Universidad Siglo 21

Trabajo Final de Grado. Manuscrito Científico

Licenciatura en Relaciones Internacionales

Cooperación entre la OEA y el Mercosur en materia de seguridad cibernética electoral (2014-2019)

Cooperation between the OAS and Mercosur in matters of electoral cybersecurity (2014-2019)

Carolina Elin Córdoba *VRIN00724*

Tutora: Maria Iness Sesma

Córdoba, Noviembre 2019

Índice

Resumen

En el presente Trabajo Final de Grado se analizó la cooperación llevada a cabo por la Organización de Estados Americanos (OEA) y los países miembros del Mercosur (Argentina, Brasil, Paraguay y Uruguay) en relación a la seguridad cibernética en los procesos electorales durante el período 2014-2019. En el marco de las Relaciones Internacionales y desde la perspectiva de la teoría neoinstitucionalista, se detalló la cooperación internacional en el campo de la ciberseguridad. A partir de una metodología cualitativa de tipo longitudinal, se priorizó la descripción de amenazas cibernéticas, actores y estrategias llevadas a cabo para hacer frente a los desafíos que derivan de la utilización de nuevas tecnologías de información y comunicación en las diferentes etapas de los procesos electorales. Se destacó la vulnerabilidad de la infraestructura electoral y la propagación de noticias falsas como generadoras de desconfianza en el electorado. Por lo tanto, la seguridad cibernética, en la agenda de los países, busca generar confianza en los ciudadanos y garantizar los derechos políticos electorales en las democracias. Sin embargo, a la luz de los resultados, se evidenció la carencia de políticas que regulen las actividades en el ciberespacio y la necesidad de adecuarse a las nuevas amenazas que socavan la credibilidad de los procesos democráticos.

Palabras Claves: Sistema electoral – Seguridad del Estado – Protección de datos – Cooperación internacional.

Abstract

In this Final Degree Project, the cooperation carried out by the Organization of American States (OAS) and the member countries of Mercosur (Argentina, Brazil, Paraguay and Uruguay) in relation to cybersecurity in electoral processes during the period 2014-2019. Within the framework of International Relations and from the perspective of neo-institutional theory, international cooperation in the field of cybersecurity was detailed. Based on a qualitative longitudinal methodology, the description of cyber threats, actors and strategies carried out to face the challenges arising from the use of new information and communication technologies in the different stages of electoral processes was prioritized. . The vulnerability of the electoral infrastructure and the spread of false news were highlighted as generators of distrust in the electorate. Therefore, cybersecurity, on the agenda of the countries, seeks to generate trust in citizens and guarantee electoral political rights in democracies. However, in light of the results, the lack of policies that regulate activities in cyberspace and the need to adapt to new threats that undermine the credibility of democratic processes was evidenced.

Keywords: Electoral systems – State segurity – Data protection – International cooperation.

Introducción

La utilización de Tecnologías de Información y Comunicación (TIC) se ha vuelto cada vez más frecuente en los últimos años. Las computadoras, teléfonos inteligentes y otros dispositivos similares han revolucionado la vida cotidiana ofreciendo nuevas oportunidades como así también desafíos. La información a la que podemos acceder puede ser manipulada o pirateada sin las medidas de seguridad cibernética adecuadas. Los Estados no son ajenos a la utilización de tecnología, cada vez son más las aéreas donde se implementan avances tecnológicos, lo que acrecienta los desafíos y vulnerabilidades. Las TIC ofrecen ventajas y desventajas a las democracias. Por un lado, permite a los políticos y candidatos acercarse a los ciudadanos a través de las redes sociales, comunicar noticias oficiales y hasta votar electrónicamente durante el proceso electoral. Por otro lado, la utilización de tecnología sin la salvaguarda correspondiente puede ser abusada. Esto genera inconvenientes cuando la información o los procesos electorales son objetivos de ciberataques para influir indebidamente en las elecciones democráticas. La ciberseguridad se relaciona con la protección de sistemas y datos conectados a internet, también se usa aquí para incluir la seguridad de las tecnologías electorales fuera de línea y proteger la integridad del proceso electoral de las operaciones de desinformación e influencia. Si la seguridad cibernética no está garantizada, en lugar de facilitar la comunicación entre ciudadanos y políticos y crear confianza en el proceso electoral, las TIC pueden utilizarse para fomentar la desconfianza en las instituciones y procesos democráticos.

Por otra parte, las elecciones periódicas son una característica intrínseca de aquellos países que han elegido la democracia como forma de gobierno. Defender la conducción de elecciones genuinas y periódicas es una obligación de derecho internacional para esas naciones. Ciertas garantías democráticas son vinculantes para los miembros de Naciones Unidas y pueden describirse como compromisos legales fundamentales que requieren elecciones libres y justas que se celebren regularmente (García San José, 2006). Estas garantías se enuncian en el Artículo 21 de la Declaración Universal de Derechos Humanos de 1948 y en el Artículo 25 del Pacto Internacional de Derechos Civiles y Políticos de 1966. Otros componentes importantes, articulados en la Carta Interamericana Democrática de 2001, incluyen las libertades personales y políticas, el estado de derecho, la protección de los derechos humanos y la participación permanente de los ciudadanos en la política.

