UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE GESTIÓN PÚBLICA Y GOBERNABILIDAD

La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado Peruano, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Doctor en Gestión Pública y Gobernabilidad

AUTOR:

Pereyra Acosta, Manuel Antonio (ORCID: 0000-0002-2593-5772)

ASESORA:

Dra. Soria Pérez, Yolanda Felicitas (ORCID: 0000-0002-1171-4768)

LÍNEA DE INVESTIGACIÓN:

Reforma y modernización del Estado

LIMA – PERÚ

2021

Dedicatoria

A mis padres y hermana, por la formación y el cariño que me brindaron.

A mi esposa Ursula y mis hijos Tamara, Thalia, Gabriel y Thiago por ser el motor en mi vida.

Agradecimiento

A Dios todo poderoso, por la vida.
A mi familia, por su amor.
A mis maestros del doctorado y a mi asesora Dra. Yolanda Soria Pérez, por su compromiso como docente, el cual fue fundamental para el desarrollo y culminación de la tesis.

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

El uso moderno y vigente de la tecnología en el ciberespacio permite todas las cosas buenas y malas en la realidad que nos ha tocado vivir. El presente trabajo de investigación tuvo como objetivo determinar la influencia de la Ley de gobierno digital en la ciberdefesa del Estado peruano, estudio realizado durante el año 2021. El método utilizado fue del tipo descriptivo, con enfoque cualitativo y diseño de estudio de caso. En primer lugar, se realizó una recopilación de información a través de artículos, trabajos de investigación y libros respecto a dos variables: El gobierno digital y la ciberdefensa; luego se ordeno dicha información de manera lógica y teórica. En segundo lugar, se manejó la técnica de la entrevista, teniendo como instrumento dos guías de preguntas que se entregaron a los expertos en los campos de gobierno digital y ciberdefesa, como tercer punto se realizó el análisis correspondiente y como conclusión se logró determinar la influencia que tiene la Ley de gobierno digital sobre la ciberdefensa del Estado peruano. Cualquier cambio sea positivo o negativo en el gobierno digital influye en la ciberdefensa del país, esto podría afectar o beneficiar el manejo de la información digital del Estado peruano y de sus activos críticos nacionales.

Palabras claves: Gobierno digital, ciberdefensa, ciberespacio, transformación digital, seguridad digital.

Abstract

The modern and current use of technology in cyberspace allows all the good and bad things in the reality that we have had to live. The objective of this research work was to determine the influence of the Digital Government Law in the cyber defense of the Peruvian State, a study carried out during the year 2021. The method used was descriptive, with a qualitative approach and a case study design. In the first place, a compilation of information was carried out through articles, research papers and books regarding two variables: digital government and cyber defense; then said information was ordered logically and theoretically. Second, the interview technique was used, having as an instrument two question guides that were delivered to experts in the fields of digital government and cyber defense, as a third point the corresponding analysis was carried out and as a conclusion it was possible to determine the influence that has the Law of digital government on the cyber defense of the Peruvian State. Any positive or negative change in the digital government influences the cyber defense of the country, this could affect or benefit the handling of digital information of the Peruvian State and its critical national assets.

Keywords: Digital government, cyber defense, cyberspace, digital transformation, digital security.

I. INTRODUCCIÓN

Desde la aparición de la Internet haya 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, Presidencia del Consejo de Ministros (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.

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; dentro de la formulación del problema, se tratará de resolver el problema general de investigación, ¿Cuál es la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano?, la investigación también tiene tres problemas específicos por resolver, Problema específico 01: ¿Cuál es la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano? Problema específico 02: ¿Cuál es la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano? y finalmente el Problema específico 03: ¿Cuál es la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?

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, por su cambio vertiginoso y la falta de conocimiento del recurso humano por ser temas especializados. Los resultados de la investigación podrán sugerir ideas, recomendaciones o hipótesis a futuros estudios. Considerando una justificación practica la investigación realizada contribuye al Estado peruano en general y de manera específica a sus instituciones públicas como la Presidencia del Consejo de Ministros (PCM) donde se encuentra la Secretaria de gobierno digital (SGDI), El Ministerio de Defensa y sus Fuerzas Armadas, El Ministerio del Interior y la Policía Nacional, El Comando Conjunto de las Fuerzas Armadas, La Dirección Nacional de Inteligencia y a cualquier otra institución pública que tenga como responsabilidad proteger los activos críticos nacionales. Los efectos de la investigación podrán ayudar al personal de las instituciones públicas que hemos mencionado para tomar mejores decisiones, conociendo nuevas formas de realizar un procedimiento respecto a la ciberdefensa. 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 el Estado peruano; el

trabajo ofrece mejorar la conciencia de seguridad para proteger y cuidar la información del Estado y de sus instituciones públicas.

Continuando con la metodología se plantea alcanzar el siguiente objetivo general: Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Asimismo, para cumplir con el objetivo general se ha planteado desdoblar 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.

II. MARCO TEÓRICO

Referente a los trabajos anteriores examinados en el contexto nacional sobre las variables de ciberdefensa y gobierno digital 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, el cual fue aprobado por DL N° 1412 en el año 2018, el cual consiente valorar el nivel de avance en que se encuentra los cinco objetivos estratégicos de e-government.

Ormachea (2020) presento como objeto de investigación, el plantear estrategias constituidas de ciberseguridad requeridas para robustecer la seguridad nacional. El trabajo desarrollado en el Centro de Altos Estudios Nacionales (CAEN), fue tipo descriptivo y enfoque epistemológico; el diseño no experimental y propositivo. La población estaba formada por estrategias y políticas usadas de manera internacional para neutralizar las ciberamenazas, y la muestra estaba conformada por las estrategias de ciberseguridad utilizadas por los países Bajos, EE. UU., España y Perú. Se utilizó como métodos de reunión de datos a la observación y el análisis de documentos; los instrumentos manejados fueron las fichas de registro y de análisis. Se localizó que, en los indicadores referentes a cooperación regional, bilateral y multilateral, el Perú ha presentado actuaciones diferentes; además, el Estado y el ciudadano peruano aún circulan por los enfoques de la concientización y del proceso de las capacidades cibernéticas militares, como indicadores prevalentes en la creación de las políticas de ciberseguridad. Concluyó que la ciberseguridad compone una obligación social que obliga articulación entre lo público y lo privado, cosa que en el Perú aún no se termina; como resultado, el diseño de la Estrategia Nacional de Ciberseguridad del Perú forma una necesidad que obliga ser cumplida.

Al respecto, Taipe (2020) tenía como objeto de investigación, analizar el Sistema de Seguridad Cibernética Nacional cara a los ciberataques como amenaza

a la seguridad nacional; dicho trabajo fue desarrollado en el CAEN, lo que pretende la investigación es contribuir a la solución del problema presentado por los ciberataques. El método que utilizo fue del tipo descriptivo, con diseño no experimental y 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.

Respecto a las normas legales de nuestro país y el gobierno digital, Vilca (2018) presenta como trabajo de investigación, un tema de interés particular relacionando la variable normas legales con la ciberdefensa. El estudio de campo realizado nos permite alertar sobre la incidencia de la criminalidad nacida por medio de las tecnologías de la información y comunicación; la investigación realizada es del tipo descriptiva, con enfoque cualitativo, intenta mostrar y detallar peculiaridades y rasgos del código penal peruano; presenta un diseño no experimental y utiliza las técnicas de análisis documental, la técnica de revisión bibliografía y la encuesta. Vilca concluye su investigación indicando que la legislación en Perú no está al nivel avanzado, ni a la rapidez de la evolución del delito informático, es fundamental contar con un marco legal adecuado al cambio tecnológico. Es obligatorio implantar en el orden jurídico peruano, normas claras y precisas que permitan la adecuada administración, gestión y control de la información nacional, así como los activos críticos nacionales. La capacitación en temas de cibercrimen debe de ser constante y a nivel nacional.

Continuando respecto a gobierno digital, Chucuya (2017) presento un trabajo de investigación para la Universidad Nacional del Altiplano, la misma que trata sobre evaluar la pertinencia de implementar un tipo de gobierno electrónico para la gestión municipal de la provincia de Chucuito distrito de Juli, tratar de generar mejoras en la gestión pública de la municipalidad y ofrecer servicios rápidos y transparente a los ciudadanos; a través del estudio comparativo de los hallazgos de las encuestas antes y después de efectuar el sistema. La investigación está realizada bajo un enfoque experimental y alcance cualitativo. La población está

formada por empleados de la municipalidad y algunos ciudadanos de Chucuito, N = 43. Chucuya concluye que la implementación del modelo de gobierno electrónico para gestionar la municipalidad de la provincia de Chucuito, distrito de Juli fue conveniente y adecuado conforme al resultado de las encuestas realizadas y al estudio de las referencias y documentos presentados.

