Universitat Autònoma de Barcelona

Facultat de Ciències Polítiques i Sociologia

Treball de Fi de Grau

Títol: La evolución de la política de ciberseguridad de Canadá entre 2010 y 2018.

Autora: Maria Fernanda Macuaran Ochoa.

Tutor: Alessandro Demurtas.

Data: 18 de mayo de 2019.

Grau en: Ciència Política i Gestió Pública.

ÍNDICE

1. INTRODUCCIÓN

1.1 Contextualización y relevancia del objeto de estudio

Durante los últimos años, el ciberespacio se ha transformado en un complejo mundo de interacciones que, tal como menciona Pons Gamón (2017), se enfocan principalmente en el uso de tecnologías, Internet y el intercambio de información. Su importancia es de tal magnitud que "todos los ciudadanos y las sociedades que conforman tienen una dependencia casi total de los sistemas informáticos para todos los procesos económicos y sociales" (Pons Gamón, 2017: 81).

Los Estados también pueden ser incluidos en esa categoría de dependencia, se benefician de las redes implementando mecanismos digitales que les permitan modernizarse para administrar eficientemente. Confían en las Tecnologías de la Información y Comunicaciones (TIC) por ser "una nueva fuente de crecimiento y un motor para la innovación, el bienestar social y la expresión individual" (OECD, 2012: 11)[1]. Sin embargo, aunque el ciberespacio ofrece oportunidades y ventajas, es un ámbito en el que no se está exento del riesgo, y las amenazas delictivas se producen con frecuencia. "Los Estados están siendo nuevas fuentes de amenazas, además de individuos y grupos que pueden estar relacionados con el crimen organizado, potencialmente con el terrorismo, así como con intereses económicos y comerciales" (OECD, 2012: 25), de tal manera, la vulnerabilidad de los Estados aumenta y se exponen a factores que pueden atentar contra el bienestar y la seguridad nacional.

En este sentido, ante el auge de los ciberataques que afectan el normal funcionamiento de los sistemas informáticos de un país por filtración o robo de información, "las naciones y organizaciones han ido reaccionando de forma progresiva para enfrentarse contra esta amenaza global" (Pons Gamón, 2017: 87), cuyas consecuencias no implican directamente crisis humanitarias o conflictos bélicos, pero son tan peligrosas que se presentan como uno de los problemas principales del siglo XXI.

[1] *Todas las traducciones, del inglés al castellano, son propias de la autora.*

El cibercrimen es un desafío con carácter silencioso, que, según Pons Gamón (2017), ha llevado a la adaptación y modificación de la legislación de distintos países y organizaciones, enfocándose en acciones que garanticen la protección en el ciberespacio. "Se ha convertido en una prioridad política nacional apoyada por un liderazgo más fuerte" (OECD, 2012: 9), condicionando la creación de estrategias que protejan las infraestructuras de información a nivel individual, empresarial y estatal. Según la Organización para la Cooperación y el Desarrollo Económicos (2012), existe una nueva generación de políticas denominadas Estrategias de Ciberseguridad, que se han desarrollado entre 2009 y finales de 2011 por países como Australia, Alemania, Canadá, Estados Unidos de América, Francia, Japón y Reino Unido. Actualmente, por la constante e indetenible evolución de los ciberataques a nivel mundial, se ha expandido y consolidado entre un mayor número de Estados.

Canadá es uno de ellos, destacando durante años como uno de los líderes en temas de ciberseguridad, integrando el top 10 del *Global Cybersecurity Index* de la *International Telecommunication Union* (2017), de los países comprometidos en este ámbito. "Canadá enfatiza que la colaboración internacional es esencial para asegurar el ciberespacio y tiene el beneficio de ser visto a nivel internacional y nacional como un socio confiable para hacer que el ciberespacio sea más seguro" (OECD, 2012: 33), por tal razón, siendo además un actor destacado en el sistema internacional en términos económicos y comerciales, se considera un Estado relevante para estudiar la importancia de las políticas de ciberseguridad en Occidente.

1.2 Objetivos del trabajo

Teniendo en cuenta lo mencionado en los párrafos anteriores, el objetivo del Trabajo Final de Grado será analizar la evolución de la política de ciberseguridad de Canadá entre 2010 y 2018, con el fin de comparar las acciones que se han tomado durante los últimos años. Con este estudio se intentará responder cómo se desarrolla la política de ciberseguridad del Gobierno de Canadá, comprender su estructura y forma de implementación para determinar si el camino que sigue en materia de ciberseguridad es adecuado, si sus planes son suficientes para protegerse ante las ciberamenazas, y si debería ser un ejemplo a seguir por otros Estados.

Usando como fuente principal los documentos de la Estrategia de Ciberseguridad de Canadá (2010), y la Estrategia Nacional de Ciberseguridad (2018), se tendrán como pautas de análisis identificar sus amenazas, definir sus actores principales y evaluar sus pilares de acción, así como las medidas que han implementado a nivel estratégico para complementar su Estrategia Nacional durante el período seleccionado.

1.3 Marco teórico y metodología

Las políticas públicas se definen como "la acción del Estado dirigida a cumplir ciertos objetivos" (Méndez, 2000: 80) determinados ante una situación o problema específico, cuyas consecuencias afectan a toda la sociedad. Según Méndez (2000), tales políticas implican el uso de recursos económicos o legales para ejecutar actividades propuestas a través de un plan de acción, dirigido al logro de metas globales de carácter público. Considerando que incluyen un diagnóstico de las causas de un problema, así como las medidas que lo pudieran mitigar, destacan dos elementos básicos para el análisis de una política pública: la solución y la estrategia (Méndez, 2000: 86). Definir qué se espera lograr y cómo, es de suma importancia, independientemente del ámbito en que se desarrolle la política.

