UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE RELACIONES INTERNACIONALES

LA CREACIÓN DE ESTRATEGIAS NACIONALES EN CIBERSEGURIDAD COMO ACCIONES NECESARIAS PARA EL FUNCIONAMIENTO DE LAS ADMINISTRACIONES PÚBLICAS EN AMÉRICA LATINA

CURSO DE ESPECIALIZACIÓN EN INSTRUMENTOS JURÍDICOS NACIONALES E INTERNACIONALES SOBRE SEGURIDAD DIGITAL EN EL SALVADOR

PARA OBTENER EL TÍTULO DE

LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTADO POR:

JACQUELINE BEATRIZ MENDOZA VÁSQUEZ

DOCENTE ASESOR:

JORGE ALBERTO ARANDA

CIUDAD UNIVERSITARIA, SAN SALVADOR, OCTUBRE DE 2021

LA CREACIÓN DE ESTRATEGIAS NACIONALES EN CIBERSEGURIDAD COMO ACCIONES NECESARIAS PARA EL FUNCIONAMIENTO DE LAS ADMINISTRACIONES PÚBLICAS EN AMÉRICA LATINA

RESUMEN

Este ensayo plantea la necesidad de crear Estrategias Nacionales en Ciberseguridad para el funcionamiento eficiente y eficaz de los servicios públicos en Latinoamérica como una estrategia capaz de dar respuesta a los nuevos desafíos derivados del uso de las TIC's y demás herramientas tecnológicas para garantizar y o avanzar en el funcionamiento total de las administraciones públicas latinoamericanas. Se delinea un breve esbozo sobre algunos procesos modernizadores que han tenido lugar en la región y se describe la experiencia de cuatro países latinoamericanos en la creación de estas estrategias. Se concluye que las reformas de Estado y los avances tecnológicos conducen a adaptarse a estos cambios y dar respuesta a las amenazas en el ciberespacio.

INTRODUCCIÓN

Los diferentes puntos de inflexión que tuvieron lugar el siglo pasado han delineado el mundo como lo conocemos hoy en día. Desde la creación de organismos internacionales para la búsqueda de la paz hasta la aparición del internet, han implicado un cambio drástico en las formas de comunicación y realización de actividades. El sujeto e impulsor de buena parte de estos cambios ha sido el actor internacional por excelencia, el Estado. De tal manera que conforme ha avanzado el tiempo se han puesto en marcha diferentes maneras de manejar lo público.

Desde finales de siglo pasado los Estados latinoamericanos han iniciado la implementación de diferentes iniciativas para brindar servicios públicos de calidad, emprendiendo procesos modernizadores diferentes entre sí. El último de estos procesos de modernización incluye el uso de las Tecnologías de la Información y de herramientas tecnológicas en la administración pública de forma masiva. Sin embargo, han surgido numerosas vulnerabilidades tanto físicas como lógicas en los sistemas operativos de ciberseguridad utilizados en instituciones del sector público. La creación de Estrategias Nacionales de Ciberseguridad se vuelve prioritario y

necesario para trazar los lineamientos a seguir para garantizar el funcionamiento de las administraciones públicas.

Este ensayo académico busca reseñar las diferentes estrategias que se han implementado en Latinoamérica en la búsqueda de modernización del Estado. Continuando con la ejemplificación de cuatro casos emblemáticos de países latinoamericanos en la creación de Estrategias Nacionales en Ciberseguridad. Y, finalmente se presenta la experiencia salvadoreña en cuanto a ciberseguridad y su avance en la creación de medidas en la materia

EL PROCESO DE MODERNIZACIÓN DEL ESTADO EN LATINOAMÉRICA

Administrar los asuntos públicos conlleva ejecutar una serie de acciones más bien complicadas de realizar por la complejidad misma de lo que implican. La administración pública como ente encargado de los servicios y asuntos públicos ha registrado un sinnúmero de reformas para mejorar la organización y funcionamiento de ésta. Este conjunto de procesos de reformas está dado por la preocupación en la prestación de servicios, eficiencia y eficacia pública, descentralización territorial, mayor participación privada y ciudadana, etc. Todas estas estrategias involucran una completa transformación de las diferentes políticas gubernamentales y la burocracia bajo la lógica de recolección y canalización de demandas y estrategias.

Dentro de este contexto surge la interrogante, ¿Cómo se puede caracterizar a la administración pública latinoamericana? Esta respuesta conlleva factores comunes pero diferenciados. Las diferencias son dadas por los contextos nacionales de cada nación tales como la densidad poblacional, la extensión territorial, la forma de gobierno, etc. Pero, en conjunto, se les podría definir a algunas como administraciones públicas fuertemente centralizadas, altamente burócratas, con tendencia al populismo, con altos índices de corrupción, entre otros rasgos.

Es así como los Estados latinoamericanos y consecuentemente sus respectivas administraciones públicas realizan prácticas en su actividad administrativa que han sido catalogadas en numerosas ocasiones como ineficientes. Desde hace décadas se ha intentado contrarrestar estas prácticas y dar respuesta a los fenómenos que causan este retroceso en la gobernabilidad, Estado de derecho y desarrollo. Las iniciativas varían, pero

uno de los objetivos es la modernización del Estado para garantizar el manejo óptimo de los recursos públicos y los servicios públicos de calidad.

