacia costarricense? Es decir, se busca constantemente cerrar acuerdos de cooperación que permitan fortalecer la capacidad del Estado para responder ante futuros ataques informáticos?
3. En su opinión, ¿qué tan preparado está Costa Rica, desde el ámbito diplomático, para enfrentar incidentes cibernéticos que comprometen la seguridad nacional?
4. ¿Considera que existen suficientes canales diplomáticos establecidos para una rápida asistencia internacional en ciberseguridad? ¿Podría mencionar algunos ejemplos concretos?
5. ¿Cuál cree que debe ser el papel del Ministerio de Relaciones Exteriores en la formulación de políticas de ciberseguridad y cooperación internacional?
6. ¿Desde su perspectiva, ¿qué recomendaciones haría para fortalecer la diplomacia costarricense frente a futuros ciberataques, especialmente en la protección de infraestructura crítica?

Anexo 4: Cuestionario 3. Yuliana Leitón Álvarez, Especialista en Ciberseguridad en el Banco Nacional de Costa Rica.

1. Desde su experiencia, ¿cuál considera que fue el impacto del ciberataque a la CCSS para la seguridad cibernética en Costa Rica?
2. ¿Qué mecanismos de cooperación o comunicación se establecieron durante o después del ataque?
3. ¿Considera que las alianzas internacionales ayudaron de alguna forma a compartir información sobre amenazas o a mitigar riesgos?
4. Desde su perspectiva, ¿qué tan efectiva fue la respuesta del Estado costarricense en términos de ciberseguridad tras el ataque a la CCSS?
5. ¿Qué papel considera que juega la diplomacia internacional en el fortalecimiento de las capacidades nacionales de ciberseguridad?
6. ¿Qué mejoras recomendaría en los protocolos de respuesta y colaboración público-privada en casos de ciberataques que afectan infraestructuras críticas?