En temas de seguridad, estos aspectos requieren de gran precisión por la gravedad de los riesgos que involucra la defensa y protección de los ciudadanos. En la actualidad, existe una nueva generación de políticas públicas de seguridad enfocadas al mundo digital, no solo por el auge del uso de las tecnologías y del Internet, sino también por el incremento de amenazas a los sistemas informáticos estatales que regulan las redes de distribución y servicios gubernamentales básicos. De hecho, "la mayoría de los sistemas militares modernos están tan íntimamente relacionados con el ciberespacio que dependen de él para sus operaciones fundamentales" (Snyder et al., 2015: 1). Por tal razón, las estrategias de ciberseguridad forman parte esencial de la categoría de políticas públicas, integrando aspectos que van desde lo militar, a lo económico e incluso social.

Este tipo de políticas conllevan un alto grado de complejidad, pero en su mayoría pretenden "mejorar la coordinación gubernamental. Refuerzan la cooperación público-privada. Destacan la necesidad de respeto de valores fundamentales como la privacidad, la libertad de expresión

y el libre flujo de información" (OECD, 2012: 13), así como exigen una mayor cooperación internacional, asegurando "crear las condiciones para que Internet impulse la prosperidad, el crecimiento y el bienestar" (OECD, 2012: 18).

En resumen, las políticas nacionales de ciberseguridad deben ofrecer seguridad en el empleo del ciberespacio, sin que supongan una violación de la privacidad y demás derechos de los ciudadanos. Es recomendable que se desarrollen "en un ambiente de participación que contemple al sector público, privado, académico y la sociedad civil, pues condicionará su legitimidad" (Sancho Hirare, 2017: 12), elemento fundamental del éxito de su futura implementación, agrupando a distintos sectores de la población.

Por último, se afirma que la gestión eficaz de la ciberseguridad se logra a través de métodos eficientes que mitiguen los riesgos de la explotación cibernética y el ciberataque, es decir: las vulnerabilidades de los sistemas informáticos, amenazas a esos sistemas, y el impacto que generan dichas amenazas si logran explotar las vulnerabilidades existentes (Snyder et al., 2015: 5), ya que suponen un peligro para el desenvolvimiento y funcionamiento regular de la administración del Estado y de la vida ciudadana cotidiana.

Una vez enunciadas las categorías de análisis para el desarrollo del trabajo, es importante mencionar que su metodología se basa en un análisis cualitativo y comparativo que permita obtener las conclusiones para estimar la postura e influencia de Canadá en temas de ciberseguridad, cuál es la importancia de sus políticas puestas en marcha y cómo inciden en el sistema internacional.

En primer lugar, se estudian los documentos gubernamentales y académicos en los que se explique la visión canadiense sobre la ciberseguridad, cómo actúan en ese ámbito. Luego, se investigan los componentes básicos y planes de acción definidos en sus dos estrategias principales de ciberseguridad, 2010 y 2018, para observar sus propuestas y lineamientos. Posteriormente, evaluar sus resultados y consecuencias analizando la evolución y puesta en práctica de la política, identificando sus posibles aportaciones para el sistema internacional. Las estrategias analizadas son la primera y la última, respectivamente, implementadas por el Gobierno canadiense para atender esta problemática durante el período de estudio seleccionado,

siendo las más útiles para evaluar sus acciones en el tema en cuestión.

2. LA CIBERSEGURIDAD EN CANADÁ

En Canadá, la infraestructura digital tiene un papel relevante en la vida de sus ciudadanos, y en el funcionamiento del Gobierno, aprovechando las ventajas que ofrece el ciberespacio para gestionar servicios institucionales, mejorar la calidad de vida e incentivar su economía. Sin embargo, su exponencial confianza en el uso de tecnologías cibernéticas lo ha convertido en un Estado vulnerable, cuyos sistemas informáticos son un atractivo para diversos servicios de inteligencia, delincuentes y redes terroristas (Government of Canada, 2018).

De tal manera, los Gobiernos de Canadá liderados por Stephen Harper (2006-2015) y Justin Trudeau (2015-Actualidad), han incluido estrategias específicas en sus planes de Gobierno para proteger a sus usuarios, acabar con el desarrollo de crímenes y actividades ilegales cibernéticas, y enfrentar las ciberamenazas que roban secretos de seguridad industrial y nacional (Arnold, 2018: 6). Manifestando así, su compromiso para garantizar que el territorio canadiense sea próspero y seguro.

De acuerdo con Arnold (2018: 7), desde el origen de la política de ciberseguridad el enfoque canadiense se basa en la existencia de amenazas, con una actuación fundamentada en leyes y estrategias, implementadas en un orden multisectorial, complementado por la participación de actores no estatales y la cooperación internacional. Además, destaca una característica particular, la participación de todos los niveles de gobierno: local- regional, provincial y territorial-federal (OECD 2012: 21). En este sentido, la acción de Canadá frente al riesgo cibernético ha sido notable, incluyendo diversos pilares de acción y actores diferenciados que, en función del desarrollo de la problemática en cuestión, han cambiado con el tiempo. A continuación, se describen las estrategias de seguridad y medidas alternativas aplicadas entre el período 2010-2018.

2.1 Estrategia de Ciberseguridad de Canadá: Por una Canadá más fuerte y próspera (2010)[2]

En el año 2010, el éxito en el ciberespacio se consideró uno de los grandes logros nacionales durante el Gobierno canadiense de Stephen Harper. Por ello, se decidió proteger este ámbito a través de la puesta en marcha de lo que sería la estrategia de ciberseguridad pionera en el país, que destaca la participación del sector privado y de multiniveles de gobierno, para fortalecer las capacidades de defensa a la par de un incentivo innovador de las tecnologías, para el desarrollo de la economía (p. 8).

Según esta estrategia de seguridad, los ataques cibernéticos se consideran la principal amenaza, pudiendo ser sencillos o sofisticados, incluyen el uso, acceso no autorizado y manipulación de información electrónica o estructuras digitales para procesarla, siendo de carácter público o privado (p. 3). De igual forma, se plantean algunas características comunes a este tipo de ataques: son de bajo costo, fáciles de implementar, tienen una alta efectividad con el desarrollo de pocas capacidades y son de bajo riesgo por ser difícil detectar su origen. Por otra parte, además de ataques cibernéticos, se distinguen tres tipos de amenazas:

- Ciberespionaje patrocinado por el Estado y actividades militares: Son ataques provenientes de servicios de inteligencia/militares de otros países. Se consideran los más sofisticados ya que, "están bien dotados de recursos, son pacientes y persistentes. Su propósito es ganar ventaja política, económica, comercial o militar" (p. 5).