Estos procesos modernizadores de Estado pueden implementarse en los tres poderes u órganos que lo componen siendo estos el Legislativo, el Judicial y el Ejecutivo. Este último es el órgano encargado de la administración pública por excelencia. Estas reformas buscan la reconstrucción de la relación rota del ciudadano con el Estado por la burocracia. De manera general, el proceso de modernización del Estado pretende reducir el exceso de leyes, reglamentos, procesos engorrosos para concretizar dinámicas que fortalezcan las acciones estatales. Asimismo, se implementan primordialmente para que el manejo de recursos públicos se realice de forma más eficiente y eventualmente lograr el mejoramiento progresivo del funcionamiento de otras áreas.

En Latinoamérica, estas reformas iniciaron el siglo pasado y fueron la respuesta a las realidades nacionales de cada país. Fenómenos tales como la polarización, la desigualdad, la sobrerregulación, la burocracia, se presentaban como obstáculos en la optimización del quehacer público latinoamericano. Se debe tener en cuenta que los procesos reformatorios aplicados han variado cada periodo, implicando el involucramiento total del Estado o la búsqueda de la reducción de este.

Como antecedentes inmediatos de las reformas a la administración pública en Latinoamérica se tienen el Estado de Bienestar de John Maynard Keynes[1] y el estructuralismo[2] de la CEPAL. Ambas fueron medianamente funcionales hasta los años 70´s; pues desde esa década se vuelve visible cómo el gasto fiscal y la burocracia impedían el funcionamiento del Estado latinoamericano.[3] Fue precisamente la crisis de la deuda externa en la región, el detonante que llevó a la implementación de los denominados Programas de Ajuste Estructural (PAE). El resultado del Consenso de Washington incluyó

[1] La teoría del Estado de Bienestar o Keynesianismo tiene como principios económicos el estímulo a una política de intervencionismo estatal, a través de la cual el Estado utilizaría medidas fiscales y monetarias con el objetivo de mitigar los efectos adversos de las recesiones, depresiones y períodos de auge económico.

[2] El estructuralismo sostiene que el deterioro de los términos de intercambio en el comercio internacional con un esquema centro industrial- periferia agrícola reproduce el subdesarrollo y amplía la brecha entre países desarrollados y países subdesarrollados. Dadas estas condiciones estructurales, el estructuralismo postula que los países no desarrollados deben tener Estados activos con políticas económicas que impulsen la industrialización a fin de lograr unas condiciones de desarrollo autónomo.

[3] María Fernanda Ramírez*, "Las reformas del Estado y la administración pública en América Latina y los intentos de aplicación del New Public Management",* Estudios Políticos, no. 34 (2009): 119 https://www.redalyc.org/articulo.oa?id=16429062006.

una política neoliberal y PAE´s que delineaban la privatización, reformas tributarias, gasto público, desregulación, liberalización comercial y financiera, etc.

La implementación de estos Programas de Ajuste Estructural era clave en tanto las administraciones públicas presentaban también graves problemáticas socioeconómicas y déficits en la calidad de servicios públicos. Los caudillismos o neocaudillismos estaban siempre presentes en los diferentes gobiernos, sin importar la línea ideológica y eran fenómenos difíciles de disuadir. Además, algunas instituciones públicas latinoamericanas distribuían el manejo estatal en marcadas dosis de partidocracia que las convertía en una especie de entidad al servicio de diferentes sectores. De tal manera que eran fenómenos varios los que se intentaban superar mediante la implementación de estos Programas de Ajuste Estructural.

En teoría, las estrategias de *descentralización, privatizaciones, desregulación, reducción del personal en la administración pública*,[4] debían cambiar estas dinámicas. Pero, ¿cuáles fueron los resultados de la implementación de estas medidas? Al respecto se tiene que, para 1997 los resultados eran más bien agridulces; pues estas medidas crearon sociedades latinoamericanas más polarizadas. De nuevo, se necesitaban estrategias para dar respuesta a esto y dotar al Estado de capacidad funcional y organizativa, volverlo más eficiente y transparente en su actividad. Se buscaba eficacia de la intervención estatal, eficiencia económica de la provisión y mejoramiento de los servicios públicos y creación de un entorno para desarrollo del sector privado.[5] Esto se podía lograr a través de las reformas de segunda generación siendo estas: la reconfiguración de la administración pública, reestructuración del gobierno nacional y local, reforma legislativa.[6]

Estas iniciativas coinciden con reformas administrativas implementadas por países de la Organización para la Cooperación y el Desarrollo Económico (OCDE), bajo la denominación de *New Public Management.*[7] En el caso de América Latina estas estrategias buscaban mejorar la gobernabilidad del Estado mediante el fortalecimiento estatal; para así concretar un Estado capaz de garantizar elementos básicos de gobernabilidad. La New Public Management se presentaba entonces como otra nueva estrategia de gestión pública

[4] Ibid. 122.
[5] Ibid. 124.
[6] Ibid.
[7] La Nueva Gestión Pública por su traducción al español.

para mejorar los servicios públicos. Y se planteaba también como una forma de aplicar un poco de lo privado en lo público.