En referencia a los trabajos anteriores examinados en el contexto internacional sobre las variables de ciberdefensa y gobierno digital, 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 (CSIS), Los autores nos muestran una gran realidad en los gobiernos actuales, su rápida y acelerada carrera de digitalizar todo, de usar la tecnología, de la misma manera los ataques informáticos también evolucionan grandemente, quizás mucho más avanzados y rápidos que los gobiernos, todo lo que se crea para atacar a la tecnología, están siendo más efectivos que los gobiernos digitales. Si realizamos procedimientos rutinarios en ciberdefensa, perderemos batallas importantes. Assante, Roxey y Bochman (2015) 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 CSIS, los autores describen eventos a suceder el año 2025, ciberataques desarrollados en cuatro de las ciudades más grandes e importantes del planeta: Ciudad 01-Bangkok, víctima de un ciberataque a su infraestructura del agua; infraestructura critica para esa ciudad, en vista que con la tecnología usada en el funcionamiento de su infraestructura podía producir la fuerza necesaria para la distribución, esto permitía tener agua, energía eléctrica y orden interno. Ciudad 02-Shanghai, víctima de un ataque a la infraestructura de transporte, los sistemas informáticos que gestionan los aeropuertos, aerolíneas, trenes, metro, autobuses y más se han visto afectados de forma masiva. Ciudad 03-Ciudad de México, ciberataque a las infraestructuras inteligentes como ascensores, escaleras mecánicas, alarmas de incendio, sistema de rociadores,

luces del estadio Azteca y las páginas web del gobierno. Ciudad 04-New York, víctima de ataque ciberfisico, apagones, cortes de electricidad, transporte, comunicaciones, afectación a infraestructuras criticas como el agua y alcantarillado. Los autores concluyen 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 y en las infraestructuras críticas, todas ellas sin la seguridad adecuada. Incluso los sistemas más fuertes y seguros son susceptibles a los ataques informáticos.

Al respecto, Estevez y Janowski (2016) también sostienen la importancia del gobierno digital, los ciudadanos y ciudades inteligentes en su artículo de investigación elaborado para la Universidad Nacional de La Plata en Argentina, el artículo presenta el avance de gobierno digital, expone cómo los gobiernos tratan de indagar procedimientos digitales innovadores para dar respuesta a las presiones que afrontan, cómo institucionalizan las innovaciones, estudian rápidamente el impacto de las innovaciones en los ciudadanos y lidia el nuevo paradigma de ciudades inteligentes como una manera de réplica de los gobiernos locales en la etapa más adelantada de gobierno digital. Como comentarios finales, Estevez y Janowski indican que no existe una fórmula secreta para desarrollar el gobierno digital, ni tampoco única, cada gobierno debe de conocer en principio su realidad propia, su realidad local y posterior a ello aplicar eficientemente las tecnologías digitales, sin perder de vista los marcos regulatorios necesarios para proteger al ciudadano.

En el libro *El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital*, editado por Roseth, Reyes y Santiso (2018) los cuales presentan como objetivo terminar con los tramites largos y engorrosos que tienen los gobiernos de Latinoamérica, libro realizado por El Banco Interamericano de desarrollo (BID) donde utiliza como muestra casos y estadísticas propias de los países de la región, basándose de gran forma de información coleccionada de las instituciones de gobierno digital (u organizaciones análogas) y de las autoridades de registro civil y administración tributaria, la metodología utilizada es la descriptiva y concluye como los gobiernos de América Latina y el Caribe pueden hacer frente al desafío de los tramites utilizando las tecnologías digitales.

Otro libro referente a gobiernos digitales es el de Luna, Gil y Sandoval (2015) *Avances y retos del gobierno digital en México*, donde nos describen el gobierno digital en México y toda la revolución tecnológica que experimenta el mundo y que puede ser muy bien aprovechada para atender al ciudadano de una manera más eficiente buscando en todo momento el valor público, el libro fue elaborado de manera conjunta entre El instituto de Administración Pública del estado de México (IAPEM) y de la universidad Autónoma del estado de México, A.C. (UAEM), la muestra utilizada es el gobierno digital de México, sus portales del gobierno estatal, el gobierno digital entre los años 2005 y 2012 y el gobierno abierto entre 2013 y 2018, los autores concluyen que el libro compone un conjunto de buenas prácticas que podrían ser comprendidas dentro de un portal estatal o para el desarrollo de portales de gobierno, herramientas importantes para todo gobierno digital y otras herramientas como encuestas de satisfacción, estudios de usabilidad, uso de las tecnologías digitales sociales, desarrollo de plataformas digitales, entre otros que contribuyen satisfactoriamente en un gobierno digital.

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 CSIS 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, la inversión se podría presentar en tecnologías y mecanismos que actuarán para reducir la ventaja proporcionada a la ofensiva en el ciberespacio y mejorar la estabilidad de la crisis sufrida posterior a un ciberataque, el endurecimiento de la infraestructura crítica y la construcción de sistemas resilientes proporcionan un buen comienzo para enfrentar un ataque informático.

Siguiendo en el campo de la ciberguerra; Hussain (2019) presento un estudio para el CSIS 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; ataques a la red, ataques de intermediario, rastreo de paquetes, ataques de denegación de servicio (DDOS), ataques Wi-Fi, suplantación de

identidad cibernética, ataques a la cadena de suministro, ataques de radio, ataques criptográficos, ataques de patitos de goma, ataques a redes con espacios abiertos, utilización de software espía y más, los actores malintencionados tienen una variedad de herramientas que pueden poner en peligro la integridad del comando nuclear, sistemas de control y comunicación. Como conclusión, Hussain advierte la destrucción de un país si no se protege con los medios adecuados la información propia de las infraestructuras tecnológicas de los paises; entre ellos se trata de cuidar la información de los centros de comando y control, centros de comunicaciones y centro de comando nuclear y protegerlos contra los ataques de los enemigos cibernéticos.

La investigación realizada sustenta la categoría gobierno digital en las siguientes teorías:

La organización para la cooperación y el desarrollo económico (2016), indica que el gobierno digital trata del uso de las TIC´s de las maniobras de modernismo para brindar valor público. Descansa en el sistema digital del gobierno.

La Ley de Gobierno digital de Perú (2018), en su artículo 6; indica como gobierno digital al uso principal de las TIC`s en la administración pública para brindar valor público. Se sostiene en un conjunto de elementos integrados por personal público, ciudadanos y otros interesados, quienes utilizan el entorno digital del gobierno.

La SGDI de la PCM, es el órgano líder en el uso de las TIC`s por parte del Estado. Ente responsable de la transformación digital y administra los espacios digitales del Estado. Para ello brinda los siguientes servicios:

Figura 1

Servicios digitales orientados al ciudadano

Tomado de SGDI (2018).

Nota: La figura muestra los servicios digitales que la ley de gobierno digital orienta a los ciudadanos peruanos.

La Ley de gobierno digital nos indica cinco servicios orientados al ciudadano peruano; identidad digital, interoperabilidad entre instituciones públicas, seguridad digital, datos para la toma de decisiones y la arquitectura digital. Con estos cinco servicios la PCM pretende contribuir con la gobernanza digital del país.

Asimismo, para poder dirigir adecuadamente el gobierno digital en el Perú, la SGDI presenta las responsabilidades de cada sector, se muestra la siguiente imagen:

Figura 2

Rectoría en Seguridad Digital

Tomado de SGDI (2018).

Nota: Muestra los órganos rectores en seguridad digital conforme al ordenamiento brindado por la SEGDI.

La PCM, a través de la SGDI, se ordena en cuatro campos para controlar la seguridad del gobierno digital: i) La defensa, a cargo del ministerio de defensa a través de la ciberdefensa. ii) La inteligencia, a cargo de la Dirección Nacional de Inteligencia, a través de la seguridad digital en inteligencia. iii) La justicia, a cargo del Ministerio de Justicia y Derechos Humanos, Ministerio del Interior, Ministerio Publico, Policía Nacional del Perú y Poder Judicial, a través de la ciberdelincuencia y, por último, iv) La Institucional, a cargo de las instituciones del sector público, a través del sistema de gestión de la seguridad de la información.

La secretaria de gobierno digital, brinda los siguientes servicios digitales a los ciudadanos de Perú: 1) Gob.pe: Único sitio de trato digital del Estado peruano con los peruanos, según el DS 033-2018-PCM y su tarea es proponer un uso sencillo de ingreso de información de la institución, diligencias y servicios públicos digitales, es administrada por la PCM, a través de la SEGDI. 2) Laboratorio de gobierno y transformación digital: Espacio de creación en conjunto (la academia, la civilidad, sector público, privado y ciudadanos), participen en la transformación digital del Estado. 3) Plataforma Declaración Jurada de Intereses (DJI): Instrumento que muestra información de los relaciones familiares, políticos, económicos, comerciales e institucionales de los funcionarios que utilizan los bienes y recursos públicos. 4) Plataforma de Transparencia Estándar (PTE): En este servicio se encuentra información sobre el uso de los recursos públicos y la gestión institucional de las organizaciones del estado. 5) Plataforma Nacional Datos Abiertos (PNDA): Nos ayuda a obtener datos gubernamentales de distintas temáticas. 6) Plataforma de Software Público Peruano (PSPP): Orientado para el funcionario público que requiere software para mejorar la gestión de su entidad. De esta manera, el organismo público alcanzará utilizar un programa ya creado en lugar de desarrollar uno nuevo, ahorrando recursos. Esto ayuda a la expansión del gobierno digital. 7) Plataforma Infraestructura Datos Espaciales (IDEP): Grupo relacionado de elementos tecnológicos que facilitan la utilización de la información geográfica del Estado. 8) Plataforma Digital GEOPERÚ: Reúne los datos espaciales de los diversos sectores del Estado. 9) Plataforma Nacional de

Interoperabilidad (PIDE): Infraestructura tecnológica administrada por la SGDI, que ofrece la ejecución de servicios de manera pública en forma virtual. 10) Plataforma Digital de Gestión Documental - Cero Papel: Herramienta tecnológica usada para controlar la documentación en el sector público sin uso de papel, solo de manera digital. 11) Equipo de respuesta ante incidentes de seguridad digital: Oficina de la SGDI de la PCM delegada de liderar los esfuerzos para solucionar, predecir y enfrentar los ciberdesafíos, y sistematizar la respuesta ante los ciberataques. También es conocido con el nombre de PECERT y su tarea principal es suministrar al país de seguridad en el medio digital. 12) Colección de reportes de alertas de seguridad digital y los análisis técnicos realizados de distintos ataques a la ciberseguridad de instituciones públicas y empresas privadas.