Los ataques cibernéticos en los procesos electorales no solo vulneran los procesos democráticos sino también los derechos políticos de los ciudadanos. Hasta hace poco era difícil de creer que se pudiera influir en las elecciones perturbando su realización mediante ciberataques o condicionando el voto de los ciudadanos mediante operaciones de desinformación y propagación de noticias falsas. Sin embargo, esto ocurrió en las elecciones presidenciales de Estados Unidos en 2016 y en las legislativas de 2018, donde se registraron operaciones de influencia cibernéticas en la proximidad de las elecciones y disparó la fragilidad de los sistemas electorales (Arteaga, 2011). En este caso, la consultora *Cambridge Analytical* compró datos privados de los usuarios de *Facebook*, sin su consentimiento, y se estima que pudieron utilizarse para influir en los resultados electorales de Estados Unidos y el referendo del *Brexit* (BBC, 2019). Es importante hacer mención de este hecho ya que

sentó un precedente importante sobre la necesidad de proteger los datos en línea, creando mayor conciencia y atención sobre el tema.

El mundo cibernético constituye un nuevo campo e implica una nueva forma de la relación en la esfera internacional. Por lo tanto, desde el punto de vista de las relaciones internacionales, la ciberseguridad cobra relevancia en cuanto supone un nuevo paradigma a escala global donde las estrategias y la cooperación se convierten en prioridades de agendas estatales para proteger los derechos democráticos y lograr el progreso a través de las TIC. La dinámica de este fenómeno desafía a la comunidad internacional en la búsqueda de una respuesta coordinada. Por lo tanto, demanda un estudio detallado para reconocer las amenazas que ponen en peligro los procesos electorales a nivel global. Es preciso aclarar que, si bien es factible fortalecer los sistemas para evitar o estar preparados ante una amenaza, los ciberataques tienen las características de ser de bajo costo, difícilmente rastreables y es muy poco probable atribuir su autoría. Se sabe que hay gobiernos que contratan a *hackers* para que realicen acciones en favor de sus intereses, pero es muy probable que estos actores no estén en el territorio de esos Estados (Leiva, 2015). Las amenazas cibernéticas en los procesos electorales abarcan actos hostiles o ilegales diseñados para socavar la integridad de las elecciones. Estos incluyen ataques contra la infraestructura destinados a violar la confidencialidad, integridad y disponibilidad de datos relacionados con las elecciones (Banghart, 2018). Con respecto a las redes sociales y publicaciones online, son utilizadas para socavar la credibilidad de las campañas mediante noticias falsas y ataques masivos contra partidos políticos, candidatos o personas públicas. El objetivo final de la seguridad cibernética es brindar certeza y confianza a los ciudadanos en todas las instancias del proceso electoral, “aunque no es el único elemento que contribuye a generar

confianza, sí resulta básica en un ambiente cada vez más apalancado por la tecnología" (Mendoza, 2018).

Los ciberataques exploran vulnerabilidades técnicas o crean la percepción de que tales vulnerabilidades existen. Estos pueden estar dirigidos directamente a la tecnología de la elección o a las campañas de desinformación. El primer punto incluye registro de votantes, votación electrónica, conteo, transmisión y agregación de resultados, sitios online, cuentas de correo institucionales y privadas, inclusive los sistemas de red eléctrica y enlaces de comunicación. El segundo punto hace referencia, por un lado, a operaciones online de información falsa que intentan manipular la participación electoral (Bradshaw, Howard, 2019) y por otro lado, socavar las percepciones de integridad en los procesos, instituciones y tecnologías electorales, difundiendo manipulación y malversación de datos (Wolf 2017).

En la actualidad, los países y organizaciones trabajan de manera conjunta para hacer frente a las nuevas amenazas y la seguridad cibernética es uno de los mayores desafíos. Aludiendo específicamente a América Latina, solo seis Estados han diseñado una Estrategia de Ciberseguridad en colaboración con la OEA. Estos son México, Colombia, Panamá, Paraguay, Chile y Costa Rica. Según Leiva (2015) esto se debe a dos factores que bloquean la adopción de políticas de seguridad cibernética en el resto de los países, por un lado la falta de recursos y por otro lado la carencia de experiencia práctica y conocimientos especializados para diseñar este tipo de medidas. No obstante, la Organización de Estados Americanos (OEA) ha estado comprometida en delincuencia y seguridad cibernética por más de una década, fomentando la labor de los Estados Miembros para fortalecer su capacidad de proteger a las personas, economías e infraestructura de los ciberataques. En 2004 se aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la

Seguridad Cibernética, que promovía el esfuerzo coordinados de los Estados Miembros en la lucha contra las amenazas cibernéticas en la región y suministraba un marco inicial para guiar el enfoque. Esto permitió crear un espacio de cooperación significativo, aumentando el intercambio de información y mejorando la protección de la infraestructura de las TIC. Además, fortaleció la capacidad de los gobiernos para responder amenazas cibernéticas. Estos compromisos se han reafirmado con los años, en la declaración del año 2016, se afirmo el papel y las responsabilidades de la OEA y los Estados Miembros en la promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica. El Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la OEA colabora con los Estados Miembros elaborando estrategias de ciberseguridad nacional y brinda capacitación a los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacional y regionales. Este programa, también facilita ejercicios de gestión de crisis con operadores de la industria nacional crítica y los activos de respuesta a emergencias, la sociedad civil y el sector privado. El CICTE contribuye de muchas maneras para crear conciencia sobre las amenazas y las oportunidades relacionadas con la ciberseguridad regional (BID, OEA 2016).

