entrosur
e-ISSN:2706-6800

Research Open Access

Correspondence:

Análisis del Gobierno digital y su influencia en la ciberdefensa

Analysis of digital government and its influence on cyberdefense

Manuel Antonio Pereyra Acosta
Maestro en ingeniería de sistemas, Universidad Nacional Federico Villarreal, Lima, Perú, manuelpereyraacosta@gmail.com, https://orcid.org/0000-0002-2593-5772

Resumen

El uso moderno y vigente de la tecnología en el ciberespacio permite todas las cosas buenas y malas en nuestra realidad que nos ha tocado vivir. El presente artículo "Análisis del Gobierno digital y su influencia en la ciberdefensa", tuvo como objetivo determinar la influencia del Gobierno digital en la ciberdefesa del Estado peruano, estudio realizado durante el año 2021. El método utilizado fue del tipo descriptivo, con enfoque cualitativo e instrumento de estudio de casos. En primer lugar, se realizó una recopilación de información a través de artículos, trabajos de investigación y libros respecto a dos variables: la ciberdefensa y el gobierno digital; luego se ordeno dicha información de manera lógica y teórica. En segundo lugar, se analizó dos casos de ciberguerra el de Estonia y el de Estados Unidos, como tercer punto se realizó el análisis correspondiente y como resultado brinda recomendaciones para proteger la información digital, producto de las buenas prácticas en seguridad digital. La reflexión final es, tener conciencia de seguridad de la información en toda actividad que se realiza en el uso de las tecnologías de información y comunicaciones.

Palabras claves: Ciberseguridad, ciberdefensa, gobierno digital, transformación digital.

Article

Abstract
The modern and current use of technology in cyberspace allows all the good and bad things in our reality that we have had to live. The present article "Analysis of digital government and its influence on cyber defense", aimed to determine the influence of digital government on cyber defense of the Peruvian State, a study carried out in 2021. The method used was descriptive, with a qualitative approach and case study instrument. In the first place, a compilation of information was carried out through articles, research papers and books regarding two variables: cyber defense and digital government; then this information was ordered logically and theoretically. Secondly, two cyberwar cases were analyzed, that of Estonia and that of the United States, as a third point, the corresponding analysis was carried out and as a result it provides recommendations to protect digital information, a product of good practices in digital security. The final reflection is to be aware of information security in all activities carried out in the use of information and communication technologies.
key words: Cybersecurity, cyber defense, digital government, digital transformation.

Introducción

Desde la aparición de la Internet por los años 70, el mundo ha evolucionado de manera vertiginosa, usando esta herramienta de la tecnología moderna; su creación fue para proteger y brindar seguridad a la información contra cualquier ataque del enemigo y eso fue su motivo principal para ser creada, sin embargo, la transformación digital que experimentan los gobiernos, hoy por hoy, no avizoran los peligros a los que están expuestas nuestras organizaciones y nuestros activos críticos nacionales.

La Ley de gobierno digital en el Perú, tiene por esencia instituir los parámetros de la forma de gobernar usando las tecnologías de información y comunicaciones para una provechosa gestión de la identidad, servicios, arquitectura, interoperabilidad, seguridad y datos digitales, también el aspecto legal aplicable al uso de las tecnologías digitales de manera transversal en la digitalización de los procesos y prestación de servicios digitales por parte del sector público en los tres niveles de gobierno, PCM (2018). El Objeto de esta ley tiene un fin, el de atender al ciudadano peruano de la manera más eficiente y eficaz posible, usando la tecnología; pero su cumplimiento en el Estado peruano no ha demostrado ser muy adecuado por los problemas de seguridad de la información digital en la actualidad.

Compréndase por ciberdefensa a la característica militar que admite proceder delante a las amenazas o ataques ejecutados en y mediante el ciberespacio cada vez que dañen la seguridad de la nación, Ley de ciberdefensa (2019). El ciberespacio es el ámbito donde se desarrolla todo lo digital, hoy en día todo se realiza en el ciberespacio, se compra, se vende, se estudia, se conoce, se diseña, se modela, se paga, entre infinidad de cosas productivas, pero también se realizan robos, chantajes, extorsión, fraude, engaño y todo lo malo que puedan imaginarse puede realizarse ahora usando la tecnología y el ciberespacio. Ese uso moderno y vigente de la tecnología en el ciberespacio permite todas las cosas buenas y malas en nuestra realidad que nos ha tocado vivir.