- Uso terrorista de Internet: Diversas redes terroristas incorporan ciberoperaciones en su doctrina estratégica, con el fin principal de "apoyar sus actividades de reclutamiento, recaudación de fondos y propaganda" (p.5). Este tipo de amenaza se considera más directa, por ser expresada públicamente por grupos como Al-Qaeda, conscientes del "potencial de utilizar la dependencia del mundo occidental de los sistemas cibernéticos, como una vulnerabilidad a ser explotada" (p.5)

[2] Documento de referencia: Government of Canada. 2010. *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada.* Ottawa - Ontario: Public Safety Canada 2010.

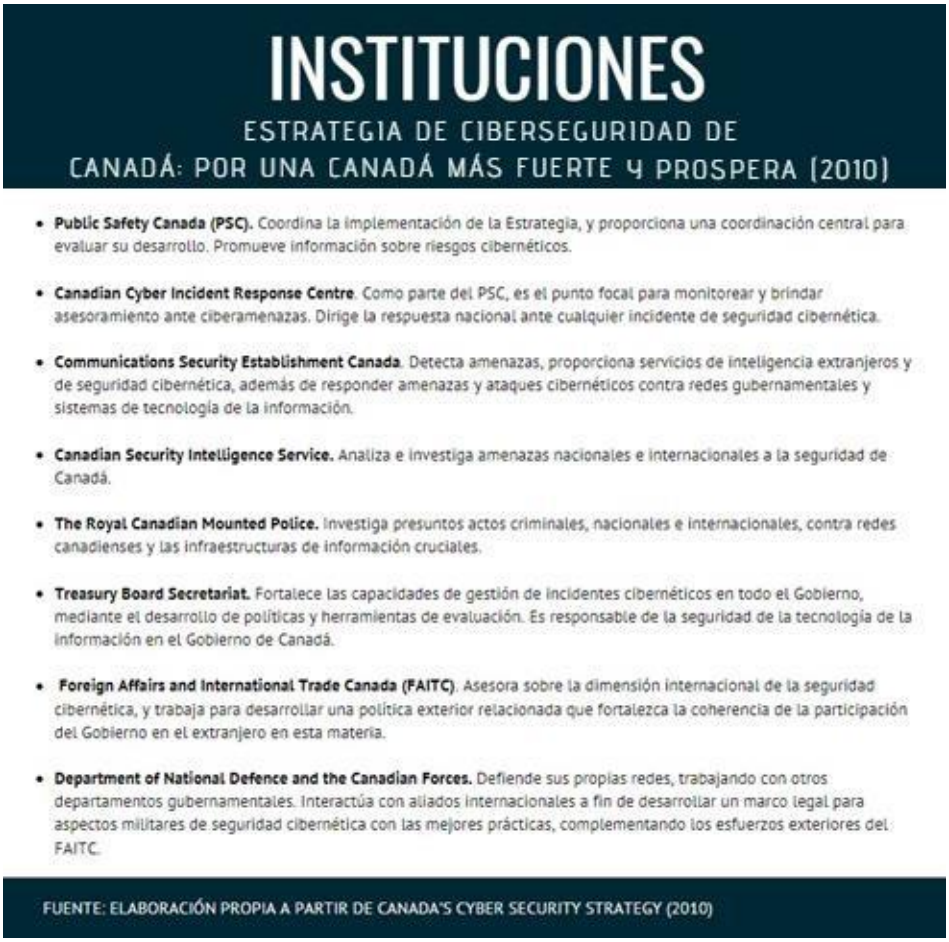
- Cibercrimen: Actividades desarrolladas por organizaciones criminales, que comúnmente implican robo de identidades, lavado de dinero, extorsión, entre otras. Son ataques a un nivel más individual o empresarial (p. 5).

Ante la evolución de las técnicas y herramientas de los ataques cibernéticos basados en su auge en el siglo XXI, cuando "más del 60% de todos los códigos maliciosos jamás detectados se introdujeron en el ciberespacio en 2008" (p. 6), la protección del ciberespacio canadiense se presenta como uno de sus desafíos principales. En este sentido, su estrategia se estructura en tres pilares de acción (Ilustración 1), que manifiestan su actuación y solución ante la problemática existente.

Ilustración 1

En cuanto a los actores principales para el desarrollo de esta estrategia, hay especial atención en la cooperación, tanto a nivel nacional como internacional, ya que, la política de ciberseguridad "enfatiza las asociaciones con canadienses, provincias, territorios, empresas y academia" (p. 8), así como "apoya los esfuerzos internacionales para desarrollar e implementar un régimen global de cibergobernanza que mejorará la seguridad" (p. 8). Existe una división de actividades muy precisa de acuerdo con las instituciones que serán mencionadas a continuación:

Ilustración 2



Con esta identificación de actores principales encargados de ejecutar la estrategia de ciberseguridad, se manifiesta una interrelación multinivel que actúa en conjunto para garantizar la seguridad cibernética del Estado, sus empresas y sus ciudadanos, cumpliendo con los objetivos establecidos a través de sus pilares de acción.