Ningún país está exento de los ataques cibernéticos en el ámbito electoral, el principal riesgo se encuentra en el sistema de votación y en las noticias falsas que constituyen una amenaza real al proceso electoral. Según el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA), 32 países incluyeron la tecnología en su sistema electoral para volverlos más ágiles y garantizar transparencia en sus procesos electorales (Miranda, 2018). En los países del Mercosur, solo Brasil aplica voto electrónico en todo su territorio y Argentina en las provincias de Salta y Neuquén y en algunos

municipios del resto del país. Paraguay, en cooperación con la OEA, implementará el voto electrónico para las elecciones de 2020 (Bestard, 2019) y en Uruguay se utiliza la boleta de papel. Como se mencionó anteriormente, el voto electrónico no es el único mecanismo que incorpora tecnología; el registro de votantes, la transmisión de datos y el escrutinio pueden verse afectados. Por lo tanto, aquellos países del Mercosur que aún no implementan el voto electrónico en todo su territorio pueden ver vulnerado alguna otra etapa del proceso electoral. La necesidad de cooperación es evidente, en un ámbito donde la tecnología de la información evoluciona al igual que las vulnerabilidades. Las elecciones dependen de diversas combinaciones de procedimientos manuales y tecnológicos. Actualmente, no existe una tecnología inaccesible ni procesos manuales totalmente a prueba de manipulaciones. Por lo tanto, la ciberseguridad electoral implica la gestión y mitigación de los riesgos a través de medidas de integridad, auditoría y control.

El papel de la OEA en la colaboración cibernética para fortalecer los procesos electorales ha llevado a generar una serie de interrogantes: ¿Cómo pueden influir los ciberataques en el proceso electoral? ¿Qué actores están involucrados en la implementación de seguridad cibernética? ¿Qué herramientas ofrece la OEA para la cooperación regional en ciberseguridad electoral? ¿Los países del Mercosur están preparados para afrontar un ataque cibernético en las elecciones?

En relación a las preguntas planteadas, en el párrafo anterior, resulta central para esta investigación analizar la cooperación de la OEA en ciberseguridad desde el marco de la teoría neoinstitucionalista de las relaciones internacionales para ofrecer una respuesta a los interrogantes mencionados. Las amenazas cibernéticas que presentan los países miembros del proceso de integración regional del Mercosur (Argentina, Brasil, Uruguay y Paraguay) y

las medidas llevadas a cabo, serán negociadas y ejecutadas con mucha más eficiencia dentro de un régimen institucionalizado que permite el intercambio y una equilibrada distribución de la información. Siguiendo la teoría neoinstitucionalista, los regímenes, deben percibirse como acuerdos promovidos desde el auto interés en un sistema donde la soberanía es el elemento constitutivo de los Estados. Según Keohane, los regímenes no dictan lo que deben hacer los Estados sino que sirven de espacio para que los actores ajusten su comportamiento, a las expectativas de otros, mediante la coordinación de políticas (Keohane, 1993). Esto permitirá la consecución de los intereses mediante la cooperación. En materia de ciberseguridad, los Estados Miembros comparten el interés por fortalecer su capacidad de respuesta y cooperan en la OEA que sirve de puente de conexión principal. En un contexto de incertidumbre, donde los Estados se encuentran en relación de interdependencia fijada por normas, reglas y procedimientos; las instituciones otorgan la capacidad de regular el comportamiento de los actores y sus efectos (Keohane y Nye, 1988). Como resultado de esta dinámica, el neoinstitucionalismo plantea la reducción de la incertidumbre en un contexto que carece de autoridad supraestatal. Al mismo tiempo, la cooperación de los Estados en la OEA facilita la obtención de ganancias absolutas donde todos ganan a partir de la mutua adecuación. La distribución de ganancias implica un rol activo de las instituciones para lograr una eficiente gestión (Keohane y Martin, 2003). En este sentido, la OEA, en el ámbito de ciberseguridad favorece la reciprocidad y el intercambio de información mediante programas de coordinación.

En relación con los antecedentes, muchos de los trabajos que desarrollan la cooperación en materia electoral la relacionan con los Derechos Humanos (Thompson Jiménez, 2015) o el fortalecimiento de la democracia representativa (Carrillo, 2016), no mencionan la ciberseguridad como un tópico relevante. Por otro lado aquellos trabajos tecnológicos que consideran la seguridad cibernética de vital importancia, no la relacionan con los procesos electorales (Martin, 2015). La ciberseguridad como estrategia de seguridad nacional (Geers, K. 2011) se trabaja en algunos países hace bastante tiempo pero en América Latina y particularmente en la región del Mercosur es un fenómeno relativamente nuevo. Por ejemplo, en Europa se trabajó como una tendencia emergente en defensa nacional (Cano, 2011) y en el ámbito internacional en cooperación con la OTAN (Artiles, 2011), como organismo que debió transformarse para hacer frente a las amenazas cibernéticas. Las amenazas cibernéticas actuales no tienen un remitente claro, han traspasado las fronteras y parece que cualquier cosa puede convertirse en un arma en cualquier momento. La tecnología ha dejado de ser una herramienta administrativa para convertirse en un instrumento estratégico. Por esto podemos hablar de ciberespionaje (Maroto, 2009), ciberterrorismo (Romero, 2011) y ciberguerra (Newmwyer, K, Cubeiro, E y Sanchez, M 2015). El ciberespacio introduce graves vulnerabilidades en las sociedades interdependientes. Desde el año 2013 en Latinoamérica, con el apoyo de la OEA, el Programa de Seguridad Cibernética del CICTE ha tratado este vacío de información con una serie de informes en colaboración con académicos expertos en seguridad cibernética. Estos informes ofrecieron una idea más detallada de los ataques cibernéticos en nuestro hemisferio.