Con referencia a los trabajos previos revisados en el contexto internacional se tiene a Assante, Roxey y Bochman (2015), cuyo objetivo fue el de analizar la influencia de la automatización de la información en la ciberdefensa del país, trabajo realizado en el centro de Estudios

Estratégicos e Internacionales, concluyen que no es recomendable digitalizar en exceso y es muy importante para la ciberdefensa contar con estrategias de protección de la información; Asimismo, Assante y Bochman (2017) sostuvieron que aprecian un avance oscuro a la internet de las cosas, la automatización, la autonomía y las megas ciudades al año 2025, estudio realizado en el centro de Estudios Estratégicos e Internacionales, concluyendo que se debe de considerar la seguridad digital en todos los campos y aspectos de la sociedad moderna, la tecnología está calando rápidamente en las ciudades, en las infraestructuras criticas sin la seguridad adecuada. Incluso los sistemas más fuertes y seguros son susceptibles a los ataques informáticos. Por otro lado; Ryseff (2017) nos habla de la ciberguerra, nos describe como las guerras han evolucionado desde los principales tanques hasta las actuales ciberarmas, el artículo científico fue escrito para el Centro de estudios estratégicos e internacionales de Los Estados Unidos de América y concluye que se debe de invertir en la ciberdefensa para evitar la crisis como producto de los ciberataques. Siguiendo en el campo de la ciberguerra; Hussain (2019) presento un estudio para el Centro de Estudios Estratégicos e Internacionales de los Estados Unidos, donde nos indica que las guerras cibernéticas buscaran atacar los centros de mando y control y las infraestructuras nucleares, esto producirá un gran daño a los paises, crisis y descontrol. Describe una gran variedad de formas de atacar las computadoras de los centros mencionados anteriormente. Como conclusión, Hussain advierte la destrucción de un país si no se protege adecuadamente la información propia de las infraestructuras tecnológicas de los paises. Orellana, Hinojosa (2019), nos muestra en su artículo publicado para la revista UNIMINUTO de Colombia, que toda transformación digital esta formalmente establecida y muestra prioridad gubernamental por generar un desarrollo y bienestar para Ecuador, el avance de las tecnologías de la información y las comunicaciones están reglamentadas en la constitución nacional de 2008, esto representa un interés nacional el lograr un gobierno digital. Referente a los trabajos examinados en el contexto nacional se tiene a Chacón (2019), donde demostró que se pueden diseñar herramientas para calcular el nivel de cumplimiento de la ejecución del gobierno electrónico en las instituciones públicas del Estado peruano, trabajo elaborado en la Pontificia Universidad Católica del Perú, la muestra utilizada fueron dos gobiernos locales y las metodologías fueron ITIL y COBIT, se concluyó que es posible diseñar herramientas de implementación de e-government dependiente al plan de gobierno digital del Perú. Asimismo, Ormachea (2020), tuvo como objetivo el proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú. El trabajo fue desarrollado en el Centro de Altos Estudios Nacionales (CAEN), de tipo descriptivo y con enfoque epistemológico; además, el diseño fue no experimental y propositivo. La población estuvo conformada por las estrategias y políticas utilizadas en el ámbito internacional para contrarrestar las ciberamenazas, y la muestra estuvo constituida por las estrategias de ciberseguridad implementadas por los Países Bajos, EE. UU., España y Perú. Se encontró que, en los indicadores referidos a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disímiles; además, el Estado y la sociedad peruana aún transitan por los enfoques de la concientización y del desarrollo de las capacidades cibernéticas militares, como indicadores prevalentes en la creación de las políticas de ciberseguridad. Por ello, se concluyó que la ciberseguridad constituye un compromiso social que demanda articulación entre lo público y lo privado, lo que en el Perú aún no se concreta; en consecuencia,

el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha. Al respecto, Taipe (2020), tuvo como objetivo analizar el Sistema de Seguridad Cibernética Nacional frente a los Ciberataques como amenaza a la Seguridad Nacional; dicho trabajo fue desarrollado en el Centro de Altos Estudios Nacionales (CAEN), lo que pretende la investigación es contribuir a la solución del problema presentado; En cuanto a la metodología utilizada, se puede señalar que ha sido de tipo descriptiva, diseño no experimental descriptiva correlacional, como resultados se aprecia que es necesario buscar desarrollar el reforzamiento de la educación, la capacitación y el desarrollo de las líneas de formación profesionales de los especialistas de ciberseguridad, adicionalmente se debe establecer una concientización en materia de ciberseguridad en todas las fases de la formación académica y profesional del ciudadano.