Esta estrategia buscaba mejorar la *planificación estratégica, mejora de sistemas de gestión presupuestaria y financiera, gestión orientada a resultados, protección del consumidor y suministros de servicios públicos.*[8] Entre todas las reformas de este modelo, la profesionalización de los funcionarios y servidores públicos fue y ha sido desde siempre una de las más difíciles y complejas. Las administraciones públicas latinoamericanas, como ya se mencionó, se han caracterizado por marcadas prácticas de partidocracia que han implicado altos índices de nepotismo.

La implementación de estas medidas fue relativa por las características estructurales e históricas de la región en relación al servicio civil y a los altos índices de corrupción. También fue especialmente complicado por la presión que ejercían los organismos internacionales a administraciones públicas que no se mostraban listas para las medidas. Además del hecho que la puesta en marcha de estas reformas modernizadoras era el intento de replicar el éxito de estas en contextos completamente diferentes.

De igual manera, y de forma paralela se han implementado procesos modernizadores del Estado cuyo centro y fin es el ser humano. De acuerdo a Armatya Sen las personas podrán beneficiarse del desarrollo en tanto amplíen su rango de toma de decisión y posibilidades. Sin embargo, el valor del capital humano puede medirse, por ejemplo, en los años estudiados por una persona, o por dimensiones socioemocionales. La primera hace referencia a las capacidades cognitivas de las personas y la segunda, a factores como la determinación, salud de una persona.

En el sector público las tendencias de desarrollo del capital humano se refieren al diseño organizacional, al liderazgo, a la cultura, y al aprendizaje. Estas iniciativas reconocían la necesidad de aumentar las capacidades de los individuos que conforman el entramado de instituciones del aparato estatal. Buscaban alejarse de prácticas generalizadas en las administraciones públicas que estableciesen jerarquías y contrata a servidores y funcionarios públicos que contasen con las capacidades para sus puestos.

[8] María Fernanda Ramírez, "Las reformas del Estado y la administración pública en América Latina y los intentos de aplicación del New Public Management",", Estudios Políticos, n° 34 (2009): 129 https://www.redalyc.org/articulo.oa?id=16429062006.

La inversión en capital humano daba paso a que el sector público generase cambios acelerados en relación a prácticas pasadas. Un manejo eficiente del recurso humano que forma parte de las administraciones públicas significaría una restructuración de las actividades de líderes y de los consiguientes resultados. Al mismo tiempo consolidaría una función pública de calidad, establecería mecanismos de profesionalización de los funcionarios, promovería sistemas transparentes y eficientes de selección de servidores públicos. Y, sobre todo permitiría que el gasto en salario fuese acorde a la experiencia, conocimientos y habilidades del funcionario o servidor público.

Por otro lado, en las últimas décadas las administraciones públicas de todo el mundo han incluido en sus actividades más y más herramientas tecnológicas. La innovación de las TIC's[9] ha sido el resultado de los aportes emanados desde diferentes posiciones en la sociedad. En consecuencia, dicha innovación ha sido enriquecida por aportes por parte de especialistas, ingenieros informáticos y por la academia. En las instituciones públicas, la tecnología utilizada ha dinamizado completamente la experiencia tanto para los empleados y funcionarios públicos como para los ciudadanos. Las interacciones y transacciones digitales entre gobiernos-ciudadanos son innumerables por lo que estrategias como el *gobierno electrónico*[10] o la *administración electrónica*[11] son pilares dentro de los planes de gobierno de las administraciones públicas.

En efecto, el uso de las nuevas tecnologías contribuye al entramado de procesos y actividades institucionales de los gobiernos. La digitalización del intercambio de información, los servicios electrónicos digitales y la red de sistemas de información interconectados se han vuelto indispensables para las administraciones públicas. La transformación digital busca garantizar el acceso fácil y rápido a los datos de los ciudadanos, esto supone que la planificación y realización de las actividades de cada Estado se realice de forma más eficiente y eficaz.

[9] Tecnologías de la Información y Comunicación.

[10] El término Gobierno electrónico se refiere al uso de las TIC en los órganos de administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar la eficiencia, transparencia y la participación ciudadana.

[11] Administración Electrónica se basa en el uso de las tecnologías de la información y comunicación para diseñar, desarrollar e implementar herramientas y entornos que permitan la comunicación, las gestiones y los trámites de la ciudadanía y las empresas con la administración, apoyada y motivada por cambios organizativos y jurídicos constantes.

La inmersión de las actividades administrativas del sector público en el ciberespacio supone que estos procesos de modernización del Estado impliquen un uso constante, activo y permanente de herramientas tecnológicas. Se tiene como resultado que, de forma simultánea al marcado progreso que los recursos tecnológicos proveen, han aparecido también, un sinnúmero de peligros en la red. El uso de estos recursos tecnológicos representa para el funcionamiento de la administración pública la exposición a, por ejemplo, el robo de información sensible. Las ciberamenazas se convierten en una constante en el ciberespacio que está siempre presente y que de manera real y directa puede afectar el accionar, eficiencia y eficacia de las administraciones públicas.