Objetivos

Objetivo General

Analizar la cooperación de la OEA en materia de ciberseguridad electoral en los países del Mercosur en el período 2014-2019.

Objetivos específicos

- Identificar las amenazas en el proceso electoral de los países del Mercosur durante el período 2014-2019
- Explicar la responsabilidad de los diferentes actores en materia de ciberseguridad electoral
- Describir el trabajo llevado a cabo por la OEA con respecto a seguridad cibernética en los países del Mercosur.

Métodos

Alcance, enfoque, diseño y tipo de investigación

El presente trabajo de investigación es de alcance descriptivo y busca especificar las características del fenómeno. La lectura crítica, demostró que si bien hay publicaciones relacionadas al tema de estudio, existen puntos poco detallados respecto a contextualización de las amenazas cibernéticas en el proceso electoral desde una perspectiva neoinstitucionalista y a la construcción e implementación de políticas de seguridad cibernética en el ámbito de cooperación de la OEA con los países del Mercosur. En consecuencia, se privilegió un enfoque cualitativo para indagar las características del objeto de estudio, sucesos, actores y demás componentes del problema que sirvan a la elaboración

del análisis. Por lo tanto, el diseño no experimental de tipo longitudinal sirvió para orientar la comprensión de los hechos en relación al contexto respondiendo con claridad a un problema donde hay poco conocimiento.

Población, muestra y participantes

Con el objetivo de no extender la investigación, se tomó como muestra los países miembros del Mercosur: Brasil, Paraguay, Uruguay y Argentina. Esta iniciativa de integración regional tiene el propósito de afrontar de manera conjunta y coordinada los fenómenos que afectan su funcionamiento. Como bloque regional comparten ciertas características representativas de Estados democráticos y cooperación regional. Sin embargo, en esta investigación, se describió la relación de cada país miembro del bloque con la OEA para conocer si el problema de seguridad cibernética en los procesos electorales también es una característica común de estos países.

Instrumentos

Para la confección del informe, se utilizaron fuentes primarias y secundarias. En un primer momento se planteó la recolección de documentos recientes y convenciones sobre ciberseguridad celebradas en el ámbito de la OEA. Entre estos documentos, se destacaron los informes elaborados en conjunto con el Banco Interamericano de Desarrollo, Amazon, Microsoft y los *Papers* publicados por el CICTE en colaboración con otras entidades. De igual manera, se analizó la evolución de las políticas se ciberseguridad trabajadas en los simposios y foros de la OEA donde participaron los países del Mercosur. Entre las fuentes secundarias, se analizaron los artículos periodísticos publicados por la prensa en línea de

cada país, como además revistas especializadas en la temática y publicaciones de académicos o investigadores considerados oportunos para la investigación.

Análisis de datos

Esta investigación, plantea un primer momento de selección de bibliografía pertinente para determinar las amenazas cibernéticas a las que están expuestos los procesos electorales en los países del Mercosur. En un segundo momento analizar el contenido referido al ámbito de la OEA para identificar de qué forma se produce la cooperación con los países de la región en materia de ciberseguridad electoral.

Resultados

Amenazas

Por un lado, durante los procesos electorales, los ataques pueden estar dirigidos hacia la infraestructura electoral con el objetivo de quebrantar la confidencialidad, integridad y disponibilidad de la tecnología y los datos. Durante las elecciones de 2014 en Brasil, se destacó la inmediatez con la que se entregaron los primeros resultados, sobre un electorado de poco más de 100 millones de personas, pero también hubo denuncias de fraude ante el triunfo ajustado de la presidente Dilma Rousseff. La empresa contratada para realizar la transmisión de datos fue Smartmatic, la cual facilitó la auditoría en su tecnología antes, durante y después de la elección. En Argentina, durante el 2019, se contrató a la misma empresa para la captura y transmisión de datos, esto implica escanear las actas de escrutinio para ser transmitidas desde los centros de votaciones. Durante las PASO (Primarias Abiertas Simultáneas y Obligatorias) realizadas en el mes de agosto el sistema no funcionó por un lapso de horas y los datos fueron demorados. En ese período, el presidente Mauricio Macri reconoció la derrota sin cómputos oficiales. A partir de esto, reconocieron que las pruebas realizadas previo a las PASO habían fallado y el sistema contaba con algunas falencias para el recuento provisional de votos, situación que genero dudas y temores en los comicios. Las auditorías realizadas en los sistemas de votación electrónica determinaron la posibilidad de quebrantar el carácter secreto de los votos y de manipular la transferencia de los resultados.