El primer estudio de caso que se analizará será el de Estonia, un país totalmente automatizado; con el documento de identidad nacional, los ciudadanos de este país pueden comprar, vender, realizar pagos a las instituciones públicas y privadas, es un país con su gobierno digital bien establecido y eficiente. Dividida políticamente en 15 condados, una población de 1,3 millones de habitantes, Estonia es uno de los países menos poblados dentro de la Unión Europea (UE), es el centro de alta tecnología en Europa, ocupa los primeros lugares del mundo en creación de Start Ups per cápita, para el año 1998 todas las escuelas ya se encontraban implementadas con computadoras, el senado y parlamento están equipadas con tecnología para emitir sus votos o acuerdos de manera remota y automatizada, en este país se encuentra el centro de cibedefensa de la Organización del tratado del atlántico norte (OTAN). El año 2007, Estonia sufrió ciberataques por medio de varias armas tecnológicas creadas para realizar ciberguerra; virus informáticos, botnets, ataques de denegación de servicio, envenenamiento de DNS, gusanos, troyanos, ingeniería social, snifers y spyware; Estonia culpo al gobierno Ruso de afectar los medios de comunicación, los bancos y diversas entidades e instituciones gubernamentales, un país que quedo en un caos total por tres a cinco días sin poder operar. La UE y la OTAN sirvieron de jueces ante esta cibeguerra, no se pudo confirmar realmente el origen de los ataques, pero sirvió de mucha experiencia para la seguridad en las tecnologías de información, este caso es el primer caso de ciberguerra analizado y evaluado en muchas aulas académicas.

El segundo caso de estudio es el de China contra Estados Unidos, se conoce este caso de estudio como Titan Rain, conjunto de ataques informáticos perpetrados desde el año 2003 hasta el año 2006 en contra de distintas infraestructuras criticas del gobierno de USA; Sandia National Laboratories es una empresa encargada de la investigación y el desarrollo del departamento de energía de los Estados Unidos, esta institución detecto comportamientos no adecuados en las computadoras de la empresa Lockheed Martin, institución del sector defensa del gobierno americano con intereses en todo el mundo. El descubrimiento fue que, durante los años 2003, 2004 y 2005 existían múltiples archivos comprimidos y encriptados para su fácil extracción y robo, rootkits para preservar la infección de manera indetectable y malware encargados de la comunicación con un centro de comando y control alojado en Corea del Sur, luego de estudios realizados y señuelos colocados conocidos como honeypot, se encontró en un equipo servidor, gigabytes de información de archivos robados correspondientes a los programas de defensa de

Estados Unidos, entre ellos información de los proyectos F-22 Raptor y MRO (orbitador de reconocimiento de marte). Finalmente se descubrió que dicha información se compartía con equipos de cómputo de Corea del Sur, Hong Kong y Taiwan, antes de ser enviados a China. Los ataques descubiertos se le atribuyeron al People's Liberation Army (PLA) las fuerzas armadas de China, sin embargo, nunca se determinó a ciencia cierta el origen del ataque. Se cree que los actores responsables de Titan Rain todavía siguen actuando en labores de ciberespionaje.

El actual trabajo de investigación intenta evaluar la implicancia que tiene la Ley de gobierno digital en la ciberdefensa del Estado peruano; contribuir con la sociedad y hacer ver a las instituciones del sector público del país, la importancia de proteger la información del Estado y lo que implica cumplir de manera segura con la reforma y la modernización del estado, a través de la Ley de gobierno digital. La investigación tiene una justificación teórica, por el conocimiento adquirido en campos como la ciberdefensa y el gobierno digital, esto permitirá para futuros investigadores conocer la realidad de la seguridad de la información en el Perú y como interviene la transformación digital en este campo difícil y complejo. Considerando una justificación practica la investigación realizada contribuye al Estado Peruano en general y de manera específica a sus instituciones públicas que tengan como responsabilidad proteger los activos críticos nacionales. Asimismo, la investigación tiene una justificación social, porque aporta a la conducta humana frente a los problemas de seguridad de la información, especialmente con el uso de la tecnología en los estados; nos ofrece mejorar la conciencia de seguridad para proteger y cuidar la información y de sus instituciones públicas.

Materiales y métodos

El método cualitativo utilizado para esta investigación, busca relatar las cualidades de un hecho o suceso sobre la exploración de conceptos para comprender el contexto. Es encontrar el máximo número de cualidades de un cierto suceso o hecho como sea posible para la obtención de nuevas teorías en la casuística que aborda el estudio en el tema de investigación presente.