Casos emblemáticos en la creación de Estrategias Nacionales en Ciberseguridad: las experiencias de Argentina, Brasil, Chile y Costa Rica

Sin lugar a dudas, el papel que tiene actualmente la ciberseguridad en las administraciones públicas es clave y primordial. Desde el ciberataque de Tallin, Estonia en 2007[12] la necesidad de crear una Estrategia Nacional de Ciberseguridad se convirtió en una exigencia a nivel mundial. Para 2011 más de setenta países habían creado y presentado estrategias de ciberseguridad. Inicialmente estos documentos tenían una marcada línea en pro de la seguridad nacional. Los avances han sido significativos y las prioridades se han diversificado de manera tal que, para 2019 los gobiernos del mundo destinaron un trillón de dólares para ciberseguridad.[13]

Las vulnerabilidades son claras, los ataques representan un crecimiento notable entre los países. Quienes cometen estos ataques en la red son conocidos y se distinguen unos de otros como ciberdelincuentes, terroristas, hacktivistas, personas con información privilegiada y script kiddies.[14] Se distingue también, la figura de Estados y amenazas que son patrocinadas por otros Estados, entre otras, las cuales merman el funcionamiento regular del Estado. Y, ¿de qué manera realizan estos ataques? mediante malware,

[12] Este ataque tuvo como efecto detonante el cambio de la estatua en honor al Ejército Rojo desde la capital, Tallin, hacia un cementerio militar en un suburbio ubicado en la misma capital de Estonia. Esto generó discordia entre ruso parlantes y los medios de lengua rusa en Estonia. Estos grupos respondieron con ciberataques hacia la banca, la prensa, organismos gubernamentales. Se saturaron los servidores de tal manera que empleados públicos no podían acceder ni siquiera a sus correos electrónicos.

[13] Juan Manuel Aguilar, "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas" Revista de Estudios en Seguridad Internacional, no. 2 (2020): 19

[14] Candela Justribó, Sol Gastaldi y Jorge A. Fernández, *"Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político- institucional y normativo",* (Argentina: Escuela de Defensa Nacional, 2014): 8.

denegación de servicios, botnets, phishing, correo basura, ramsonware, violación de datos, robo de identidad y ciber espionaje etc.

Los esfuerzos para lograr niveles aceptables en ciberseguridad han tenido lugar de manera paulatina en los últimos años concretándose mediante la creación de Estrategias Nacionales en Ciberseguridad. Estas *Estrategias Nacionales en Ciberseguridad (ENCS)* se convierten en un plan nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio. Esto es primordial en tanto se da respuesta a los ciberataques y ciberamenazas, se protege la infraestructura, los softwares, hardware, equipos informáticos utilizados en los gobiernos.

En la región latinoamericana lograr concretizar la ciberseguridad como uno de los ejes centrales en las agendas públicas nacionales debería ser una prioridad máxima. Esto bajo la premisa que comprende a la seguridad y por consiguiente a la ciberseguridad como pilar para lograr la gobernabilidad. Es así como la ciberseguridad es una condición básica para que los ciudadanos puedan beneficiarse del ciberespacio y se vuelve garante del funcionamiento de la administración pública.

Cabe aclarar que, América Latina como concepto es inmensamente complejo y amplio. Por lo tanto, a razón de realizar una ejemplificación del caso en estudio en que a la región respecta, se ha tomado a bien describir la experiencia de cuatro países cuyos avances en ciberseguridad son destacables. Esto, sin obviar que, por supuesto otros países también cuentan con índices altos y valiosos sobre ciberseguridad.

En ese sentido, Argentina ha sido pionero en la creación de medidas de ciberseguridad. Para 2004 mediante su Oficina Nacional de Tecnologías de Información creó su primera Política de Seguridad Modelo.[15] Se instauró un Comité de Seguridad de la Información adscrito al Ministerio del Interior y Transporte; el cual se encarga de supervisar la investigación y monitoreo de incidentes de seguridad.[16] También aprueba metodologías y

[15] Ministerio del Interior y Transporte, "Política de Seguridad de la Información", (Buenos Aires: Ministerio de Justicia y Derechos Humanos, 2012) http://servicios.infoleg.gob.ar/infolegInternet/anexos/200000-204999/200528/norma.htm
[16] Ibid.

procesos de la seguridad de la información, evalúa y coordina controles específicos de seguridad de la información para nuevos sistemas y servicios, entre otras.[17]

En el año 2011 lanzó su Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad para desarrollar políticas y regulaciones para proteger las infraestructuras estratégicas de la información de Estado.[18] Adscrito a este programa se crearon el Equipo de Respuesta ante Emergencias Teleinformáticas, el Grupo de Acción Preventiva, el Grupo de Infraestructuras Críticas de la Información. Este programa jugaba un rol importante pues era el encargado de coordinar los diferentes actores para la posterior creación de la ENCS.