Por otro lado, las campañas de desinformación intentan manipular la participación electoral y socavar las percepciones de integridad en los procesos electorales. Las últimas elecciones en Brasil fueron monitoreadas por la OEA y causó una importante preocupación

el uso de noticias falsas divulgadas por Whatsapp con el objetivo de manipular la elección. Se diseminaron noticias contra los candidatos fomentando posiciones extremistas y discursos de odio. La OEA reconoció los esfuerzos conjuntos del Tribunal Supremo de Elecciones, medios de comunicación, plataformas en línea y sociedad civil para combatir este tipo de contenidos con iniciativas de verificación de información. En la Argentina, las campañas de desinformación y manipulación están a cargo de personas físicas y bots (cuentas automatizadas). Las estrategias de comunicación de basan en datos, el uso de trolls (usuarios sin identidad) para atacar a opositores y activistas, y la colaboración con los medios para amplificar el mensaje. En Argentina "Reverso" y en Brasil "Comprova" son un consorcio de medios de comunicación que luchan contra la difusión de contenido engañoso que surge en la web, aplicaciones de mensajería y redes sociales. Se concentran en minimizar el alcance y el impacto de las noticias falsas relacionadas, particularmente, con la política nacional. La desinformación, durante las últimas elecciones presidenciales celebradas en Paraguay en 2018, se limitó a la difusión de titulares falsos por grupos de Whatsapp que no llegaron a trascender. El impacto que tuvieron esos titulares fue escaso pero advierten una tendencia en alza para las elecciones municipales del año 2020. La Misión de Observación, llevada a cabo por la OEA en Paraguay informó que la difusión de preferencias en boca de urna llevó a los equipos de campaña pronunciarse en tendencia mientras los votantes aun seguían en los centros votación. Esta práctica, está penada por ley y se repite en las elecciones del país. En el caso de Uruguay, surgió un gran movimiento de noticias falsas publicadas en redes sociales hacia varios precandidatos presidenciales. La reacción de asombro ante el despliegue de recursos se debió a que el país no había experimentado una campaña con estas características.

Actores

Dependiendo del contexto en que surja la amenaza cibernética, éstas pueden ser responsabilidad del Estado o del sector privado. Este último, incluye proveedores de tecnología y telecomunicaciones relacionados con las elecciones. Algunas amenazas, donde la libertad de expresión está en juego, no están reguladas en absoluto. Por este motivo, la colaboración con los medios de comunicación y redes sociales es importante para garantizar una buena comunicación incluso durante un ataque. Sin embargo, no puede limitarse a actores estatales y sector privado, la colaboración incluye a la sociedad civil, los medios de comunicación, partidos políticos y candidatos. La seguridad cibernética se convirtió en un reto que no puede ser resuelto por una única entidad, es de responsabilidad compartida entre múltiples actores por lo tanto requiere de un trabajo amplio entre los diversos sectores.

En el contexto gubernamental, muchas veces, se asocia a la ciberseguridad con agencias privadas de inteligencia. A medida que se comprende mejor y se acepta la idea de que no es solo una consideración técnica, surge un enfoque multidisciplinario que permite una relación más directa con los ciudadanos. La existencia de una organización centrada en ciberseguridad puede no ser suficiente para dar respuesta al desafío que presentan los países frente a este tipo de amenazas. Por este motivo, la colaboración con otros actores resulta esencial para salvaguardar el proceso electoral de las democracias. Aquellos que por su relevancia participan en un programa de ciberseguridad en los países miembros del Mercosur no determinan la exclusión de otros actores que puedan incluirse y ser parte integral de las decisiones. No existe una lista única que deba servir a un grupo de países miembros de la OEA. En primer lugar, los actores políticos (candidatos y partidos), como partes del proceso electoral, demostraron no ser del todo consientes de los riesgos

cibernéticos y por lo tanto no pudieron garantizar las mejores prácticas en términos de protección de datos y privacidad. En segundo lugar, el ciudadano no tuvo una comprensión básica del funcionamiento digital y de los riesgos cibernéticos, provocando que la desinformación juegue un papel fundamental en la sociedad civil. En tercer lugar, los actores gubernamentales que participaron en la ejecución y realización de elecciones democráticas carecían de expertos en la planificación de gestión de riesgo y crisis suficientemente equipados para responder de manera inmediata frente a una amenaza. Del mismo modo los proveedores de servicios de internet y medios de comunicación, incluidas las redes sociales, contribuyeron significativamente al debate público y son considerados parte de la infraestructura crítica de la región por la falta de recursos suficientes para gestionar amenazas cibernéticas.

La red resultante de competencias y responsabilidades es lo que hace esencial al enfoque gubernamental y la cooperación institucional en materia de ciberseguridad. Algunos organismos internacionales, como la OEA, organiza la cooperación a través de talleres y misiones, proyectos e informes, capacitaciones, simposios y actividades.

Cooperación OEA-Mercosur

Durante el período comprendido entre 2014 y 2019, los países del Mercosur, asistieron a Talleres Regionales en el marco de la OEA coordinados muchas veces con el Banco Interamericano de Desarrollo (BID). El objetivo fue comunicar las mejores prácticas sobre el desarrollo de políticas nacionales de seguridad cibernética, facilitar el intercambio de conocimientos e identificar los temas importantes sobre seguridad cibernética para desarrollar recomendaciones que mejoren los sistemas de los países.

Las capacitaciones y simposios que reunieron a técnicos y expertos de los países miembros de la OEA cubrieron las mejores prácticas utilizadas por el equipo de respuesta a incidentes cibernéticos, los marcos legales para prevenir y combatir los delitos y la identificación de pruebas electrónicas. Estas actividades fueron desarrolladas con la intención de lograr una mayor comprensión de la relación entre privacidad, protección de datos y ciberseguridad. La OEA en colaboración con Cisco, empresa líder mundial en tecnología, lanzó una plataforma para la educación en ciberseguridad con el objetivo de generar conciencia y democratizar la seguridad cibernética. Asimismo, junto a la fundación Citi, colaboró para fortalecer las competencias de los participantes en entornos digitales seguros, análisis de amenazas y desarrollo profesional.