El tipo de investigación a emplear es la investigación básica, porque se pretende contribuir al conocimiento existente de algo que no se conoce de manera clara y común, la ciberdefesa y de manera específica la seguridad de la información digital en las organizaciones del Estado peruano, es un tema novedoso y actual que podría enriquecer el conocimiento teórico y científico de futuros investigadores.

Se tratará de responder a la pregunta de investigación ¿Cuál es la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano? El trabajo de investigación tiene como objetivo conocer la relación que existe entre la Ley de gobierno digital y la ciberdefensa del Estado peruano.

El diseño de investigación que se utilizará será el de estudio de casos en vista que se seleccionará dos casos representativos de un fenómeno social, un caso ocurrido en un país totalmente automatizado y otro caso de espionaje entre dos potencias mundiales.

Respecto al escenario de estudio, la investigación realizada tiene un alcance en todo el territorio peruano, para mejor tratamiento de información se considera dentro de las instituciones

públicas a evaluar al sector defensa, salud y educación, en estos lugares se apreciará los aspectos relacionados al gobierno digital y la ciberdefensa.

Resultados

En esta investigación se han utilizado las técnicas de observación, análisis documental y evaluación de dos casos de ciberguerra que han sucedido en el mundo, para dar respuesta al objetivo general que es "Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano".
Respecto al análisis documental realizado se puede ordenar de la siguiente manera:

Tabla 01. *Documentos normativos a considerar en la investigación*

Nº	**Tipo de documento**	**Nombre**	**Año**	**Descripción**
01	Ley Nº 30999-PCM	Ciberdefensa	2019	Brinda los parámetros generales de la ley de ciberdefensa.
02	Decreto legislativo Nº 1412-PCM	Ley de gobierno digital	2018	Establece el marco de gobernanza del gobierno digital.
03	Decreto Supremo Nº033-PCM	Plataforma digital única del estado peruano, gob.pe	2018	Se crea la Plataforma digital única del Estado peruano y establecen disposiciones adicionales para el desarrollo del gobierno digital.
04	Decreto Supremo Nº050- PCM.	Definición de seguridad digital	2018	Define el concepto de seguridad digital en el ámbito nacional.

05	Decreto Supremo N.º 118-PCM.	Desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.	2018	Declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
06	Decreto Supremo Nº016-PCM.	Aprobación de la estrategia nacional de datos abiertos	2017	Se aprueba "La estrategia nacional de datos abiertos gubernamentales del Perú 2017-2021" y el "Modelo de Datos Abiertos Gubernamentales del Perú"
07	Decreto Supremo N.º 066-PCM.	La agenda digital peruana 2.0	2011	Se ofrece el Plan de desarrollo de la sociedad de la información en el Perú.
08	Ley Nº 27658	Ley marco de modernización de la gestión del Estado.	2002	El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos.

Fuente: Elaboración propia

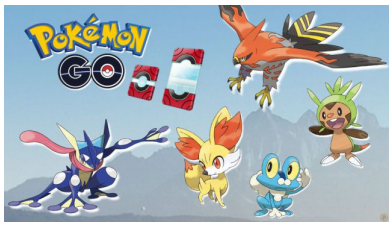
Del resultado de la investigación documental se puede afirmar que existen normas claras respecto a implementar el gobierno digital en Perú, se observa que brindan responsabilidades

precisas a las instituciones del Estado para hacer cumplir de manera segura la implementación de la transformación digital, pero no existe un control ni la supervisión adecuada de la ciberdefensa en el país. Respecto a los dos casos de cibeguerra analizados, también podemos precisar que no existe la seguridad de la información completa o total, no podemos confirmar verazmente que estamos seguros o que nuestra información está totalmente segura contra cualquier ataque informático, ni siquiera empresas fuertes tecnológicamente hablando pueden confirmar una seguridad de la información completa y absoluta.

La investigación realizada dio cumplimiento al objetivo general sobre analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano, el análisis se pudo llevar a cabo por la recolección de la información respecto al gobierno digital y la cibedefensa; asimismo los casos evaluados de Estonia y Estados Unidos nos muestran que también en paises mucho más avanzados en tecnología suceden ataques informáticos que producen pérdidas o daños a la información del Estado. Asimismo, para cumplir con el objetivo general propuesto se ha planteado desdoblar la investigación a través de los siguientes objetivos específicos (i) Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. (ii) Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. iii) Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. Estos tres objetivos se discutieron de la siguiente manera: (i) Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. El recurso humano en toda organización y principalmente en un gobierno digital y en la cibedefensa son los actores más importantes en los procesos de seguridad de la información, el recurso humano bien capacitado e instruido puede proteger la información mucho mejor que cualquier antivirus moderno, de esa manera las normas del Estado y las políticas de seguridad dispuestas, están dirigidas al recurso humano. Como segundo punto se discutió (ii) Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. Conforme a lo revisado y analizado en los casos de Estonia y Estados Unidos, la tecnología es muy importante en este proceso de proteger la información del Estado, si no se cuenta con infraestructura tecnológica adecuada en las instituciones públicas, será muy difícil de proteger la información, esto va de la mano con el recurso humano analizado en los párrafos anteriores. Un recurso humano conocedor de su tecnología podría ayudar mucho a proteger la información del Estado. Lo complejo en las tecnologías es que son muy cambiantes y pierden vigencia tecnológica muy rápidamente, la evolución tecnológica cambia de manera acelerada y pronta.