Creada en 2015 esta ENCS tiene como principios rectores el respeto por los derechos y libertades individuales, la construcción de capacidades y fortalecimiento federal sobre ciberseguridad.[19] De igual manera busca generar mecanismos de cooperación internacional en esta materia, además de implementar una cultura de ciberseguridad y fortalecer el desarrollo socioeconómico aprovechando los beneficios del ciberespacio seguro.[20] En cuanto a objetivos, pretende crear conciencia mediante educación y capacitación sobre el uso del ciberespacio, desarrollar un marco normativo, proteger-recuperar los sistemas de información del sector público.[21] Y, finalmente tiene como objetivo el contribuir a las medidas de ciberseguridad en el plano regional e internacional.[22]

Brasil por su parte, como parte de su rol de liderazgo en la región a nivel político y económico, también ha sido punta de lanza en materia de ciberseguridad. Y es que su realidad nacional en cuanto a ciberamenazas y ciberataques es directamente proporcional al tamaño de su economía y de su densidad poblacional. Se crearon la Estrategia Nacional de Defensa, la Política Cibernética de Defensa, y la Estrategia de Seguridad de la Información y Comunicaciones de la Administración Pública Federal.[23]

---

[17] Ibid.
[18] Poder Ejecutivo Nacional, "Estrategia Nacional de Ciberseguridad de la República Argentina" (Ciudad Autónoma de Buenos Aires: Comité de Ciberseguridad, 2019) https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Luisa Cruz Lobato, "La política brasileña de ciberseguridad como estrategia de liderazgo regional", Revista de Estudios de Seguridad, No 20 (2017): 16-30 https://revistas.flacsoandes.edu.ec/urvio/article/view/2576

Esta Estrategia Nacional de Ciberseguridad plantea la creación de una institución central que dirija al sistema nacional para que coordine y evalúe los esfuerzos nacionales en esta materia. Busca reforzar la capacidad de respuesta ante ciberataques a través de la creación de alianzas público-privadas. Además de generar procesos de cooperación internacional para la ciberseguridad y el intercambio de experiencias y conocimiento técnico. También se pretende proteger las infraestructuras críticas y resaltar la importancia de la resiliencia en esta temática.[24]

El caso de Chile es destacable por los resultados obtenidos con diferentes modelos de desarrollo los cuales han sido catalogados como parcialmente exitosos, por ejemplo, con las medidas liberales. Este país ha tenido experiencias valiosas incluso con la implementación de las estrategias del New Public Management. Por lo que también ha destacado en la implementación de medidas de ciberseguridad a través de su Política Nacional de Ciberseguridad. Esta política busca ejecutar medidas que puedan arrogar resultados en el corto y mediano plazo y crea las instituciones garantes de la ciberseguridad en la nación.[25]

Plantea un conjunto de objetivos para 2022 entre los cuales destaca el desarrollo de una infraestructura de las TIC que resista incidentes de ciberseguridad. También implica promover una cultura de ciberseguridad relativa al uso de las TIC, propiciar relaciones cooperativas y ejecutar un rol activo en lo regional-internacional en materia de ciberseguridad. Y principalmente plantea garantizar los derechos de los ciudadanos a la protección de sus datos y de ciberdelitos.[26]

Finalmente, en Costa Rica el proceso de desarrollo de la ENCS se construyó con base a una consulta multisectorial lo que la vuelve una experiencia enriquecedora. Esta experiencia de Costa Rica en la creación de su Estrategia Nacional de Ciberseguridad contrario a los casos anteriormente desarrollados, coloca a la persona como prioridad máxima. Al mismo tiempo pretende a través de la educación capacitar a profesionales nacionales que propongan acciones de ciberseguridad. Busca garantizar el respeto a los

[24] Ibid.
[25] José Carlos Hernández, "Estrategias Nacionales de ciberseguridad en América latina", Grupo de Estudios en Seguridad Internacional, (2018): 5
[26] Ibid.

derechos humanos y a la privacidad, coordinar a las partes interesadas y propiciar procesos de cooperación internacional para mejorar las cibercapacidades.[27]

La Estrategia Nacional de Ciberseguridad en El Salvador: innovación sin preparación no es suficiente

En el país las diferentes iniciativas relacionadas al uso, manejo y aprovechamiento de las Tecnologías de la Información datan desde finales del siglo pasado. Estas iniciativas han buscado abonar de manera directa a la calidad y optimización de los servicios públicos. Sin embargo, este proceso de modernización del Estado salvadoreño se ha caracterizado por ser paulatino e incluso un tanto lento.

En ese sentido, las estrategias de modernización estatal inician en 1999 con la creación de Infocentros Comunitarios para dar acceso a servicios de información y comunicaciones.[28] En estos telecentros se ofrecían servicios como: teléfonos, acceso al internet, correo electrónico. La Política Nacional de Informática del año 2000 pretendía mejorar el manejo-administración de información, aprovechamiento de la infraestructura, interconectividad y las redes de datos de ese momento. En el 2003 se implementó la Primera Agenda eLAC en el país para el uso de las TIC en el desarrollo; se habilitó el pago de renta online.

Por otra parte, en el año 2010 se crea la Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador y el Centro de Trámites de Importaciones y Exportaciones, CIEX como primera ventanilla única. Y para 2017 se creó el portal www.tramites.gob.sv.es el cual reúne servicios como la creación de empresas, la obtención de patentes, depósito de obras, registro de marcas, etc.