Además, durante el período analizado, los países miembros del Mercosur realizaron Ejercicios de Manejo de Crisis (EMC) que han puesto a prueba la comunicación y colaboración entre el gobierno, las TIC y los sectores de infraestructura crítica en caso de un incidente cibernético para mejorar la capacidad de respuesta. Ejemplos de estos ejercicios fueron el Cuarto Aprendizaje Aplicado de *Cyberdrill* y la *CiberEx* international en 2016.

Con el objetivo de mejorar los marcos normativos de los países de la región, la OEA se asoció con Amazon en 2017 para trabajar en la redacción de documentos sobre seguridad y protección de datos. De esta asociación surgen tres *White Papers* que buscan aumentar la ciberseguridad de los ciudadanos, el sector privado y los gobiernos; señalan la importancia de enfocar la ciberseguridad dentro de la cooperación multilateral ante una amenaza global que no entiende fronteras. Además, analizan el estado de la ciberseguridad en las Américas para incrementar la concientización de los líderes, empresas y la sociedad en general en torno a este tema. Adicionalmente, la OEA en colaboración con Microsoft lanzó un reporte

de recomendaciones para desarrollar un marco de trabajo o política de infraestructura crítica en la región de América Latina y el Caribe. Esta infraestructura incluye servicios esenciales para el buen funcionamiento de la sociedad. Consideran que el fortalecimiento de la asociación entre organizaciones públicas y privadas mejorará la capacidad de respuesta frente a ataques cibernéticos. El último *White Paper* presentado en colaboración con Amazon busca fortalecer la capacidad de seguridad cibernética en las Américas a través de un marco de seguridad del Instituto Nacional de Estándares y Tecnología (NIST). Este marco detalla una estrategia para la adopción gubernamental y dos estudios de caso globales sobre países que lo aplican en diferentes enfoques: Reino Unido y Uruguay.

Las amenazas cibernéticas ya no son vistas como un desafío tecnológico, sino como un problema comercial que debe abordarse de manera integral a través de personas, procesos y tecnologías.

Discusión

El objetivo principal de esta investigación fue describir la cooperación entre la OEA y los países miembros del Mercosur en materia de seguridad cibernética en los procesos electorales. En primer lugar, se logró identificar las amenazas que vulneran a una parte importante del proceso democrático para luego poder explicar cómo afectan a los diferentes actores que participan en las elecciones y describir las actividades de cooperación llevadas a cabo para finalmente analizar los resultados.

Primeramente, los resultados muestran que las elecciones se celebran en un entorno de irregularidades que socavan los derechos políticos de los ciudadanos en democracia. La implementación de tecnología en los sistemas electorales va aumentando al mismo ritmo que las vulnerabilidades que ponen en riesgo la integración de las elecciones. Resulta un desafío digital para los actores políticos y los ciudadanos tener en cuenta las mejores prácticas de ciberseguridad comprendiendo las normas de protección de datos y privacidad. Estas prácticas requieren conocimiento para proteger los dispositivos utilizados en los procesos electorales, de lo contrario la falta de implementación de protocolos de seguridad básicos hace que los diferentes actores sean propensos a ataques cibernéticos. Además, mantenerse informado a través de canales oficiales y verificar la información electoral antes de compartirla en las redes sociales debería ser una conducta habitual y no la excepción. La información falsa que circula en redes sociales y sitios web deviene a pensar si esas plataformas sirven de espacio para deliberar o si solo amplifican contenido para mantener al ciudadano desinformado. Sin embargo, los resultados muestran que las plataformas digitales colaboran en el esfuerzo por concientizar a la comunidad sobre los riesgos cibernéticos pero parece no ser suficiente. Los tipos de acciones y actividades que los ciudadanos realizan, al

involucrar tecnología en un entorno democrático o electoral, requieren mejorar las prácticas cibernéticas que deberían están inmersas en la cultura diaria de los interesados. Desde el neoinstitucionalismo la coordinación de políticas reduce la incertidumbre en un contexto dinámico, por lo tanto la ausencia de mejores prácticas compromete la credibilidad de la institución democrática.

En segundo lugar, se evidencia que para garantizar la relación justa y transparente de un proceso electoral, es esencial la responsabilidad compartida de los diferentes actores en ciberseguridad. Cada parte debe comprender su rol en el proceso y el riesgo cibernético asociado. Priorizar la seguridad cibernética, en las agendas de de los países, con un enfoque público-privado garantiza la continuidad del debate permitiendo una mayor intensidad durante el período electoral. Esto requiere que los Estados inviertan en el intercambio de conocimiento e información con otras entidades para fomentar la confianza y establecer las bases para un entorno cibernético estable. Los resultados demuestran que los cuatro países han cooperado en diversas actividades para acceder a recursos técnicos y de información. Sin embargo, al tener en cuenta que la cooperación es posible, los resultados evidencian que los países no siempre solicitan la asistencia de la OEA para monitorear sus procesos electorales e identificar irregularidades que permitan fortalecer las instituciones para las próximas elecciones. Por otro lado, diferentes actores, no estatales, cooperan de manera activa para reducir riesgos, concientizar a los ciudadanos y capacitar a funcionarios en seguridad cibernética. Esto evidencia el concepto de instituciones que define la teoría neoinstitucional, abarcando por un lado, actores estatales, empresas privadas e instituciones públicas (instituciones formales) y por otro lado, incluye normas, valores, culturas y tecnologías (instituciones informales). Si no hay un interés activo de los diferentes actores

involucrados, todos los esfuerzos para mejorar la ciberseguridad pueden fallar. Esto se debe a que es un desafío de responsabilidad compartida que implica colaboración para reaccionar rápidamente ante amenazas y aumentar auditorías internas. Si la ciberseguridad no está debidamente integrada al ciclo democrático, la protección resultará insuficiente y no será sostenible.