Tabla 02. *Años para alcanzar los primeros 100 millones de usuarios*

75 años

	16 años
	7 años
	4 años
	2 años
 Candy Crush	112 días
	30 días
	¿?? días

Fuente: Elaboración propia

Por último, el objetivo iii) Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano; toda la normatividad existente respecto a gobierno digital y ciberdefensa nos ayuda en guiarnos y observar ciertas conductas adecuadas

para proteger la información de los activos críticos nacionales; asimismo infringirlas puede llevarnos a cometer delito informático y ser castigados con prohibición de su libertad.

Conclusiones

El presente trabajo de investigación concluye que la Ley de gobierno digital de cualquier país pretende llevar al estado hacia la transformación digital, y para ello tiene herramientas normativas o reglamentos propios para la realidad de cada gobierno, no significando siempre que una realidad tecnología propia de un país sea igual o funcione para cualquier otro país. La Ley de gobierno digital de Perú, se encuentra bien elaborada y con responsabilidades para cada actor del gobierno, al igual que la ley de ciberdefensa, pero no se tiene un control adecuado, no se realiza evaluaciones periódicas de la seguridad digital de la información del Estado. Esta tarea es bastante complicada para los gobiernos y más aún en tiempos de pandemia donde la prioridad son la salud y la supervivencia de la persona. Pero esta realidad que nos ha tocado vivir, donde el uso de la tecnología es importante para prevenir contagios, tiene que tener su resguardo y protección adecuada, establecidas por las leyes de los Estado, Ley de gobierno digital y Ley ciberdefensa. Ambas leyes son complementarias, si falla una la otra también falla, tienen una relación muy directa, tiene que existir una mirada conjunta entre ambas leyes; el recurso humano es muy importante en esta problemática, la conciencia de seguridad de la información que cada uno tenga y las capacidades de ciberdefensa, ciberseguridad y seguridad de la información es fundamental para proteger los activos críticos del país; esa conciencia de seguridad se puede lograr con eventos académicos, foros y capacitación constante. El intercambio de experiencias en el ciberespacio nos ayuda también en ser más cautos con la información del estado.

Referencias

Decreto Legislativo Nº 1412 (2018). Decreto Legislativo que aprueba la Ley de Gobierno Digital.

Decreto Supremo N.º 066-PCM (2011). Decreto Supremo que ofrece el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0.

Decreto Supremo N.º 081-PCM (2013). Decreto Supremo que brinda la Política Nacional de Gobierno Electrónico 2013-2017.

Decreto Supremo N.º 016-PCM (2017). Decreto Supremo que brinda la estrategia nacional de datos abiertos gubernamentales del Perú 2017-2021.

Decreto Supremo N.º 033-PCM (2018). Decreto Supremo que crea la Plataforma digital única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.

Decreto Supremo N.º 050-PCM (2018). Decreto Supremo que define el concepto de seguridad digital en el ámbito nacional.

Decreto Supremo N.º 118-PCM (2018). Decreto Supremo que declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.

Hernández, R. (2010). Metodología de la investigación 5ta Edición (5ta ed.). https://doi.org/- ISBN 978-92-75-32913-9

Hussain, S. (2019). Offensive Cyber Operations and Nuclear Weapons.

Ley Nº 27658 (2002). Ley Marco de Modernización de la Gestión del Estado.

Ley N° 30999 (2019). Ley de ciberdefensa.

Orellana Parra, M. G., & Hinojosa Caballero, A. G. (2019). Tecnología y organización. Una perspectiva sistémica de las TICS en Instituciones de Educación Superior ecuatorianas. Perspectivas, (14), 13-28. Recuperado a partir de https://revistas.uniminuto.edu/index.php/Pers/article/view/2069

Ryseff, J. (2017). The Maliciously Formed Packets of August: Cyberwarfare and the Offense-Defense Balance