2.2 Estrategia Nacional de Ciberseguridad: Visión de Canadá para la Seguridad y Prosperidad en la Era Digital (2018)[3]

Esta nueva estrategia de ciberseguridad se implementa bajo el Gobierno de Justin Trudeau (2015-Actualidad), en un panorama global más dinámico, por ello, con un enfoque amplio e inclusivo promueve un rol activo de los ciudadanos ante la necesidad de mejorar sus conocimientos y habilidades sobre seguridad cibernética (p. 10). Para los canadienses, el

[3] Documento de referencia: Government of Canada. 2018. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age.* Ottawa - Ontario: Public Safety Canada 2018.

ciberespacio forma parte de su estilo de vida en todos los ámbitos, desde el personal, al empresarial, hasta llegar al gubernamental. De tal manera, se afirma que "la ciberseguridad es el compañero de la innovación y el protector de la prosperidad" (p. 2). Con este contexto, la estrategia intenta responder con mayor eficiencia a los retos de seguridad digital existentes en el escenario internacional, mientras aprovecha las oportunidades de desarrollo económico que ofrece el uso de las tecnologías.

En líneas generales, las novedades incorporadas se pueden resumir en: financiamiento para el nuevo Centro Canadiense de Seguridad Cibernética[4], para apoyar el liderazgo y colaboración entre los diferentes niveles de gobierno y socios internacionales; creación de la Unidad Nacional de Coordinación del Ciberdelito[5] para investigaciones del delito cibernético; financiamiento para fomentar la innovación, desarrollo y el crecimiento económico canadiense en el ámbito digital. Sin embargo, es importante mencionar que esta estrategia es complementada por planes de acción de seguridad cibernética (p. III).

Además, la implementación de la estrategia se alinea con otras iniciativas gubernamentales como: Ministerio de Instituciones Democráticas[6] para defender procesos electorales de las amenazas cibernéticas, y fortalecer la institucionalidad democrática; política exterior cibernética en la agenda internacional canadiense; uso del ciberespacio por las fuerzas militares; Plan de Innovación y Habilidades[7], para que Canadá sea líder de innovación mundial, generando más empleos bien remunerados y fortaleciendo la clase media.

Con respecto a las amenazas cibernéticas, se describen en constante crecimiento y perfeccionamiento, desarrolladas por "piratas informáticos individuales y amenazas internas, redes criminales, estados nacionales, organizaciones terroristas y actores patrocinados por el

[4] *Canadian Centre for Cyber Security*. Es la autoridad canadiense en materia de seguridad cibernética, dirigiendo las acciones del Gobierno en este ámbito. Para más información: https://www.cyber.gc.ca

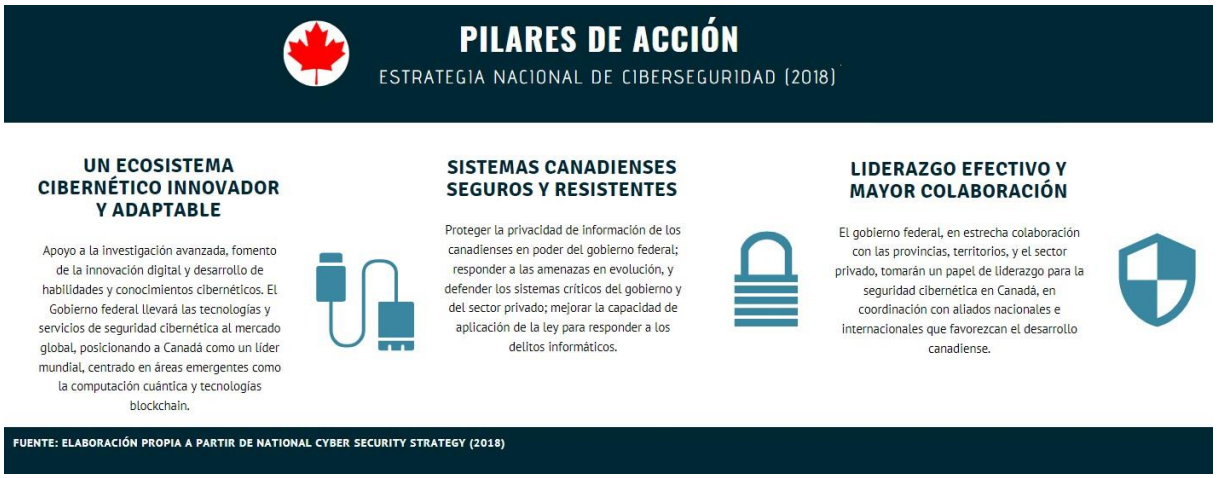
[5] *National Cybercrime Coordination Unit*. Actúa como parte de la Royal Canadian Mounted Police (RCMP), en colaboración con el Canadian Centre for Cyber Security. Para más información: http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2019-2020-departmental-plan

[6] *Minister of Democratic Institutions.* Para más información: https://www.canada.ca/en/democratic-institutions.html

[7] *Canada's Innovation and Skills Plan.* Para más información: https://www.budget.gc.ca/2017/docs/plan/chap-01-en.html

Estado" (p. 12). Siendo relevante la particularidad, de que a menudo se realizan para obtener beneficios económicos. Entre las mencionadas, aunque no explícitamente, se encuentran: suplantación de identidad, robo de propiedad intelectual nacional o estrategias de negocio confidenciales, interrupción de servicios a través de campañas de denegación de servicio distribuido (DDoS) y computación cuántica.[8] Por otra parte, los pilares de acción de la nueva visión tienen una descripción previa del contexto que los hace necesarios, y se definen de la siguiente manera:

Ilustración 3



En cuanto a los actores principales para la aplicación de esta estrategia, destaca la actuación multinivel con Provincias y Territorios para definir los mecanismos que garanticen la protección de la infraestructura digital. El Gobierno Federal propone trabajar con la academia y el sector privado con el fin de "crear nuevas oportunidades, impulsar la inversión y fomentar la investigación y el desarrollo de vanguardia" (p. 20) en el ámbito digital. Además, es importante destacar que los líderes del sector privado tienen un rol principal, como "un elemento necesario para asegurar que todos los canadienses estén lo mejor equipados posible para prevenir y responder a las amenazas cibernéticas" (p. 27). Por último, se deben mencionar nuevamente, ahora como actores, el Centro Canadiense de Seguridad Cibernética y la Unidad Nacional de Coordinación del Ciberdelito.

[8] Una computadora cuántica puede procesar gran cantidad de cálculos simultáneamente, de forma más rápida y segura p. 35).