La OEA considera a la inseguridad cibernética como un impuesto al crecimiento de los países (BID, OEA, 2016). Por lo tanto si no invierten en la seguridad de su estructura y sistemas, los costos de las amenazas cibernéticas gravaran su crecimiento económico. En éste tercer punto, los resultados arrojan luz sobre la cooperación que se ha venido realizando en el marco de este organismo para fortalecer la capacidad de respuesta de los Estados frente a un incidente. Paraguay, es el único país del Mercosur que ha implementado una estrategia nacional de ciberseguridad que le proporciona un marco normativo para organizar sus iniciativas. La importancia de adoptar una estrategia cibernética radica en la posibilidad de abordar el ciberespacio como una plataforma estable y segura para la actividad económica y reducir los riesgos de seguridad pública y nacional. Los países estudiados realizan esfuerzos en relación con la escasez de personal capacitado en materia cibernética. En el marco de la OEA se evidencia la colaboración, particularmente con el sector privado, para desarrollar conocimiento especializado y ampliar la mano de obra en el ámbito cibernético. A pesar de los esfuerzos realizados, en la región del Mercosur, los países se encuentran en una etapa temprana para lograr un ciberespacio seguro. Se observa la necesidad de creación de una estructura organizativa que distribuya responsabilidades entre los ministerios y organizaciones. Si bien se han creado Equipos de Respuesta ante Emergencias Informáticas (CSIRT) y los países trabajan para mejorar la capacidad de aplicar leyes, no es suficiente.

Desde el neoinstitucionalismo, el desarrollo de un marco jurídico que regule las conductas es crucial para la ciberseguridad.

Los principales desafíos son el desarrollo de capacidades, la cooperación en amenazas cibernéticas y el intercambio de información sobre mejores prácticas y vulnerabilidades (Wolf, 2017). Hacer frente a los desafíos que presenta la seguridad cibernética, requiere de esfuerzos diplomáticos y cooperación internacional. Desde la perspectiva del neoinstitucionalismo, la cooperación es esencial, debido que ninguna nación por sí sola, puede asegurar adecuadamente su seguridad. Esto hace que las gestiones entre los miembros del Mercosur en colaboración con la OEA sean aún más importantes, especialmente teniendo en cuenta las relaciones entre seguridad cibernética, desarrollo y crecimiento económico. Si la economía regional aprovecha los servicios de internet crecería rápidamente y una mejor seguridad en el ciberespacio les permitiría explotar las máximo ese recurso. Fortalecer la cooperación regional también facilitaría la inclusión de los países en las discusiones globales en curso. La naturaleza sin fronteras de las amenazas cibernéticas aumenta la importancia de la cooperación internacional y la armonización de marcos legales que regulen estas conductas. Por lo tanto, el análisis neoinstitucional aplicado a la investigación de un fenómeno relativamente nuevo en las relaciones internaciones, se mostró acertado, en una realidad con una agenda multidisciplinaria que requiere un trabajo cooperativo por parte de los actores internacionales.

Durante el desarrollo de esta investigación, se evidenció que debido a las características de los países del Mercosur no es posible generalizar estos resultados en otras regiones con particularidades diferentes. Debe tenerse en cuenta el contexto de cada región para hacer una evaluación del tema y posteriormente abordar los resultados. Si bien la

ciberseguridad es un tema reciente en la agenda internacional, hay países que están más avanzados en el desarrollo de normativas que regulen las conductas en el ciberespacio. Los países analizados en este informe, se encuentran en una etapa temprana de evaluación de riesgos cibernéticos y por lo tanto, aún requieren un esfuerzo importante en el fortalecimiento de sus capacidades de respuesta.

Por otro lado, se identificaron dos limitaciones principales referidas al análisis de contenido durante la investigación cualitativa: el sesgo de los medios y el lenguaje. Para mitigar el sesgo se utilizaron fuentes de noticias de alta calidad provenientes de las principales organizaciones de marca profesional y expertos académicos. Con respecto al lenguaje se utilizaron investigaciones en inglés que conllevaron un esfuerzo en la traducción exacta y datos de calidad para utilizar citas pertinentes en el desarrollo. Sin embargo, teniendo en cuenta el alcance descriptivo de esta investigación, se logró evidenciar que si bien la OEA sirve de organismo de cooperación en materia cibernética, los países del Mercosur aún carecen de regulaciones internas que promuevan mejores prácticas y una organización institucionalizada en el ámbito doméstico. Los eventos desarrollados indican la necesidad de priorizar la seguridad cibernética en la agenda de los países y adoptar una estrategia nacional que brinde seguridad y confianza en los procesos democráticos. Sin la confianza del votante en el proceso, es probable que la participación de esas mismas personas sea mínima, lo que resulta en un electorado desconectado, que es un signo de una democracia poco saludable. La percepción que deja el estudio es que les queda mucho camino por recorrer a los países de la región del Mercosur, debido a la continua evolución tecnológica sumada a los riesgos que pueda alcanzar de no tomar las salvaguardas

correspondientes. Es decir, existe una clara diferencia donde la legislación interna parece ir muy por detrás del avance tecnológico.