Actualmente, los lineamientos de modernización estatal en el país bajo el gobierno del presidente, Nayib Bukele, están dados por la Agenda Digital 2020-2030. Esta estrategia fue creada para suprimir la duplicación de esfuerzos en gobernanza digital, al mismo tiempo que se asignan recursos para crear mecanismos de seguimiento a estas iniciativas. El logro de estos objetivos se refuerza por normativa vigente como la Ley de Firma Electrónica, Ley Especial contra Delitos Informáticos y Conexos, Política Nacional de Datos Abiertos, etc. Todo esto busca impulsar una estrategia nacional innovadora,

[27] Ibid.
[28] "Agenda Digital Nacional 2020-2030: Plan de Desarrollo El Salvador Digital, Secretaria de Innovación de la Presidencia, (2020)

colaborativa, que sea capaz de estimular el emprendedurismo, la igualdad y la inclusión de todos los sectores de la ciudadanía.[29]

Es así como el pasado mes de abril la Dirección de Identidad Digital creó la Política de Ciberseguridad la cual fue aprobada por la Secretaría de Innovación. Esta política busca establecer el marco estratégico para el gobierno en relación a la prevención de ciberamenazas y ciberataques, definiendo también las instancias encargadas de cada estrategia. Pretende también crear capacidades cibernéticas que permitan al gobierno proteger las infraestructuras críticas, y fortalecer el nivel de respuesta ante los ataques. Y ha sido creada para dotar a entidades públicas y privadas del conocimiento técnico requerido para garantizar el aprovechamiento del ciberespacio y crear cultura de seguridad informática.[30]

Esta Política de Ciberseguridad define ocho estrategias a través de las cuales se dará respuesta a lo anteriormente desarrollado, primeramente, garantizando la seguridad y resiliencia de activos estratégicos. Se contempla también la creación de una entidad que coordine la ciberseguridad en el territorio nacional; la puesta en marcha de campañas para concientización sobre esta materia. Asimismo, persigue el reforzamiento de capacidades de ciberseguridad hacia las amenazas capacitando a los empleados públicos para esto. También propone reforzar el marco jurídico de ciberdelitos y la cibercriminalidad. Busca identificar, analizar y gestionar el riesgo de los peligros en el ciberespacio; promover estrategias de ciberseguridad en el plano internacional y fortalecer al equipo de respuesta ante ciberataques.[31]

Para el país esta Política de Ciberseguridad es lo que se asemeja de manera más reciente a una Estrategia Nacional sobre Ciberseguridad. Pero luego de pocos meses desde su creación, ¿Cuáles son las estrategias que han comenzado a implementarse? Pues bien, los resultados son más bien inconclusos por el momento. No se cuenta con un registro específico o campañas de información sobre la implementación de lo estipulado en dicha política, aunque registra apartados sobre educación en la materia. Solamente se puede visitar el sitio https://www.presidencia.gob.sv/ciberseguridad/ donde se enumeran los

[29] Ibid.
[30] "Política de Ciberseguridad de El Salvador", Secretaría de Innovación de la Presidencia, (2020): 4
[31] Ibid.

objetivos del gobierno en ciberseguridad, sin describir o mencionar cómo se logrará lo planteado.

Per se, la implementación aún no inicia, además no se ha informado a la población el nombre de la entidad coordinadora de ciberseguridad en el país. Por ejemplo, la aprobación de la Ley Bitcoin, y su reciente entrada en vigor debió haber sido una acción coordinada entre esta entidad y el gobierno. Sin embargo, el lanzamiento de la aplicación de la cartera virtual, *Chivo Wallet*, visibilizó una mala coordinación y falta de conocimiento de creación de aplicaciones celulares. Sin mencionar que, por la naturaleza de estas transacciones se debieron iniciar campañas de información y educación masiva incluso antes de la aprobación de la ley.

También, a pesar de que incluye elementos relativos a la creación de una cultura cibernética, no contempla mecanismos de presentación de informes. En este sentido, este escenario sí corresponde a los lineamientos desarrollados por la actual administración en relación a la apertura sobre transparencia y acceso a la información pública. Así, más allá de los procesos modernizadores se denota que innovación sin la preparación idónea no es suficiente.

Lo que sí resulta destacable es la creación de un Equipo de Respuesta ante Emergencias Informáticas, SalCERT, el cual es responsable de responder a diferentes incidentes informáticos. Se han creado también empresas privadas que proveen servicios de seguridad cibernética. Esto demuestra que el sector privado es consciente de la importancia de la inversión e innovación en esta materia. Sin embargo, se desconoce si estas fueron tomadas en cuenta para el diseño de la Política de Ciberseguridad.

Lo que se debe tener en cuenta es que, la realidad nacional dicta que se debe iniciar con la implementación de las estrategias de esta Política de Ciberseguridad. En los últimos meses, también los casos de phishing que ha sufrido la banca nacional demuestran la falta de conocimiento sobre los peligros del ciberespacio. Se vuelve visible la necesidad de que se realicen campañas de concienciación sobre ciberseguridad que contempla esta política, pues los escenarios existentes reflejan lo apremiante que esto es. No obstante, todavía es

más preocupante si se tiene analiza que el país aún no cuenta con una normativa sobre protección de datos y privacidad.

De estas nuevas realidades, las cuales son claras e inevitables, surge la necesidad de crear Estrategias Nacionales de Ciberseguridad. La implementación de diferentes líneas de acción en materia de ciberseguridad podría no solamente proteger información sensible sino ahorrar y optimizar recursos. Este último factor es clave en las administraciones públicas latinoamericanas, y en especial en la salvadoreña porque tiene otras áreas que demandan igual o mayor atención.