Respecto a la categoría ciberdefensa la investigación realizada se sustenta en las siguientes teorías:

La Organización del Tratado del Atlántico Norte (OTAN 2010) define a la ciberdefensa como “la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques”.

Al respecto, la ciberdefensa es la rama de la seguridad informática que, más allá de la ciberseguridad, a cargo de responder a los ataques, se ocupa de garantizar la seguridad digital de organizaciones y estados, Molano (2018).

La Ciberseguridad es “la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la seguridad digital y es un ámbito del marco de seguridad digital del país” (Decreto de urgencia Nº 007 Perú, 2020).

En la Cumbre de la OTAN en Varsovia 2016, el ciberespacio se registró como un nuevo dominio de las operaciones militares, al igual que de los de tierra, mar, aire y espacio.

En ese nuevo dominio, El Instituto Español de Ciberseguridad (SCSI) indica que el ciberespacio está conformado por tres capas que se superponen: 1) La capa física-Considera la componente hardware e infraestructura que soportan las redes

y sus conectores físicos (cables, computadoras, switches, equipos físicos, equipos de transmisión y recepcion de señal, etc.). 2) La capa lógica- Formada por los componentes de software que requiere la capa física para trabajar. 3) La capa social- Formada por las personas que utilizan el ciberespacio y su identidad digital. Una persona puede tener una o más identidades digitales y una identidad digital puede ser utilizada por una o más personas. Estas identidades digitales pueden ser reales o suplantadas, lo que permite disfrutar de cierto anonimato o impunidad en las acciones que se ejecuten en el ciberespacio siendo, por tanto, difícil relacionar de manera unívoca una identidad digital con una persona. Las identidades digitales están constituidas, entre otros, por cuentas de correo electrónico, cuentas de usuarios en redes o perfiles en redes sociales. Al respecto, el ciberespacio no tiene un dueño, no es físico, no existen leyes universales porque no tiene un alcance definido, podríamos recibir un ataque informático desde cualquier parte del mundo y existe la suplantación de ciber-identidad, esto vuelve más complejo de descubrir a los autores del ciberataque.

La Ley de ciberdefensa (2019) define el concepto de ciberdefensa como “capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional”.

El Decreto Supremo Nº 050-PCM del 2018 define el concepto de seguridad digital en el ámbito nacional. Dentro de indicada normatividad define ciertos aspectos a considerar para consolidar la tan ansiada seguridad digital y tiene como fin mantener la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital del país.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

El método cualitativo utilizado para esta investigación, buscó 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 realizado.

El tipo de investigación empleado, fue la investigación básica, porque se pretendió contribuir al conocimiento existente de algo que no se conocía de manera clara y común, la ciberdefensa y de manera específica la seguridad de la información digital en las organizaciones del Estado peruano, tema novedoso y actual que podría enriquecer el conocimiento teórico y científico de futuros investigadores.

El diseño de investigación que se utilizó fue el de estudio de caso en vista que se consideró las experiencias individuales de los informantes calificados y conocedores de la ciberdefensa y del gobierno digital en el Estado peruano.

3.2 Categorías, Subcategorías y matriz de categorización

Categoría 1: Gobierno digital

Categoría 2: Ciberdefensa

Matriz de categorización

CATEGORIZACIÒN	Categoría 1: Gobierno digital Categoría 2: Ciberdefensa		
	DEFINICIÒN	SUBCATEGORIAS	DEFINICIÒN
Categoría 1: Gobierno digital	La Ley de Gobierno digital de Perú, en su artículo 6; indica como gobierno digital al uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público.	Identidad digital	Característica digital del individuo, las instituciones públicas entregan la identidad digital para identificar al ciudadano de manera propia.
		Interoperabilidad entre entidades publicas	Capacidad para interactuar entre las instituciones incomparables y diversas para lograr objetivos que hayan convenido de manera conjunta, acudiendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.
		Seguridad digital	Estado de confianza en un entorno digital resultante de la gestión y utilización de un acumulado de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno.
		Datos para la toma de decisiones	Datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación.
		Arquitectura digital	Conjunto de elementos, lineamientos y estándares, que permiten dirigir los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, con motivos de promover la colaboración, interoperabilidad, escalabilidad, seguridad y el óptimo uso de las tecnologías digitales en un entorno de gobierno digital.
Categoría 2: Ciberdefensa	Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional. (Ley de ciberdefensa, 2019)	Personas	Las personas generan conocimiento que se procesa en sistemas de información que funcionan a través de redes de telecomunicaciones emplazadas en lugares concretos del terreno.
		Ciberpersonas	Constituida por cuentas de correo electrónico, cuentas de usuarios en redes o perfiles en redes sociales, DNI, cuentas bancarias, claves o contraseñas, cuentas en sistemas de información, etc.
		Conocimiento	Las ideas, manuales, planes de contingencia, diseño de redes de datos, los pensamientos de las personas, planes de operaciones en el ciberespacio, etc. Toda information que genera conocimiento en el Estado.
		Sistemas de información	Aplicaciones de personal, económicas, logísticas, legales, etc. Donde se almacena la información del Estado.
		Infraestructura TIC	Se refiere al hardware, software y los medios de comunicación que permiten la seguridad de la información del Estado.
		Terreno	También conocido como componente geográfica se refiere el lugar geográfico donde se ubica el equipo físico desde donde se interactúa con el ciberespacio.

Tipo y diseño de investigación	Tipo de investigación	Cualitativo	
	Diseño de investigación	Estudio de caso	
Método de análisis de datos	Método de muestreo	Población:	Ministerio de defensa, Ministerio de educación y Ministerio de salud
		Muestra:	Cuatro expertos
	Análisis de datos	Técnica de recolección de datos:	Entrevista
		Instrumento:	Guía de entrevista

Fuente: Ley de gobierno digital. Ley de ciberdefensa.

3.3 Escenario de estudio

Respecto al escenario de estudio, la investigación realizada tiene un alcance en todo el territorio peruano, por las características propias de la investigación el gobierno digital y la ciberdefensa tiene los siguientes datos:

Tabla 01

Documentos normativos a considerar en la investigación

Tipo de documento	Nombre	Año	Descripción
Ley N° 30999	Ley de Ciberdefensa	2019	Brinda los parámetros de la ley de ciberdefensa.
D.L.Nº 1412	Ley de gobierno digital	2018	Establece la norma de gobernanza del gobierno digital para su conveniente administración.
D.S. N.º 066-PCM	Agenda digital peruana 2.0	2011	Ofrece Plan de Desarrollo de la Sociedad de la Información en el Perú.
D.S. N.º 033-PCM	Plataforma digital única del Estado peruano.	2018	Crea la Plataforma digital única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.
D.S. N.º 050-PCM	La seguridad digital	2018	Define el concepto de seguridad digital en el ámbito nacional.

Elaboración propia.

Por ser muy amplio el alcance de la investigación y 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.

3.4 Participantes

El tipo de muestreo a utilizar es el de conveniencia del investigador.

Respecto a los participantes, se realizará la entrevista a expertos, se ha estudiado minuciosamente a cada persona especialista que puede contribuir con su conocimiento sobre el tema, seguido, se presenta una tabla con la caracterización de cada uno de los expertos:

Tabla 02

Caracterización de los expertos

Ref	Grado académico	Características	Cargos ocupados	Tiempo de experiencia
E01	Magister en doctrina y administración aeroespacial	Experto en temas de ciberdefensa	Director y jefe de Ciberdefensa en el CCFFAA y en la FAP	30 años
E02	Maestro en ciencias políticas y gobierno	Experto en temas de gobierno digital	Docente en la UNMSM en temas de ciencias políticas y gobierno	05 años
E03	Magister en Política y Gobierno	Experto en temas de TIC`s	Comandante del Servicio de electrónica de la FAP	29 años
E04	Magister en Ciencias con mención en ing. de sistemas	Experto en temas de ciberdefensa	Sub director de Telemática de la FAP	30 años

Elaboración propia.

3.5 Técnicas e instrumentos de recolección de datos

Santillán (1983), define la entrevista como técnica útil para recopilar datos en la investigación del tipo cualitativa. Lo define como un diálogo con un fin concreto, a diferencia de una simple conversación. La técnica utilizada es la entrevista a los especialistas mencionados anteriormente, ellos responderán a las preguntas de investigación de acuerdo a su experiencia y conocimiento.