3. EVOLUCIÓN DE LA POLÍTICA DE CIBERSEGURIDAD DE CANADÁ

Ante un contexto internacional versátil y un elevado número de innovaciones tecnológicas, las acciones del Gobierno de Canadá han de renovarse constantemente para proteger a sus ciudadanos en el sector digital, ya que "prácticamente todo lo que hacen los canadienses se relaciona con la tecnología de alguna manera: per cápita, pasan la mayor parte del tiempo online antes que cualquier país del mundo, con 43.5 horas por canadiense al mes" (Government of Canada, 2018: 4). Con datos precisos del *Communications Security Establishment* (2019), las redes gubernamentales canadienses son de suma importancia y han incrementado de tal manera, que acumulan más de cincuenta y siete mil servidores, nueve mil conexiones de internet, y acceden a ellas unos trescientos setenta y siete mil funcionarios, más los millones de ciudadanos que hacen uso de los servicios que ofrecen.

Para analizar la evolución de la política de ciberseguridad, es oportuno mencionar que, en octubre de 2016, se realiza una consulta pública en línea para revisar las medidas aplicadas con anterioridad, con la finalidad de mejorar la protección de las infraestructuras cibernéticas, identificando los desafíos del momento. Según el Gobierno de Canadá (2018), la intención es generar un nuevo enfoque que permita su posicionamiento como líder internacional en la materia, determinando cuál es el rol federal más adecuado. Con ello, se recopilaron las opiniones de ciudadanos, expertos, académicos y líderes empresarios, bajo el planteamiento "de tres ideas relevantes para la seguridad cibernética: privacidad, colaboración y el uso de personal calificado de seguridad cibernética" (Department of Public Safety and Emergency Preparedness, 2019).

En este sentido, un gran avance de su política de ciberseguridad es la estrategia emitida en 2018, fundamentada en buena medida en los resultados de esta consulta pública, denominada Revisión Cibernética[9] que además de definir objetivos claros, incorpora aspectos más técnicos e innovadores, como acelerar el desarrollo de ciudades inteligentes en Canadá, con la iniciativa *Smart Cities Challenge.* Así como el incentivo de estudiantes y trabajadores a desenvolverse en los campos de ciencias, tecnología, ingeniería y matemáticas (Government of Canada, 2018:

[9] Para más información, se recomienda consultar el reporte de resultados de la *Cyber Review*: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-en.aspx)

22), develando un interés mayor por la inclusión y participación de la sociedad civil, debido a que "el Gobierno de Canadá prevé un futuro en el que todos los canadienses desempeñen un papel activo en la configuración y el mantenimiento de la resistencia cibernética de la nación." (Government of Canada, 2018: 2).

Además, se produce la unificación de las funciones de seguridad cibernética y la experiencia operativa de tres instituciones fundamentales en la estrategia de ciberseguridad de 2010: *Public Safety Canada, Shared Services Canada* y *Communications Security Establishment.* Estos departamentos se unen para conformar el Centro Canadiense de Seguridad Cibernética, "una organización única, innovadora y con visión de futuro, como parte del Communications Security Establishment (CSE)" (Communications Security Establishment, 2019). Establecido desde octubre de 2018, mejor conocido como *Cyber Centre*, se define como principal punto de contacto y liderazgo del Gobierno Federal en asuntos operacionales de seguridad cibernética, abarcando tareas de gestión de amenazas, asesoramiento y orientación técnicos, así como distribución de información.

Otro cambio notorio se manifiesta con la relevancia que adquiere el tema en la agenda política, al dedicar poco más de quinientos millones de dólares del presupuesto anual de 2018[10], solo para un quinquenio. Siendo así, la mayor inversión del Gobierno en ciberseguridad, superando los cuatrocientos treinta y un mil quinientos millones de dólares, destinados en la estrategia de 2010, para diez años de gestión.

3.1 Medidas Complementarias

De igual manera, para suplementar las políticas de ciberseguridad puestas en marcha entre 2010-2018, el Gobierno de Canadá ha implementado distintas medidas a nivel estratégico, que manifiestan acciones específicas que han realizado durante el período en cuestión, para garantizar la protección de sus ciudadanos y empresas en el ciberespacio.

En primer lugar, se encuentra *Get Cyber Safe,* una campaña de concientización especialmente dirigida a los ciudadanos, que ofrece herramientas de asesoramiento y

[10] *Budget Plan* (2018). Disponible en: https://www.budget.gc.ca/2018/docs/plan/toc-tdm-en.html

orientación para que las personas de distintas edades tengan un mejor entendimiento de lo que representa la seguridad cibernética y puedan navegar en Internet con mayor libertad. Gestionada por el Centro Cibernético, a través de redes sociales y su propia página web[11] proporciona consejos y datos útiles respaldados por la experiencia, para el fomento de una educación cibernética (Canadian centre for Cyber security, 2019).

Un elemento destacado de esta campaña es que ha designado octubre, como el *Mes de Concientización sobre Seguridad Cibernética,* "para ayudarnos a todos a ser más conscientes de lo que podemos hacer para estar seguros en línea" (Get Cyber Safe, 2019), siendo una acción compartida con Estados Unidos de América, el Reino Unido, Australia y Nueva Zelanda, manifestando la cooperación con aliados internacionales.

En cuanto a legislaciones, destaca la implementación desde 2014 de una de las leyes anti-spam[12] más reconocidas, la *Legislación Canadiense Anti-Spam*[13] que protege a los consumidores y empresas del mal uso de la tecnología digital, ayudando a que estas puedan mantenerse competitivas en un mercado global. Específicamente entre 2014-2015, produjo una reducción del correo no deseado de origen canadiense de un 37%, según datos del Innovation, Science and Economic Development Canada (2015).