El Salvador desde siempre se ha caracterizado por ser un país con leyes que pueden resultar innovadoras, sin embargo, en la práctica su aplicación básicamente es nula. La creación de estas leyes es necesaria, sí, pero no es la única medida que se debe tomar para dar respuesta a las amenazas del ciberespacio. Se debe buscar que esas políticas y todas las relativas al ciberespacio, protección del usuario, y otras, no se quede en letra muerta.

Los procesos modernizadores iniciados por la administración pública se suelen quedar estancados precisamente porque no se llegan a implementar de forma contundente. Aunque se tiene la intención, no se concretan en la práctica. Es por ello que, se debe buscar dar ese paso extra para concretar procesos que resulten verdaderamente provechosos para la ciudadanía. Y, en un país como El Salvador, donde el gobierno implementa estrategias "innovadoras", esto es vital.

CONCLUSIONES

Desde siempre, las administraciones públicas han sido los actores encargados de suministrar toda clase de servicio público. Hoy en día, la especie de fusión que ha tenido lugar entre las tareas cotidianas de la vida y el ciberespacio es una realidad. Así como también son una realidad los riesgos que este panorama representa. El ciberespacio dejó de ser un escenario en el cual participan solamente algunos actores para ser un escenario que abarca múltiples actores y múltiples perspectivas.

Las iniciativas como el gobierno electrónico o la administración electrónica han contribuido al constante mejoramiento de los servicios públicos. Estas iniciativas dependen de manera directa y casi en su totalidad del uso de las Tecnologías de la Información y Comunicación. Al mismo tiempo que esta relación ofrece mejoras a los procesos

administrativos, también implica la aparición de riesgos inminentes para la ciudadanía. La realización de este tipo de estrategias de modernización del aparato estatal perdería porcentajes significativos de resultados positivos por no garantizar procesos digitales seguros.

Los Estados latinoamericanos se suelen caracterizar por ser Estados cuyos métodos de organización y manejo no han ofrecido los mejores resultados para sus poblaciones. Para solventar esto, la región ha sido objeto de numerosas intervenciones por parte de organismos internacionales con el fin de solventar estas problemáticas diagnosticadas en la administración pública. Es así como el proceso de modernización del Estado en América Latina se ha caracterizado por buscar y utilizar fines y herramientas diferentes entre sí. Desde medidas que perseguían la reducción del Estado en todos los aspectos posibles hasta la puesta en marcha de estrategias centradas en el ser humano.

En ese sentido, cada una de estas iniciativas han pretendido solventar las problemáticas surgidas del mal funcionamiento de la administración pública latinoamericana. De tal forma que, con el transcurso de los años, y con el desarrollo de herramientas tecnológicas, estos intentos de reforma se han vuelto más complejos y elaborados. El proceso modernizador más reciente es el que implica la utilización casi dependiente de las TIC's y de herramientas tecnológicas de forma masiva.

Con el uso activo de aparatos tecnológicos en la administración pública se vuelve visible un grado perceptible de mejora en la calidad de los servicios públicos. Los procesos, trámites y solicitudes de servicios específicos han sido optimizados en la mayoría de los países latinoamericanos, siendo esto solamente uno de los beneficios. Actualmente, además de solventar desafíos propios de la prestación de servicios públicos se deben crear nuevos sistemas de control, regulación, protección de las actividades en el ciberespacio.

La respuesta clave para solventar problemáticas derivadas es la creación de estrategias nacionales de ciberseguridad, las cuales son indispensables para los procesos digitales implementados por las administraciones públicas. Estos procesos serán realizados efectivamente y de manera segura en cuanto se garantice la protección de las transacciones. En el caso de las administraciones públicas latinoamericanas estas medidas deben ser primordiales por los contextos nacionales propios de cada país, pues no se logrará avanzar en cuanto no se garantice un ciberespacio seguro. En este sentido,

experiencias como las de los casos emblemáticos demuestran no solamente la voluntad política sino la concienciación en la materia en los gobernantes de estos países.

Así, con las ENCS las administraciones públicas deben garantizar el cuido de información sensible de los ciudadanos para propiciar la confidencialidad de estos en los servicios públicos. Entre las consecuencias de la falta de ENCS se distingue el riesgo del daño a infraestructuras críticas lo cual puede ser devastador para el panorama de un país. Por ejemplo, en el sector salud en la región se han iniciado procesos de digitalización de los expedientes médicos de la ciudadanía; numerosos procesos de gestión de citas médicas se realizan en línea. El bloqueo de la red de equipos informáticos del sistema hospitalario podría dejar sin acceso a este derecho a muchos ciudadanos.

Es importante la creación de estas ENCS en tanto de manera especial, los gobiernos latinoamericanos deben solventar problemáticas que también requieren una gran cantidad de recursos. Entendiendo que, contrario a países por ejemplo Canadá o Estonia, estas administraciones públicas deben solventar situaciones estructurales como la seguridad o la salud las cuales son deficitarias. Se debe entonces iniciar, de manera pronta, la implementación de medidas de ciberseguridad que sean también preventivas y no solamente respuestas a ataques.

El Salvador igual que otros países de la región se encuentra en una etapa formativa. Esto implica que esta Política de Ciberseguridad por ser nueva aún no ha iniciado una implementación que arroje resultados medianamente significativos. Es importante que, ante el panorama actual, la implementación paulatina de estas se inicie lo más pronto posible para dar respuesta a la coyuntura actual. La importancia de estas ENCS es tanta que abona a salvaguardar la vida misma de las personas.