Milles (2012), indica que el instrumento es como el manual de técnicas de investigación donde se recolectan datos para el estudio propuesto que generalmente se generan por la característica de una situación o problema, tomándose siempre el panorama general de la información. Como instrumento se usará la guía para la entrevista, este servirá para que los entrevistados respondan a las preguntas de manera apropiada, ordenada y fluida, lo que nos permitirá captar ideas y expresar libremente sus puntos de vista frente a las preguntas abiertas del investigador. El instrumento consta de diez preguntas abiertas que se relacionan con los propósitos utilizados para resolver nuestras interrogantes. Se adjuntan como anexos la Matriz de categorización apriorística, las matrices guías de preguntas a los expertos y las guías de entrevistas realizadas.

3.6 Procedimiento

Se recolecto información respecto a dos aspectos: El gobierno digital y la ciberdefensa. La recolección de información consistió en la búsqueda utilizando la internet de normas, leyes, libros digitales, artículos científicos respecto a los aspectos indicados. Luego de dicha recolección se analizó y ordeno dicha información. Se consideró entrevistar a expertos en relación al gobierno digital y a la ciberdefensa, se analizó las entrevistas y se consideró realizar una segunda entrevista a los mismos expertos para despejar todas las dudas surgidas del primer análisis realizado. Para finalizar luego de repasar toda la información recopilada (Internet y las entrevistas a expertos) se realiza las conclusiones correspondientes y se recomienda el accionar a la problemática presentada.

3.7 Rigor científico

El Código de ética de la UCV (2017), nos indica sobre rigor científico se logra con el desarrollo de un método, y juicios claros que accedan disponer de la mejor evidencia científica en la investigación desarrollada. Para esto, se deberá realizar un proceso de recojo e interpretación de datos, lo que significa un examen minucioso de las respuestas obtenidas antes de publicarlos.

El presente trabajo de investigación sigue el método científico y está orientado a

aportar en mejorar en la problemática expuesta y de su contexto social. Es preparado por el autor siguiendo los lineamientos de la universidad César Vallejo conforme lo indica las líneas de investigación de manera específica el programa académico de posgrado.

Para que el trabajo de investigación tenga credibilidad, se presenta la documentación consultada y dicha información se corroboran con las entrevistas ejecutadas a los expertos en ciberdefensa y gobierno digital, asimismo se realizan tablas y matrices que muestren la credibilidad del trabajo correspondiente.

3.8 Método de análisis de datos

El procesamiento de los datos se realizará de forma digital con la utilización de herramientas informáticas, Microsoft Word y Microsoft Office Excel 2010. El análisis de la información conlleva al procedimiento de los datos obtenidos en la técnica empleada y la aplicación del instrumento. Se utilizará la matriz de categorización apriorística, matriz de datos y la triangulación para emitir los resultados.

3.9 Aspectos éticos

Ospina (2001) El compromiso del investigador debe regirse por estándares científicos cognitivos, por lo que su propósito no debe ser falsificar información y datos, y mucho menos plagiar. Por lo tanto, los investigadores tienen la responsabilidad de innovar en la búsqueda de soluciones para crear diferentes valores axiomáticos dentro de paradigmas morales y éticos.

El proyecto de investigación ha sido planteado con el máximo valor fidedigno y cognitivo que constituye la aplicación del respeto por las leyes y normas a los derechos de autor, respetando las investigaciones de los autores que han sido consultados, ejecutando con objetividad el proceso de los datos recogidos de las respuestas de las entrevistas y analizando los resultados claramente para establecer un nuevo conocimiento sobre la problemática planteada y de responder algunas dudas existente sobre la investigación.

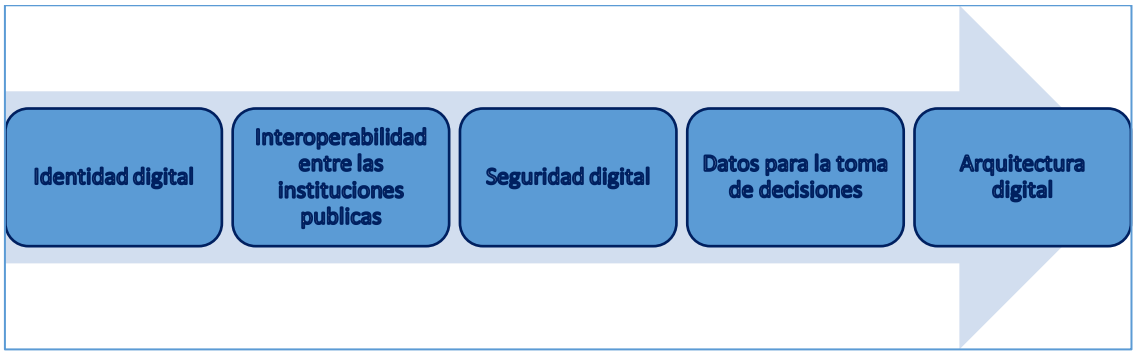
IV. RESULTADOS Y DISCUSIÓN

Continuando con el trabajo de investigación, en esta parte se describió los resultados obtenidos de las entrevistas realizadas a los expertos escogidos en ciberdefensa y en gobierno digital; el procedimiento realizado para la obtención de los resultados es el siguiente: 1) Recopilación de información tal y como el experto lo describió, sin modificar, ni aumentar, ni reducir nada. 2) Selección y categorización en base a colores 3) Interpretación de las respuestas. Este procedimiento se sigue de manera rigurosa para cumplir con los objetivos de la investigación.

Respecto al objetivo general de la investigación, OG: Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano; los cuatro expertos en ciberdefensa y en gobierno digital, concuerdan que la Ley de gobierno digital tiene una implicancia directa en la ciberdefensa del Estado de Perú, cada una de las subcategorías del gobierno digital (identidad digital, interoperabilidad entre entidades públicas, seguridad digital, datos para la toma de decisiones y la arquitectura digital) tienen implicancia en la ciberedefensa.

Figura 3

Categoría gobierno digital



Nota: La figura muestra las subcategorías del gobierno digital orientadas para atender a los ciudadanos peruanos.

Asimismo, se planteó desdoblar el objetivo general de 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.

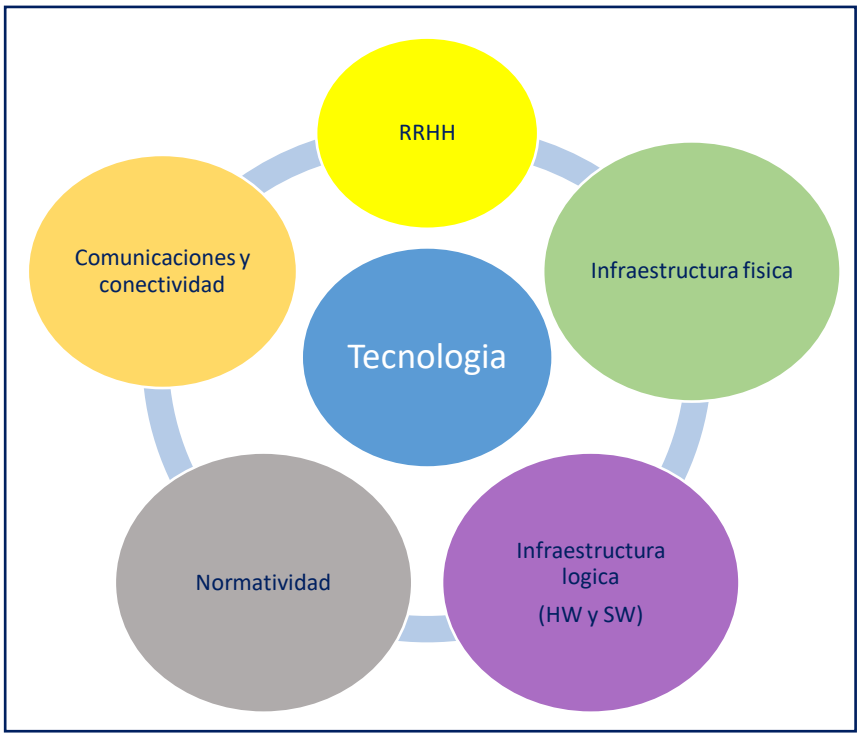
Respecto al aspecto recurso humano, los expertos coinciden que es importante para cumplir el gobierno digital el contar con un recurso humano capacitado y con conocimiento de gobierno digital. El recurso humano tiene la participación principal en el cumplimiento de la Ley de gobierno digital, de igual manera es el eslabón más débil del gobierno digital y de la cibedefensa. Concuerdan que el recurso humano no se encuentra capacitado ni en el uso de las herramientas tecnológicas para el gobierno digital, ni para la ciberdefensa del país; deben recibir capacitación en gobierno digital y en ciberdefensa o seguridad digital. De acuerdo a los datos recopilados se ha podido evidenciar que existen tres tipos de recurso humano diferenciados respecto a las capacitaciones o instrucciones; 1) Recurso humano usuario, formado por las personas que utilizan el gobierno digital, 2) Recurso humano administrador o técnico, formado por las personas que administran las tecnologías, los sistemas, son los responsables de que funcione de manera adecuada el gobierno digital y 3) Recurso humano responsable de la seguridad de la información digital, son las personas que deberían de realizar las auditorias informáticas, realizar las pruebas de vulnerabilidad entre muchas otras técnicas de protección de información digital. Se extrajo que las capacitaciones protegerán al recurso humano de fallas o errores en el uso de las herramientas del gobierno digital. La subcategoría del gobierno digital indica identidad digital a la característica del recurso humano para interactuar en los entornos digitales, en el gobierno digital; la subcategoría seguridad digital tiene mucha relación con la ciberdefensa, ambas tratan sobre la información digital. Un recurso humano sin conocimiento de las herramientas ofrecidas por el gobierno digital es un factor peligroso para la seguridad digital y por consiguiente peligroso para la ciberdefensa.