También se debe hacer referencia al *Instituto Canadiense para la Ciberseguridad*[14], como centro nacional para la innovación en seguridad cibernética, enfocado en la capacitación y colaboración en la industria. Creado en 2017, como parte de la Universidad de New Brunswick, es un claro ejemplo de la colaboración multinivel, para el fortalecimiento y desarrollo de propuestas favorables para los canadienses. Esta vinculación se observa con la inversión de dos mil doscientos setenta millones de dólares por parte del Gobierno de Canadá, y mil novecientos ochenta y nueve millones por parte de la Provincia de New Brunswick para concretar esta iniciativa (Atlantic Canada Opportunities Agency, 2019), que se ha convertido en un pilar

[11] *Get Cyber Café* (2019). Disponible en: https://www.getcybersafe.gc.ca/index-en.aspx
[12] De acuerdo con el Government of Canada Spam Reporting Centre, su definición más simple es la de mensaje no deseado, sea correo electrónico, texto o software no solicitados. https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home
[13] Para más información: (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/canadas-anti-spam-legislation/)
[14] *Canadian Institute for Cybersecurity* (2019). Disponible en: https://www.unb.ca/cic/

fundamental para Canadá y el mundo, por sus novedosos proyectos.

3.2 Resultados

La innovación digital se ha convertido en el motor económico canadiense del siglo 21, y la ciberseguridad tiene un papel influyente en eso, por sus aportaciones a la actividad económica y el desarrollo, "contribuyendo con mil setecientos millones de dólares del Producto Interno Bruto de Canadá, generando más de once mil trabajos bien remunerados" (Government of Canada, 2019). No obstante, los resultados específicos en materia de ciberseguridad son inciertos y variables.

En un estudio realizado en 2018 por la compañía *ESET Cybersecurity Barometer (*2018), basado en una encuesta a mil canadienses sobre el tema, se demostró que nueve de cada diez consideran el delito cibernético como un desafío para la seguridad interna. En su mayoría, expresan una preocupación relevante, con un porcentaje menor de quienes efectivamente han recibido alguna amenaza en el ciberespacio. Una pregunta interesante de este barómetro, es "¿La policía y demás autoridades canadienses están haciendo lo suficiente para luchar contra el ciberdelito?", obteniendo el resultado de que solo un 49% de los encuestados dieron una respuesta afirmativa (10% totalmente de acuerdo y un 39% de acuerdo). Sin embargo, aunque no es un porcentaje tan alto, en comparación con los encuestados estadounidenses que están de acuerdo en un 44%, la valoración de las autoridades canadienses es mayor (p.5).

Otro dato relevante es que en contraste con la misma encuesta realizada en la Unión Europea en 2017, bajo el nombre *Special Eurobarometer: Cyber Security*, solo un 46% de los 28 países se considera bien informado sobre los posibles riesgos del cibercrimen, ante un 62% en Canadá, cuyos ciudadanos afirman en un 67%, que su información no es debidamente protegida por el Gobierno Federal.

Desde una perspectiva empresarial, la situación varía un poco. De acuerdo con la Encuesta Canadiense de Ciberseguridad y Cibercrimen de 2017[15], un 21% de las empresas informan que

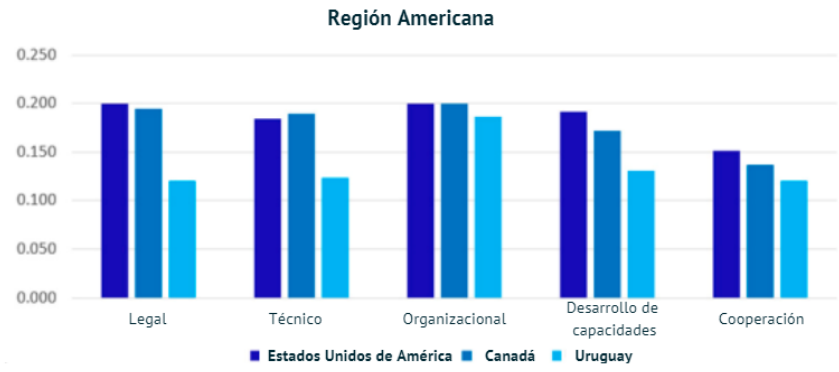
[15] *Canadian Survey of Cyber Security and Cybercrime*. Para más información: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm

se vieron afectadas por un incidente de seguridad cibernética, con la distinción que las grandes empresas (41%) tenían más del doble de probabilidades que las pequeñas empresas (19%) de identificar un incidente relevante sobre sus operaciones.

De tal manera, es evidente que, como se afirma en el *ESET Cybersecurity Barometer* (2018), la velocidad a la que se encuentran los sistemas y los datos es indetenible, y los delitos en el espacio cibernético son exponenciales, siendo difícil garantizar plenamente la confianza del público respecto a su protección. Aun así, el trabajo de Canadá en la ciberseguridad sigue siendo predominante, ocupando la posición número nueve del top diez de países comprometidos con el tema a nivel mundial (Global Cybersecurity Index, 2018) junto a Noruega, con una puntuación de 0.892 sobre un valor máximo de 1, siendo el segundo líder en la región americana tras los Estados Unidos de América, seguido por Uruguay (Ilustración 4).

Ilustración 4

Top tres de puntuación en la región americana, en relación a los cinco pilares del Global Cybersecurity Index (GCI)



FUENTE: ELABORACIÓN PROPIA A PARTIR DE LA FIGURA 6.2.1 DEL GLOBAL CYBERSECURITY INDEX (2018)

Como se puede observar en la gráfica, existen diferencias sutiles entre los dos primeros países. Canadá destaca en el ámbito legal con la existencia de instituciones y un marco jurídico sobre ciberseguridad; funcionamiento de instituciones técnicas; y en el pilar organizacional, por la implementación de estrategias y políticas de coordinación institucional, con menor puntuación en el desarrollo de capacidades, como la existencia de programas de investigación, educación y

capacitación; y en la cooperación, por menor nivel de marcos de la misma y redes de intercambio de información.