RECOMENDACIONES

Se recomienda para la creación de futuras investigaciones académicas en la materia:

1. Realizar estudios comparativos relativos al estado de las iniciativas de gobierno electrónico; el impacto final de la pandemia en el retroceso o avance de dichos objetivos.

2. Ampliar el estudio del impacto de las iniciativas mencionadas anteriormente; los resultados de las diferentes líneas impulsadas por los gobiernos para efectuar los cambios necesarios.
3. Analizar el estado de las Estrategias Nacionales en Ciberseguridad en la región.
4. Analizar resultados varios de la experiencia de la implementación de estas ENCS en los países que ya las han creado.
5. Estudiar experiencias de otros países aparte de los presentados en este ensayo en relación al cumplimiento de sus respectivas ENCS.
6. Profundizar en los efectos que ha tenido la pandemia para las administraciones públicas en relación al mayor uso y creación de plataformas digitales. Para esto se puede tomar en cuenta el manejo que han tenido los gobiernos centrales para la divulgación de datos oficiales sobre los casos de Covid-19. También la calidad y el aumento o no de oferta de servicios en línea de forma extra a los que ya se ofrecían previo a la pandemia.

Finalmente se tiene a bien realizar recomendaciones para el cumplimiento de la Política de Ciberseguridad en el país:

1. Iniciar con la puesta en marcha de las medidas que contempla la Política de ciberseguridad en el país.
2. Iniciar lo más pronto posible con la implementación de campañas de concienciación y educación en materia de ciberseguridad para la ciudadanía.
3. Garantizar espacios de dialogo para la inclusión de los diferentes actores nacionales interesados en la temática.
4. Propiciar la creación de estudios superiores en ciberseguridad.
5. Impulsar la especialización de profesionales en ciberseguridad.
6. Impulsar las campañas de concienciación y educación en ciberseguridad.
7. Participar en foros internacionales sobre ciberseguridad.

BIBLIOGRAFÍA

- Agenda Digital Nacional 2020-2030: Plan de Desarrollo El Salvador Digital. Secretaria de Innovación de la Presidencia, (2020). https://innovacion.gob.sv/downloads/Agenda_Digital.pdf
- Aguilar, Juan Manuel. La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. Revista de Estudios en Seguridad Internacional, n. 2 (2020): 29-36. https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/
- Contreras, Belisario y Miguel Porrúa. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y El Caribe. Banco Interamericano de Desarrollo y Organización de los Estados Americanos, (2020). http://dx.doi.org/10.18235/0002513
- Hernández, José Carlos. Estrategias Nacionales de ciberseguridad en América latina. Grupo de Estudios en Seguridad Internacional. (2018). 4-6. https://www.researchgate.net/publication/325397629
- Justribó Candela, Sol Gastaldi y Jorge A. Fernández. Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo. Argentina: Escuela de Defensa Nacional, 2014. http://www.bdo3c.f-sc.org/archives/508.pdf
- Lobato, Luisa Cruz. La política brasileña de ciberseguridad como estrategia de liderazgo regional. Revista de Estudios de Seguridad, n° 20 (2017): 16-30 https://doi.org/10.17141/urvio.20.2017.2576
- Ministerio del Interior y Transporte. Política de Seguridad de la Información. Buenos Aires: Ministerio de Justicia y Derechos Humanos. 2012 http://servicios.infoleg.gob.ar/infolegInternet/anexos/200000-204999/200528/norma.htm
- Paniagua Ramírez, Alejandro. Ciberseguridad para la Administración Pública Federal en México: Propuesta de Política Pública para la Protección de los Sistemas de la Información como Activos Estratégicos de las Instituciones. Tesis de maestría, Instituto Tecnológico y de Estudios Superiores de Monterrey, 2014.

https://www.academia.edu/17017569/Ciberseguridad_para_la_Administraci%C3% B3n_P%C3%BAblica_Federal_en_M%C3%A9xico

- Pisanty, Alejandro. Ciberseguridad nacional. Revista de administración pública, n°1, (2019). https://www.inap.mx/portal/images/pdf/rap148.pdf.
- Poder Ejecutivo Nacional. Estrategia Nacional de Ciberseguridad de la República Argentina. Ciudad Autónoma de Buenos Aires: Comité de Ciberseguridad, 2019. https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf
- Política de Ciberseguridad de El Salvador. Secretaria de Innovación de la Presidencia. https://consulta.innovacion.gob.sv/system/documents/attachments/000/000/003/original/0e8a02f53673daa587b66691b1770faeb1e71c8a.pdf
- Ramírez, María Fernanda. Las reformas del Estado y la administración pública en América Latina y los intentos de aplicación del New Public Management. Argentina: Universidad de Buenos Aires, 2004. https://www.redalyc.org/articulo.oa?id=16429062006.
- Sancho Hirare, Carolina. Ciberseguridad. Presentación del dossier. Revista Latinoamericana de Seguridad. N° 20 (2017). https://revistas.flacsoandes.edu.ec/urvio/article/view/2859
- Valenzuela, Daniel Álvarez. Ciberseguridad en América Latina y ciberdefensa en Chile. Revista chilena de derecho y tecnología, n. 1, (2018). https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071925-842018000100001