Respecto al resultado obtenido del objetivo específico 02, analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano; los expertos coinciden en manifestar que la tecnología es otro de los aspectos necesarios para atender el gobierno digital, su atención adecuada implica significativamente en la ciberdefensa de Perú;

asimismo, la tecnología requiere actualización constante, para no perder vigencia y no permitir que esa tecnología falle; también referente a la tecnología, resaltan la importancia de los principios que deben estar presentes en la seguridad de la información (Confiabilidad, integridad y disponibilidad) en todo momento y lugar. La tecnología está relacionada con las subcategorías del gobierno digital (identidad digital, interoperabilidad entre las instituciones públicas, seguridad digital, datos para la toma de decisiones y arquitectura digital). Los expertos indican, que las tecnologías no solo están formadas por hardware y software, también manifiestan que se debe de considerar las comunicaciones, la infraestructura física y los elementos necesarios para administrar, mantener, actualizar y operar; este esfuerzo conjunto ayudara a proteger la ciberdefensa del país (ver figura 4).

Figura 4

Aspecto tecnología



Elaboración propia.

Nota: La figura muestra los elementos a considerar en la administración de la tecnología.

El ultimo resultado obtenido respecto al objetivo específico 03, analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la

ciberdefensa del Estado peruano; indican que existe normas claras y vigentes para el cumplimiento del gobierno digital, pero no existen normas respecto a ciberdefensa. En relación a gobierno digital, las normas están dadas por el gobierno, pero no realizan un control adecuado de su cumplimiento; por el lado de la ciberdefensa, no existe norma, la Ley de ciberdefensa se realizó el año 2019, desde ahí no se tiene un reglamento que aclare el actuar de la ciberdefensa en el Estado peruano. Los expertos consultados también concuerdan en lo siguiente: El cambio rápido de la tecnología produce una falta de normas y una desactualización acelerada de dicha normatividad requerida para proteger la información digital de la ciberdefensa y la información usada en el gobierno digital.

De los hallazgos analizados en los párrafos anteriores, se obtuvo la certeza que la Ley de gobierno digital tiene implicancia en la ciberdefensa del Estado peruano por encontrar mayor similitud que diferencias, entre las entrevistas realizadas y los autores considerados en el marco teórico.

Para esto, el resultado concerniente al aspecto recurso humano, Taipe (2020), mostro como objetivo de investigación, analizar el sistema de seguridad cibernética nacional frente a los ciberataques como amenaza a la seguridad nacional y como resultado indico 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. Los expertos consultados también concuerdan que falta capacitación y conocimiento respecto a la ciberdefensa y uno de los expertos en gobierno digital propone y observa que la capacitación podría estar gestionada en base a tres perfiles requeridos de personas; i) usuario del sistema. ii) personal técnico especialista de la administración de la tecnología del gobierno digital y por ultimo iii) el personal que realiza el control o las auditorias informáticas al sistema del gobierno digital. Teniendo al personal capacitado en cada campo de acción de la ciberdefensa, tendremos ciudadanos responsables del uso de las herramientas del gobierno digital. Al respecto, la Ley de ciberdefensa fortalece estas iniciativas de Taipe y de los expertos consultados, en la cuarta disposición complementaria final, indica el desarrollo de currículos de educación superior en materia de ciberdefensa; se

refiere al trabajo en conjunto entre el Ministerio de defensa y el Ministerio de educación, los cuales deben de implementar cursos y capacitación respecto a seguridad digital y cibedefesa en las instituciones educativas universitarias y tecnológicas a nivel posgrado y pregrado.

Vilca (2018), también concuerda con Taipe (2020) y con los expertos consultados, respecto a la necesidad de capacitación en temas de cibercrimen y la constancia de educación en estos campos a nivel nacional. Asimismo, Vilca manifiesta en su investigación que la legislación en Perú no está al nivel avanzado. La tecnología presenta un avance mucho más acelerado que la legislación y eso se puede apreciar por la falta de sanciones a los delincuentes informáticos, capturar al ciberdelincuente es mucho más complejo y difícil que capturar a un delincuente común, por la particularidad que presente su campo de acción en el ciberespacio, así como también las estrategias de enmascamiento o suplantación de identidad que se podrían utilizar en los modernos ataques informáticos. Cuando se presenta un ataque informático siempre se podría presentar tres situaciones diferentes; i) La pérdida económica. ii) La denuncia legal por incumplimiento o perdida de la información de los clientes y iii) La pérdida de imagen o reputación ante la sociedad o los clientes.

En el aspecto normativo coinciden con 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; ni el gobierno digital ni la ciberdefensa están utilizando herramientas que contribuyan con el cumplimiento de la protección de la información. Chacón (2019) propone utilizar ITIL y COBIT como herramientas de implementación del gobierno digital. El Gobierno digital utiliza la Norma Técnica Peruana en todas las instituciones del sector público. Lo que se observó es que no existe un buen control del cumplimiento de esta norma técnica, porque cada uno de los entrevistados manifiestan fallas en el sistema de seguridad de la información; se cuenta con un marco normativo adecuado, una estructura organizacional para gestión de la seguridad de la información y una herramienta propia de gestión, pero no se cuenta con un control adecuado del cumplimiento de esta norma técnica.

Al respecto, Ormachea (2020), tuvo como objetivo de investigación, el proponer estrategias integradas de ciberseguridad necesarias para fortalecer la

seguridad nacional del Perú. Los expertos consultados, también llegaron a coincidir en que se requieren estrategias integradas para proteger la seguridad digital y existe una carencia de normatividad para la ciberdefensa; Ormachea (2020) tiene una observación nueva, no considerada por los expertos consultados, la articulación que debe de existir entre lo público y lo privado.

El instituto español de estudios estratégicos del ministerio de defensa y el departamento de seguridad nacional de España, publicaron el 2017 un estudio monográfico en materia de ciberseguridad titulado “Ciberseguridad: la cooperación público-privada”. Trata la cooperación público-privada desde 04 campos: 01) el advenimiento de la transformación industrial y las tecnologías facilitadoras; 02) el análisis, intercambio de información y modelo integral de respuesta a las ciberamenazas desde el sistema de seguridad nacional; 03) la protección de las infraestructuras críticas, y 04) la cultura, capacitación y nuevos perfiles profesionales. La Ley de seguridad nacional del 2017 y la Estrategia nacional de ciberseguridad del 2019 de España, respaldan la cooperación público-privada (CPP).

Para Esteves y Janowski (2016) los gobiernos tratan de indagar procedimientos digitales innovadores para dar respuesta al cumplimento de la transformación digital que se experimenta a nivel global. El nuevo paradigma de las ciudades inteligentes como respuesta a lograr el gobierno digital no son la mejor solución ni la única, cada gobierno es diferente y único, cada gobierno debe conocer su realidad propia sea regional o local, sus fortalezas y debilidades con una mirada interna y sus amenazas y oportunidades con una mirada externa. También los entrevistados expertos en temas de gobierno digital, concuerdan en manifestar, al igual que Esteves y Janowski (2016) que los marcos regulatorios son importantes considerar en este gobierno digital como parte de la aplicación eficiente de las tecnologías digitales. Siempre es necesario controlar el uso del gobierno digital, dentro de la ciberdefensa también es importante el aspecto normativo y las reglas de uso y administración de las tecnologías de información y comunicación.

Por otro lado, en el aspecto tecnología, Roseth *et al*. (2018) se pronuncian al respecto de terminar con los tramites largos y engorrosos que tiene los gobiernos de Latinoamérica para atender al ciudadano, utilizando las tecnologías digitales, concepto muy parecido a lo indicado por Esteves y Janowski (2016)

años anteriores. Las tecnologías digitales ayudaran mucho a lograr desarrollarse el gobierno digital, pero tendrá que ser utilizada de manera responsable. El uso de la tecnología sin previa planificación, evaluación y control no beneficiará al país, por lo contrario, solo será un cumulo de malos procedimientos, información falsa o equivocada producto de una falta de gestión de la tecnología, produciendo todo esto un desorden y descontrol de la información del Estado.

Luna *et al.* (2015) concuerdan con Roseth *et al.* (2018) y con Esteves y Janowski (2016) respecto al aprovechar la tecnología para atender al ciudadano de una manera más eficiente, buscando en todo momento el valor público. Asimismo, proponen un conjunto de buenas prácticas que podrían ser incluidas dentro del portal del estado. En el Perú contamos con un portal de gobierno digital donde podemos encontrar información importante respecto al gobierno digital. Este portal tiene los siguientes servicios digitales para ofrecer al ciudadano: 1) Gob.pe. 2) Laboratorio de gobierno y transformación digital. 3)Plataforma Declaración Jurada de Intereses (DJI). 4)Plataforma de Transparencia Estándar (PTE). 5) Plataforma Nacional Datos Abiertos (PNDA). 6) Plataforma de Software Público Peruano (PSPP). 7)Plataforma Infraestructura Datos Espaciales (IDEP). 8)Plataforma Digital GEOPERÚ. 9)Plataforma Nacional de Interoperabilidad (PIDE). 10)Plataforma Digital de Gestión Documental - Cero Papel. 11) Equipo de respuesta ante incidentes de seguridad digital. 12)Colección de reportes de alertas de seguridad digital y los análisis técnicos realizados de distintos ataques a la ciberseguridad de instituciones públicas y empresas privadas.