Empero, incluso respecto a Reino Unido, líder global de este índice de la International Telecommunications Union (ITU), Canadá sigue demostrando su fortaleza en materia de ciberseguridad, en el año 2018 (Ilustración 5):

Ilustración 5

Comparación entre Reino Unido y Canadá, de la puntuación total del Global Cybersecurity Index (GCI)

rank	Estado	Puntuación Total	Legal	Técnico	Organizacional	Desarrollo de capacidades	Cooperación
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
9	Canada	0.892	0.195	0.189	0.200	0.172	0.137

FUENTE: ELABORACIÓN PROPIA A PARTIR DE LA TABLA 5.1 DEL GLOBAL CYBERSECURITY INDEX (2018)

3.3 Contribuciones al sistema internacional

Como sugiere Arnolds (2018), el Gobierno de Canadá destaca por su iniciativa de lograr un enfoque global de seguridad cibernética, basado en la integración de grandes potencias que compartan su preocupación por el ciberespacio, bajo "el contexto de una respuesta multilateral al riesgo cibernético que es, en el mejor de los casos, parcial y provisional" (p. 7), siendo necesaria la aplicación del Derecho Internacional para complementarlo.

De tal manera, la participación de Canadá es de gran relevancia en el escenario mundial, siendo uno de los cincuenta y cinco Estados en firmar y ratificar en 2017, el Convenio de Budapest del Consejo de Europa, "único tratado multilateral centrado específicamente en el ciberdelito" (Arnolds, 2018: 7). Así mismo, su Gobierno Federal implementó una política exterior de ciberseguridad, enunciada en su Estrategia Nacional de Ciberseguridad de 2018, demostrando su objetivo de expandir y cooperar con otros Estados sobre esta temática, para fomentar el desarrollo de planes y políticas de ciberseguridad.

También conviene destacar que Canadá es uno de los actores que, según Dupont (2018), genera vínculos colectivos para combatir el delito informático a nivel internacional. Con base en el ranking que plantea el autor, del número de iniciativas en que los actores participan, qué tan cercana es su interacción con otros, y su capacidad de intermediación con quienes están menos cualificados en la ciberseguridad, se manifiesta su posición principal en el segundo lugar de la primera variable, por su vinculación en iniciativas de la Commonwealth, Interamericanas y Asiáticas. Teniendo a su vez, "el perfil de enlace más diversificado" (Dupont, 2018: 26) ocupando el puesto número cuatro, y el número seis en su cercanía con otros actores.

En este sentido, su papel de influencia en el sistema internacional se evidencia con distintas iniciativas que ha desarrollado a lo largo del tiempo, para asegurar la cooperación y protección cibernética. En primer lugar, destaca su compromiso en el continente americano con el financiamiento a los proyectos de la Organización de Estados Americanos (OEA) y sus Estados miembros, para reducir la delincuencia organizada trasnacional, incluyendo los delitos cibernéticos. Esta acción se realiza a través del Programa de Fortalecimiento de Capacidades Contra el Terrorismo de Canadá[16], que para 2011, contribuyó con más de un millón de dólares para ayudar a los países americanos a monitorear y responder a las amenazas cibernéticas (Comité Interamericano Contra el Terrorismo, 2012).

Además, en 2018 se reafirmó la vinculación canadiense con la OEA, tras la definición de *Global Affairs Canada* y *Public Safety Canada* como asociados en el programa de Seguridad Cibernética de su Comité Interamericano Contra el Terrorismo (CICTE) (Comité Interamericano Contra el Terrorismo, 2018). Con respecto al continente europeo, su rol también es notorio, manifestado con su iniciativa para formalizar el "Acuerdo entre Canadá y la Unión Europea sobre procedimientos de seguridad para el intercambio y la protección de información clasificada"[17], expresando su compromiso en ciberseguridad, para fortalecer la cooperación en la lucha antiterrorista (Europa Press, 2017).

[16] *Counter-Terrorism Capacity Building Program* (CTCBP). Para más información: https://international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/capacity_building-renforcement_capacites.aspx?lang=eng

[17] Documento disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22017A1215(01)&from=IT

Por último, se debe mencionar que Canadá es Miembro de instituciones como el *Global Forum on Cyber Expertise*, una plataforma global para Estados, organizaciones internacionales y empresas del sector privado, con el objetivo de intercambiar las mejores prácticas en el desarrollo de capacidades cibernéticas. Destacando que, "junto con socios de ONG, la comunidad tecnológica y la academia, los miembros de GFCE desarrollan iniciativas prácticas para desarrollar la capacidad cibernética" (Global Forum on Cyber Expertise, 2019).

4. CONCLUSIONES

En el presente trabajo, se ha planteado la pregunta de cómo se desarrolla la política de ciberseguridad del Gobierno de Canadá entre 2010 y 2018. De tal manera, se ha explicado este concepto básico para contextualizar el trabajo, y se ha estudiado la evolución de las estrategias de Canadá en seguridad cibernética. Analizando su estructura básica, describiendo sus objetivos principales, actores relevantes, e identificando las amenazas que suponen una preocupación para sus ciudadanos. Además, se ha investigado sobre las acciones y medidas complementarias que han aplicado durante el período en cuestión.

Dentro de este marco de referencia, es posible afirmar que la ciberseguridad es un tema primordial en Canadá, tanto para sus gobernantes, como para sus empresarios, y también para el resto de sus ciudadanos, considerando la importancia que le dan al uso de espacios digitales. En consecuencia, sí se ha producido una evolución de la política de ciberseguridad, pues se implementó una primera estrategia en 2010, sustituida en 2018, para ser más apta a los desafíos de la era. Esto demuestra que el Gobierno Federal canadiense tiene un verdadero compromiso con esta temática, al intentar innovar e incluir aspectos relevantes que anteriormente habían sido dejados a un lado, para estar al margen de los retos que se van generando con el transcurrir de los años.