A partir de lo expuesto, y en lo que respecta a futuras investigaciones, sería interesante profundizar en los incentivos necesarios a la hora de implementar políticas domésticas que regulen el comportamiento de los actores en materia de seguridad cibernética. En otras palabras, parece que la experiencia de otros países no es suficiente y que las amenazas no son de gran magnitud para legislar sobre este tema. Esta conducta parece indicar que prevenir o estar preparados no es una característica de los países en estudio.

Finalmente, se evidencian como desafíos principales la concientización para todos los actores involucrados en el proceso electoral, la necesidad de marcos legislativos que traduzcan el debate activo en políticas con un sentido de urgencia y la continuidad en el interés por la seguridad cibernética durante todo el ciclo democrático. Los resultados sugieren que existe una creciente conciencia de las amenazas en los países del Mercosur con respecto a la necesidad de mejorar las prácticas cibernéticas durante los procesos electorales. Sin embargo, los recursos disponibles significan que el progreso se limita al ciclo político. Es importante que la planificación cambie a un enfoque holístico más amplio que fortalezca la integridad del proceso democrático fomentando la comprensión real de los riesgos y beneficios que traen aparejado las TIC. Desde la perspectiva neoinstitucional, la cooperación continua entre los diversos actores involucrados fortalece el proceso democrático fomentando el debate independiente como fuerza impulsora basada en hechos. Por último, es preciso reconocer que el progreso depende además, de recursos financieros que promuevan las mejores prácticas de seguridad cibernética en el proceso electoral. Es importante que los

actores políticos asignen marcos legislativos y presupuestos adecuados para los desafíos que supone la creciente amenaza al núcleo de las democracias.

Referencias

Arteaga Martín, F. (2011). Propuesta para la implantación de una Estrategia de Seguridad Nacional en España. *Boletín Elcano*, (142), 35.

Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia*, (149), 165-214.

Banghart (2018). Foro de Análisis y Discusión "Ciberseguridad en las elecciones". *The aspen institute* (edición digital). Recuperado de http://aspeninstitutemexico.org/foro-de-analisis-y-discusion-ciberseguridad-en-las-elecciones/

Banco Interamericanos de Desarrollo (BID) y Organización de los Estados Americanos (OEA) (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?

BBC News Mundo, (2019) *Cambridge Analytica*: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. Recuperado de https://www.bbc.com/mundo/noticias-49093124.

Bestard, (2019) La OEA ayudará a Paraguay en la Instalación del voto electrónico. Recuperado de https://www.efe.com/efe/america/politica/la-oea-ayudara-a-paraguay-en-instalacion-del-voto-electronico/20000035-3987243

Bradshaw, S. y Howard, P. (2019) *The Global Disinformation Order 2019. Global Inventory of Organised Social Media Manipulation*.

Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *SISTEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS)*, *119*, 4-7.

Carrillo, M. (2006). Cooperación internacional. En D. Nohlen, D. Zovatto, J. Orozco y J. Thompson. (Eds.), Tratado de derecho electoral comparado de América Latina (pp. 84-107). Ciudad de México, México: FCE.

García San José, D. (2006). El concepto de democracia en derecho internacional.

Geers, K. (2011). *Strategic cyber security*.

Keohane, R. (1993). Instituciones Internacionales y Poder Estatal. Buenos Aires: Grupo Editor Latinoamericano.

Keohane, R. y Nye, J. (1988). Poder e Interdependencia. La política mundial en transición. Buenos Aires: Grupo Editor Latinoamericano.

Keohane, R. y Martin, L. (1995). The promise of institutionalist theory. *International security*, *20*(1), 39-51.

Leiva E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software*, *3*(4). pp. 161-176, ISSN 2314-2642.

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. En *La violencia del siglo XXI. Nuevas dimensiones de la guerra* (pp. 45-76). Instituto Español de Estudios Estratégicos.

Martin, P. (2015) Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos. *Instituto español de estudios estratégicos*.

Mendoza (2018) Foro de Análisis y Discusión "Ciberseguridad en las elecciones". *ebizLatam* (edición digital). Recuperado de http://www.ebizlatam.com/la-importancia-de-la-ciberseguridad-en-procesos-electorales/

Miranda (2018) El voto electrónico en Brasil. *"El espectador"* (edición digital) Recuperado en https://www.elespectador.com/noticias/el-mundo/el-voto-electronico-en-brasil-articulo-814081

Montano (2017). De la ciberseguridad, a la ciberpolitica. *10 Temas de Ciberseguridad*.

Newmeyer, K., Cubeiro, E., Y Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra

OEA (2017) "Paraguay y Chile adoptan Planes Nacionales de Ciberseguridad con apoyo de OEA" Recuperado de https://www.oas.org/es/centro_noticias/fotonoticia.asp?sCodigo=FNC-21545

Romero, J. C. (2011). Estrategias nacionales de ciberseguridad: Ciberterrorismo. *Cuadernos de estrategia*, (149), 257-322.

Thompson, J. (2015). Las obligaciones internacionales en materia electoral: un enfoque a partir del sistema interamericano de derechos humanos. *Revista de Derecho Electoral*, (20), 4.

Wolf (2017) *Cybersecurity and Elections: An International IDEA Round-table Summary*