La investigación realizada por Chucuya (2017) confirma la conveniencia de implementar un modelo de gobierno electrónico para la municipalidad de la provincia de Chucuito, conforme al resultado de las encuestas realizadas y al estudio de las referencias y documentos presentados. Siempre será conveniente el uso de la tecnología para realizar la gestión pública; La Ley de gobierno digital en su capítulo I nos indica; que el gobierno digital es el uso de manera estratégica de las tecnologías de información, de comunicaciones y datos en la forma de administrar del sector público para la creación de valor para el ciudadano. Se apoya en un medio compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto

de los derechos de los ciudadanos y personas en general en el entorno digital. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades del sector público en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los peruanos. Este uso de la tecnología en el gobierno digital de Perú tendrá que ir de la mano con la ciberdefensa para prevenir los posibles ataques a la información del Estado peruano, protegiendo la información de nuestros activos críticos nacionales.

Conforme lo investigado por Assante *et al.* (2015) la influencia de la automatización de la información en la ciberdefesa de un país es recomendable efectuarla con planificación y contar con estrategias de protección de la información. El cambio vertiginoso de las tareas administrativas en el sector público orienta a la digitalización de los procesos, datos, información y conocimiento, este cambio ha llevado a tomar conciencia de la seguridad de la información, todos estos elementos mencionados anteriormente, se encuentran digitalizados y expuesto a posibles incidentes que atenten contra la protección de la información. Estos incidentes que amenazan la seguridad de la información se pueden clasificar en dos grupos: i) Incidentes naturales como los terremotos, sismos, maremotos, lluvias, tsunamis, inundaciones, huaycos, entre cualquier otro fenómeno natural que dañe la infraestructura tecnológica o los medios de transmisión y recepción de la información. ii) Incidentes artificiales como los virus informáticos, los troyanos, los malwares, los gusanos informáticos, las bombas lógicas o los ataques de los crakers, los piratas informáticos, los delincuentes informáticos, terrorismo, delincuencia, robos, grupos hacktivistas; toda acción creada por el hombre utilizando medios tecnológicos.

De la misma manera Assante y Bochman (2017) sostuvieron que aprecian un avance oscuro a la automatización de las cosas y a las ciudades inteligentes si no se considera la seguridad digital en todos los campos y aspectos de la sociedad moderna; concuerdan con lo que manifiestan Assante *et al.* (2015) respecto a la evolución desmedida de la tecnología sin el debido cuidado y planificación previa. Es común ver personas que se descargan un aplicativo necesario para estar a la moda o no aislarse de este mundo digital, sin tomar la conciencia correspondiente de saber a qué estarán expuestos; de igual manera, los gobiernos se implementan de medios tecnológicos y digitalizan todos sus

procesos para poder lograr el tan ansiado gobierno digital, pero tenemos que trabajar con conciencia de seguridad a nivel estado y con actores colaboradores. Los expertos consultados también concuerdan con Assante *et al.* (2015) y coinciden en pensar sobre la importancia que se debe de tener en la protección de la información para prevenir futuros ataques cibernéticos.

Al igual que la tecnología avanza rápidamente, también evoluciona la ciberguerra; Ryseff (2017) concuerda con lo indicado por los autores anteriores respecto a tomar medidas de protección digital, propone que los paises deben de invertir en ciberdefensa para evitar los ciberataques y mantener la operatividad de un Estado. La ley de ciberdefensa nos indica que la ciberdefensa es la capacidad militar que permite actuar frente a las amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional y nos habla de seis aspectos a considerar para proteger la información del Estado: i) Las personas. ii) La ciberpersona. iii) El conocimiento. iv) Los sistemas de información. v) Las infraestructuras TIC`s. vi) El terreno. Cada uno de estos aspectos fueron analizados por los expertos a través de las entrevistas realizadas y todos ellos concuerdan con los autores Ryseff (2017), Assante *et al.* (2015), respecto a proteger la información con medidas implementadas en cada uno de los aspectos considerados líneas anteriores.

En toda guerra convencional los centros de comando y control integran la información en conjunto de los elementos requeridos para la guerra, información del recurso humano, aeronaves, tanques, buques, barcos, vehículos motorizados, satélites, radares, logística de operación, entre toda información que permita administrar y controlar las fuerzas. Hussain (2019) coincide en que las guerras modernas, las guerras cibernéticas buscan atacar los centros de mando y control. Existen una variedad de formas para atacar los centros de datos de las instalaciones de comando y control, de esta manera se tratarán de dejar ciegos, sordos y mudos a los paises adversarios, tomando la ventaja para operar las demás capacidades militares existentes como la aviación, el ejército o la armada. Sin control de la información es muy probable que se pierda la guerra. La ciberguerra trata de esto, de atacar la confidencialidad, la integridad y la disponibilidad de la información, principios fundamentales para alcanzar la seguridad de la información.

V. CONCLUSIONES

Primera: Se logró determinar que la Ley de gobierno digital tiene influencia en la ciberdefensa del Estado peruano. Cualquier cambio sea positivo o negativo en el gobierno digital influye en la ciberdefensa del país, esto podría afectar o beneficiar el manejo de la información digital del Estado peruano y de sus activos críticos nacionales.

Segunda: Se logró determinar la influencia del aspecto recurso humano de la ley de gobierno digital sobre la ciberdefensa del Estado peruano y se reafirmaron las sub categorías planteadas en esta investigación como son: Identidad digital en el gobierno digital y las personas y las ciberpersonas para la ciberdefensa. El recurso humano y su identidad digital son pieza clave para la seguridad digital, su gestión y atención adecuada en el gobierno digital ayudaran a prevenir futuros daños a la seguridad de la información digital del Estado peruano.

Tercera: Se logró determinar la influencia del aspecto tecnología de la ley de gobierno digital sobre la ciberdefensa del Estado peruano y se reafirmaron las sub categorías planteadas en esta investigación como son: Arquitectura digital respecto al gobierno digital y sistemas de información e infraestructura TIC referente a la ciberdefensa. La tecnología por ser transversal en todo campo de acción, también corresponde considerarla en las siguientes sub categorías: Identidad digital, interoperabilidad entre entidades públicas, seguridad digital y datos para la toma de decisiones en lo que corresponde para el gobierno digital y personas, ciberpersonas, conocimiento y terreno respecto a la categoría principal de ciberdefensa. La tecnología considera la infraestructura tecnológica (hardware, software y comunicaciones), la infraestructura física y de administración (centro de datos, centro de operaciones de seguridad, centro de monitoreo de redes, entre otros).

Cuarta: Se logró determinar la influencia del aspecto normativo de la ley de gobierno digital sobre la ciberdefensa del Estado peruano; no se reconoce claramente entre las sub categorías analizadas (identidad digital, interoperabilidad, seguridad digital, datos, arquitectura digital, persona, conocimiento, infraestructura o terreno), pero se respalda su importancia en los hallazgos de la investigación. Las normas sirven para controlar conductas que pueden traer daño a los demás y para mantener el bienestar de la población

general. Su importancia es clave tanto para el gobierno digital como para la ciberdefensa de un país.

VI. RECOMENDACIONES

Primera:

A los funcionarios responsables del gobierno digital en la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, deberán de controlar el cumplimiento de las políticas de seguridad digital a través de las instituciones públicas del país.

Segunda:

La SGDI de la PCM, elaborar un plan de capacitación en seguridad digital considerando la participación de todo el recurso humano de las instituciones públicas del Estado. Considerar los tres niveles de capacitación (usuario, administrador de las tecnologías y auditores de seguridad digital).

Tercera:

La SGDI de la PCM, elaborar un inventario de las tecnologías con las que cuentan las instituciones públicas, de esta manera se podrían hacer futuros diagnósticos y análisis de la situación real de las tecnologías de información y comunicaciones en el Estado.

Cuarta:

La SGDI de la PCM, elaborar un inventario de la normatividad vigente respecto a gobierno digital; el MINDEF y el CCFFAA deberán elaborar lo mismo respecto a cibedefensa. Posterior a este inventario se recomienda analizar el total de normas vigentes y diseñar el plan de inspección del cumplimiento de dichas normas a través de las instituciones públicas del país. En caso se requieran normatividad como el caso de la ciberdefensa, se sugiere que sean creadas todas estas normas en comité de trabajo con todos los actores correspondientes para elevar dichas propuestas por conducto regular hasta los responsables de las FFAA y CCFFAA.

VII. PROPUESTA

1. Denominación

   Plan de capacitación en seguridad digital.

2. Descripción

   Conforme a la necesidad de alcanzar la conciencia de seguridad digital en todas las actividades del gobierno digital y de la ciberdefensa del Estado peruano, se requiere capacitar al recurso humano de las instituciones públicas del país. Se considera la capacitación en los tres niveles de personas: Usuario, administrador de las tecnologías y auditores de seguridad digital.