En términos generales, el desarrollo de su política de ciberseguridad se efectúa a través de un gobierno multinivel, que incentiva la participación de Provincias y Territorios, con la gestión de diversas instituciones especializadas en la temática, y la inclusión con carácter prioritario, del sector privado y académico. Aunque hay opiniones opuestas sobre la suficiencia de sus propuestas para garantizar la seguridad en el ciberespacio, es indiscutible su interés por lograr

tal protección, ya que las tecnologías digitales se consideran un motor para su crecimiento y desarrollo económico. Por ello, el Gobierno de Canadá no deja de estar exento de innumerables vulnerabilidades que son constantemente explotadas por adversarios extranjeros, estatales o no estatales, ya que mientras más dependencia exista a las plataformas digitales, más indefenso se puede estar.

Es difícil afirmar plenamente cuál es el camino adecuado que debe seguirse en materia de ciberseguridad, sin embargo, es evidente que en Canadá se produce un esfuerzo latente por determinarlo. Siendo líder en el escenario internacional en este sector, a la par de Reino Unido o los Estados Unidos de América, concede gran relevancia al fomento de la integración y cooperación de distintos actores para una mayor protección ante el desarrollo indetenible de las ciberamenazas.

5. BIBLIOGRAFÍA

Atlantic Canada Opportunities Agency. 2017. "Canadian Institute for Cybersecurity opens at the University of New Brunswick". https://www.canada.ca/en/atlantic-canada-opportunities/news/2017/01/canadian-institute-cybersecurity-opens-university-new-brunswick.html (Mayo 01, 2019)

Brent J. Arnold. 2018. "Cyber Security in Canada: Structure and Challenges." En *Governing Cyber Security in Canada, Australia and the United States (Special Report):* 5-7 Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf (Noviembre 15, 2018)

Canadian Centre for Cyber Security. 2018. "About the Cyber Centre". https://www.cyber.gc.ca/en/about-cyber-centre (Abril 29, 2019)

Comité Interamericano Contra el Terrorismo. 2012. "Organización de los Estados Americanos y el Gobierno de Canadá Cooperan en Seguridad Cibernética**."** En *Newsletter nro. 90*. Organización de los Estados Americanos. http://www.oas.org/en/sms/cicte/CICTE-newsletter/cicte_news_oct_2012.html (Mayo 17, 2019)

Comité Interamericano Contra el Terrorismo. 2018. "Proyecto de Plan de Trabajo del Comité Interamericano Contra el Terrorismo para el 2018-2019." Organización de los Estados Americanos, 18vo Período Ordinario de Sesiones. http://www.oas.org/en/sms/cicte/documents/sessions/2018/doc%208%20Plan%20de%20Trabajo%20CICTE01207S03.doc (Mayo 17, 2019)

Communications Security Establishment. 2018. "Canadian Centre for Cyber Security". https://cse-cst.gc.ca/en/backgrounder-fiche-information (Abril 29, 2019)

Department of Public Safety and Emergency Preparedness. 2019. "Cyber Security in Canada: Renewing Our Approach". https://www.publicsafety.gc.ca/cnt/cnslttns/cbr-scrt/rnwng-

pprch-en.aspx (Febrero 4, 2019)

Dupont, Benoît. 2018. "Mapping the International Governance of Cybercrime" En *Governing Cyber Security in Canada, Australia and the United States (Special Report):* 23-27 Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf (Marzo 23, 2019)

Europa Press. 2017. "La UE y Canadá reforzarán su cooperación en ciberseguridad y acuerdan intercambiar información clasificada." https://www.europapress.es/internacional/noticia-ue-canada-reforzaran-cooperacion-ciberseguridad-acuerdan-intercambiar-informacion-clasificada-20171204194323.html (Mayo 18, 2019)

ESET Survey Report Canada. 2018 . "ESET Cybersecurity Barometer Canada 2018". https://www.welivesecurity.com/wp-content/uploads/2018/11/ESET_Cybersecurity-Report2018.pdf (Mayo 01, 2019)

Get Cyber Safe. 2018. "About Get Cyber Safe". https://www.getcybersafe.gc.ca/cnt/bt/index-en.aspx (Abril 29, 2019)

Global Forum on Cyber Expertise. 2019. https://www.thegfce.com/ (Mayo 05, 2019)

Government of Canada. 2010. *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada.* Ottawa - Ontario: Public Safety Canada 2010. http://publications.gc.ca/site/eng/9.693830/publication.html (Noviembre 24, 2018)

Government of Canada. 2018. *National Cyber Security Strategy: Security and prosperity in the digital age.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl- cbr-scrt-strtg-en.pdf (Noviembre 13, 2018)

Innovation, Science and Economic Development Canada. 2015. "Digital 150." http://www.ic.gc.ca/eic/site/028.nsf/eng/home (Mayo 01, 2019)

International Telecommunication Union. 2017. "Global Cybersecurity Index 2017". https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Noviembre 15, 2018)

International Telecommunication Union. 2018. "Global Cybersecurity Index 2018". https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Mayo 05, 2019)

Méndez, José Luis. 2000. "La Política Pública Como Variable Dependiente: Hacia un Análisis Más Integral de las Políticas Públicas." En *Lecturas Básicas de Administración y Políticas Públicas*, 75-110. http://www.jstor.org/stable/j.ctv6jmx1d.7 (Febrero 18, 2019)

Organización para la Cooperación y el Desarrollo Económicos (OECD). 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.* OECD Digital Economy Papers, No.
211. Paris: OECD Publishing. https://doi.org/10.1787/5k8zq92vdgtl-en (Noviembre 24, 2018)

Pons Gamón, V. 2017. "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". En *Revista Latinoamericana de Estudios de Seguridad*, 20: 80-93. https://dialnet.unirioja.es/servlet/articulo?codigo=6110845 (Enero 15, 2019)

Sancho Hirare, Carolina. 2017. "Ciberseguridad. Presentación del dossier" En URVIO, Revista Latinoamericana de Estudios de Seguridad, 20: 8-15. https://revistas.flacsoandes.edu.ec/urvio/article/view/2859/1603 (Febrero 18, 2019)

Snyder, Don, et al. 2015. "Cybersecurity Management." En *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*, 1-17. http://www.jstor.org/stable/10.7249/j.ctt19rmd15.7 (Febrero 24, 2019)