3. Justificación

   La seguridad digital es responsabilidad de todos, por este motivo los integrantes de una organización deberán tener una adecuada conciencia de seguridad para proteger la información digital en las instituciones públicas del Estado, contra cualquier amenaza posible de atacar las infraestructuras tecnológicas del Estado y por ende la información propia del país. En la actualidad existen amenazas como: El ciberterrorismo, la ciberdelincuencia, los malwar, virus informático, troyanos, grupos hacktivistas, los fenómenos naturales que podrían dañar la infraestructura tecnológica del Estado, entre otras formas de perjudicar al ciudadano o al Estado peruano a través del uso de medios informáticos en el ciber espacio. La importancia de la propuesta radica en proteger la información del Estado peruano contra cualquier tipo de amenaza o incidente cibernético.

4. Objetivos

   Objetivo general: Capacitar en seguridad digital al recurso humano de las instituciones públicas del Estado peruano.

   Objetivo específico 01: Diseñar la capacitación en seguridad digital.

   Objetivo específico 02: Ejecutar la capacitación en seguridad digital.

   Objetivo específico 03: Controlar y corregir el conocimiento en seguridad digital en las instituciones públicas del Estado peruano.

5. Plan de actividades

CAPACITACION EN SEGURIDAD DIGITAL

ORD	ACTIVIDAD	TIEMPO	RESPONSABLES
1	Elaboración y aprobación de los cursos necesarios para la capacitación. Considerar los tres niveles de capacitación (usuario, administrador y control)	1 semana	SGDI
2	Elaboración y aprobación de los silabus para las capacitaciones.	1 semana	SGDI
3	Ejecución de las capacitaciones	6 meses	Las instituciones publicas del país, a través de sus órganos de administración.
4	Evaluación de lo aprendido	1 semana	Las instituciones publicas del país, a través de sus órganos de administración.
5	Corrección, análisis e interpretación de las evaluaciones	2 semanas	Las instituciones publicas del país, a través de sus órganos de administración.
6	Retroalimentación, mejoras y propuestas de solución	1 semana	Las instituciones publicas del país, a través de sus órganos de administración.

6. Recurso y presupuesto

RECURSOS Y PRESUPUESTO PARA LA CAPACITACION EN SEGURIDAD DIGITAL

RECURSOS	CARACTERISTICAS	PRESUPUESTO
Humano	Personal conocedor de seguridad digital y educación virtual.	800 soles (50 soles x cada hora académica) x tres niveles = 2400 soles
Tecnológico	Computadora, tablet o lap top con conexión a internet.	Asignado por cada institución.

NOTA: - Cada capación es por 16 horas académicas. - El presupuesto requerido debe de ser coordinado y asumido por el Ministerio de educación.

7. Evaluación y control

Al ser una propuesta para el Estado peruano y sus instituciones públicas, la evaluación y el control de esta propuesta debe de ser realizada por la PCM a través de la SGDI.

REFERENCIAS

Abad, et al. (2019). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. Alicante, España: 3Ciencias. DOI: http://doi.org/10.17993/IngyTec.2019.59

Aguilar-Antonio, J.M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO. Revista Latinoamericana de Estudios de Seguridad, (25), pp. 24-40. DOI: https://doi.org/10.17141/urvio.25.2019.4007

Andina (31 de agosto de 2018). ¿Cuáles son los ciberataques más comunes en el Perú? Andina. Disponible en: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

Applebaum, A. (2017). "Why does Putin want to control Ukraine? Ask Stalin." October 20. Accessed January 6, 2018.

Disponible en: https://www.washingtonpost.com/outlook/why-does-putin-want-control-ukraine-askstalin/2017/10/20/800a7afe-b427-11e7-a908-a3470754bbb9_story.html?utm_term=.9fb81

Armas, J. (2018). Ciberseguridad: cómo adoptar medidas para proteger sus activos de información. Review of Global Management, 4(2), 20-21 DOI: https://doi.org/10.19083/rgm.v4i2.1127

Assante y Bochman (2017). IoT, Automation, Autonomy, and Megacities in 2025: A Dark Preview. Article of Center for strategic e international studies (CSIS). Disponible en: https://scienceimpact.mit.edu/sites/default/files/documents/170427_Assante_Megacities_Web.pdf

Assante, et al. (2015). The Case for Simplicity in Energy Infrastructure. Article of Center for strategic e international studies (CSIS). Disponible en: https://csis-website-prod.s3.amazonaws.com/s3fs-

public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf

Ball, T. (2017). “Crowdstrike CTO: Theft and destruction are ‘just a few keystrokes’ apart.” Computer Business Review. September 29. Accessed December 29, 2017. Disponible en: https://www.cbronline.com/news/cybersecurity/crowdstrike-cto-theft-destruction-just-keystrokes-apart/

Bernal, C. (2010). Metodología de la Investigación. (2da edición). México: Pearson Prentice Hall. Disponible en: https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Broad, et al. (2017). “Trump Inherits a Secret Cyberwar Against North Korean Missiles.” The New York Times, March 5: A1. Page 121-137. DOI: https://doi.org/10.25253/99.2017193.09

Cano, J., y rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. RISTI, 32(6), 7-9.DOI: https://doi.org/10.17013/risti.32.0

Carhuancho-Aguilar, José, Morales-Cordero, Jenny Redacción de la sección discusión de los artículos médicos en el contexto de la Salud Pública. *Horizonte Médico* [en línea]. 2013, 13(1), 51-57[fecha de Consulta 1 de Julio de 2020]. ISSN: 1727-558X. Disponible en:

https://www.redalyc.org/articulo.oa?id=371637128008

Coats, D. (2017). “Worldwide Threat Assessment of the Intelligence Community.” Washington, DC: Director of National Intelligence, Feb 2018. Disponible en: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Cybersecurity Ventures (2016). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Recuperado el 12 de enero de 2020 de:

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Chacon, K. (2019). “Diseño de un mecanismo de medición del nivel de cumplimiento de la implementación de gobierno digital en los gobiernos locales del Estado peruano”. (Tesis para optar el título profesional de Ingeniera Informática). Pontificia Universidad Católica del Perú.

Choucri, et al. (2013). Institutional Foundations for Cyber Security: Current Responses and New Challenges. MIT. Massachusetts, EUA, 27 pág. Disponible en https://cams.mit.edu/wp-content/uploads/2013-16.pdf

D. L. Nº 1412-2018-PCM. Decreto Legislativo que aprueba la Ley de Gobierno Digital. https://leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01412.pdf

D.S. Nº 066-2011-PCM. Decreto Supremo que ofrece el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0. https://portal.mtc.gob.pe/comunicaciones/tic/documentos/agenda digital20.pdf

D. S. Nº 081-2013-PCM. Decreto Supremo que brinda la Política Nacional de Gobierno Electrónico 2013-2017. https://cdn.www.gob.pe/uploads/document/file/357106/DS_N%C2%BA_081-2013-PCM.pdf

D. S. Nº 016-2017-PCM. Decreto Supremo que brinda la estrategia nacional de datos abiertos gubernamentales del Perú 2017-2021. Diário Oficial El peruano (2017). https://busquedas.elperuano.pe/download/url/decreto-supremo-que-aprueba-la-estrategia-nacional-de-datos-decreto-supremo-n-016-2017-pcm-1484961-4

D. S. Nº 106-2017-PCM. Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN). Diario Oficial El peruano (2017).https://busquedas.elperuano.pe/download/url/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1

D. S. Nº 033-2018-PCM. Decreto Supremo que crea la Plataforma digital única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital. Diario Oficial El peruano (2018).https://busquedas.elperuano.pe/download/url/decreto-supremo-que-crea-la-plataforma-digital-unica-del-est-decreto-supremo-n-033-2018-pcm-1629595-1

D. S. Nº 050-2018-PCM. Decreto Supremo que define el concepto de seguridad digital en el ámbito nacional. Diario Oficial El peruano (2018).https://busquedas.elperuano.pe/download/url/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1

D. S. N.º 118-2018-PCM. Decreto Supremo que declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial. Diario Oficial El peruano (2018).https://busquedas.elperuano.pe/download/url/declaran-de-interes-nacional-el-desarrollo-del-gobierno-digi-decreto-supremo-n-118-2018-pcm-1718338-2

D. S. Nº 029-2021-PCM. Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. Diario Oficial El peruano (2021).

https://busquedas.elperuano.pe/download/url/decreto-supremo-que-aprueba-el-reglamento-del-decreto-legisl-decreto-supremo-n-029-2021-pcm-1929103-3

Digital Attack Map (2021). Recuperado el 12 de enero de 2021 de: https://www.digitalattackmap.com/

ESET (14 de enero de 2019). Ciberataques en crecimiento. *El Peruano*. https://elperuano.pe/noticia-ciberataques-crecimiento-74748.aspx

Espinoza, J. (2018). Entre la figura electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. Revista del Instituto de Ciencias Jurídicas de Puebla, México, 12(41), 241-266. Disponible en http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-241.pdf

Estevez y Janowski (2016). Gobierno digital, ciudadanos y ciudades inteligentes. Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/53440/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Firdous, M. (2020). Cyber Warfare and Global Power Politics. CISS Insight Journal, 8(1), pp. 71-93. Disponible en http://journal.ciss.org.pk/index.php/ciss-insight/article/view/137/131

Finnemore, M. (2017). Cybersecurity and the Concept of Cyber Norms. November 30. Accessed December 2, 2017. Disponible en http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870.

FireEye. January 2017. APT 28: At the Center of the Storm. Special Report, FireEye iSight Intelligence. Disponible en https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

GCI (2018). Global Cybersecurity Index. International Telecommunication Union. Recuperado el 12 de enero de 2021 de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Gestión (11 de junio de 2019). Radiohead responde a hackers: libera sesiones robadas de música inédita. Gestión. Recuperado de https://gestion.pe/tecnologia/radiohead-responde-hackers-libera-sesiones-robadas-musica-inedita-269828-noticia/.

Gomes, C. (2017). La nueva era de la información como poder y el campo de la ciberinteligencia. URVIO: Revista Latinoamericana de Estudios de Seguridad, (20), pp. 94-109. DOI: https://doi.org/10.17141/urvio.20.2017.2577

Greenberg, A. (2017). "How an Entire Nation Became Russia's Test Lab for Cyberwar." June 20. Accessed July 6, 2017. Recuperado de https://www.wired.com/story/russian-hackers-attack-ukraine/.

Hackmageddon (2020). Cyber Attacks Statistics. Recuperado el 12 de enero de 2020: https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/

Hernández, et al. (2014). Metodología de la Investigación. (6ta ed.). México: Mc Graw Hill

Hussain, S. (2019). Offensive Cyber Operations and Nuclear Weapons. Article of Center for strategic e international studies (CSIS). Recuperado de https://csis-website-prod.s3.amazonaws.com/s3fs-public/190313_Shah_OffensiveCyber_pageproofs2.pdf

Kapersky (2020). Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado el 12 de enero de 2020: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Kello, L. (2017). The virtual weapon and international order. Reino Unido: Yale University Press, 320 pág. Recuperado de https://yalebooks.yale.edu/book/9780300220230/virtual-weapon-and-international-order

Korzak, E. (2017). "UN GGE on Cybersecurity: The End of an Era?" July 31. Accessed September 15, 2017. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspaceless-safe/.

Ley Nº 27658 (2002). Ley Marco de Modernización de la Gestión del Estado.https://www.minagri.gob.pe/portal/download/pdf/cetsar/ley-modernizacion.pdf

Ley N° 30999 (2019). Ley de ciberdefensa. Recuperado de https://busquedas.elperuano.pe/download/url/ley-de-ciberdefensa-ley-n-30999-1801519-5

Luna, et al. (2015). Avances y retos del gobierno digital en México. ISBN: 978-607-8087-27-3.
Recuperado de http://ri.uaemex.mx/handle/20.500.11799/41353

Martín, P. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. Instituto Español de Estudios Estratégicos, 8. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

Moreno, et al. (2020). Ciberseguridad en América Latina. Revista de Administración Pública INAP. Ciberseguridad Nacional; 148 (1): pp.23-46. Recuperado de:

https://www.academia.edu/40689299/Ciberseguridad_estado_de_la_cuesti%C3%B3n_en_Am%C3%A9rica_Latina

NCSI (2019). National Cyber Security Index. E-Governance Academy, Recuperado el 12 de enero de 2021 de: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Norma Técnica Peruana. NTP-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición.

Newmeyer, P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal; 1(3): pp. 9-19. Recuperado de http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf

OEA (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. 186 pág. Recuperado el 12 de enero de 2021 de: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OEA & BID (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 204 pag. Recuperado el 12 enero de 2021 de: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Ormachea J. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Artículo de investigación, Revista de Ciencia e Investigación en Defensa-Centro de Altos Estudios Nacionales (CAEN). Recuperado de:

https://recide.caen.edu.pe/index.php/Recide/article/view/29/31

Perper, R. (2017). “North Korea may be behind a massive cyber attack on a South Korean bitcoin exchange that caused it to collapse.” December 21. Accessed January 6, 2018. http://www.businessinsider.com/northkorea-south-korea-bitcoin-heist-2017-12.

Poema, A., y Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. Sciéndo, 22(4), 275-282. Recuperado de:

https://1library.co/document/qor0wx0q-problematica-ciberseguridad-proteccion-sistemas-informaticos-sociales-peru-mundo.html

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO: Revista Latinoamericana de Estudios de Seguridad, (20), 80-93 DOI: https://doi.org/10.17141/urvio.20.2017.2563

Ryseff, J. (2017). The Maliciously Formed Packets of August: Cyberwarfare and the Offense-Defense Balance. Article of Center for strategic e international studies (CSIS). Recuperado de https://csis-website-prod.s3.amazonaws.com/s3fs-public/170907_Ryseff_Cyberwarfare_And_the_Offense_Defense_Balance.pdf?wmiLQuqdILwMEO5YnxfQJY1IA4Ytbp_2

Rogers, M. (2017). "Statement Before the Senate Committee on Armed Services." May 9. https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

Roseth, et al. (2018). El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital.
Disponible en https://publications.iadb.org/es/el-fin-del-tramite-eterno-ciudadanos-burocracia-y-gobierno-digital

Samaan, J. (2010). Cyber command: The rift in US military cyber-strategy. The RUSI Journal, 155(6): pp. 16-21. DOI: https://doi.org/10.1080/03071847.2010.542664

Sánchez, H y Reyes, C (2015). Metodología y diseños en la investigación científica. (5ta.Ed.) Lima – Perú: Business Support Aneth S.R.L.

Santos, et al. (2019). El hacking como comportamiento típico en las nuevas formas de delincuencia organizada. Espirales: revista multidisciplinaria de investigación, 3(26), 60-70. DOI:

https://doi.org/10.31876/re.v3i26.460

Sharp, T. (2017). “Theorizing cyber coercion: The 2014 North Korean operation against Sony.” Journal of Strategic Studies 40(7): 898-926.DOI: https://doi.org/10.1080/01402390.2017.1307741

Sheldon, J. (2012). “Deciphering Cyberpower: Strategic Purpose in Peace and War.” Strategic Studies Quarterly, vol. 5, no. 2, 2011, pp. 95–112 DOI: https://doi.org/10.1080/13523260.2013.771031

Sicherheitstacho (SF). Overview of Current Cyber Attacks. Deutsche Telekom. Recuperado el 12 de enero de 2021 de: https://www.sicherheitstacho.eu/start/main

Stanković, N. (2019). The conceptual analysis of identities and interests in the thought of Alexander Wendt. Politeia, 9(18), pp. 37-154. DOI: 10.5937/politeia0-22860

Taipe, D. (2020). Sistema de Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la seguridad nacional. Artículo de investigación, Revista de Ciencia e Investigación en Defensa-Centro de Altos Estudios Nacionales (CAEN). Recuperado de: http://recide.caen.edu.pe/index.php/Recide/article/view/11

Tucker, P. (2017). “Russia Will Build Its Own Internet Directory, Citing US Information Warfare.” November 28. Accessed November 29, 2017. http://www.defenseone.com/technology/2017/11/russia-willbuild-its-own-internet-directory-citing-us-information-warfare/142822/.

Vilca, G. (2018). “Los hackers: Delito informático frente al código penal peruano”. (Tesis para obtener el título profesional de Abogado). Universidad Nacional Santiago Antúnez de Mayolo. Recuperado de: http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1. Matriz de categorización apriorística

Título:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021
Línea de investigación:	Reforma y modernización del estado
Nombre:	Mg. Manuel Antonio Pereyra Acosta

ÁMBITO TEMÁTICO	PROBLEMAS	OBJETIVOS	ELEMENTOS DE LA INVESTIGACIÓN
Reforma y modernización del estado	**Problema General** ¿Cuál es la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano? • **Problema Específico #1** ¿Cuál es la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano? • **Problema Específico #2** ¿Cuál es la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	**Objetivo General:** Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. **Objetivo Específico #1** Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano. **Objetivo Específico #2** Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	Análisis de la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. **CATEGORIAS** • Categoría A: Gobierno digital. • Categoría B: Ciberdefensa.

	• **Problema Específico #3** ¿Cuál es la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	**Objetivo Específico #3** Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	
TIPO Y DISEÑO DE INVESTIGACIÓN	**PARTICIPANTES**	**ELEMENTOS DE INVESTIGACIÓN**	
Enfoque cualitativo. Tipo: Orientado a la comprensión del problema. Diseño: Estudio de casos.	2 Magister expertos en ciberdefensa. 2 Magister expertos en gobierno digital.	TÉCNICA: entrevista semiestructurada. INSTRUMENTO: guion de entrevista. FORMA DE ADMINISTRACIÓN: individual. ÁMBITO DE APLICACIÓN: Los aspectos de identidad digital, interoperabilidad entre entidades públicas, seguridad digital, datos para la toma de decisiones y arquitectura digital del gobierno digital y los aspectos de personas, ciberpersonas, conocimiento, sistemas de información, infraestructura TIC y terreno de la ciberdefensa del Estado peruano. MATERIAL DE APOYO: Cuaderno de campo.	

Anexo 2. Matriz de guía de preguntas al experto en ciberdefensa.

Problema General	¿Cuál es la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano?		
Objetivo general	Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano.		
Problemas específicos	**Objetivos específicos**	**Categoría**	**Preguntas al experto en ciberdefensa**
• **Problema Específico #1** ¿Cuál es la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	• **Objetivo Específico #1** Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	1.- ¿Cuál es la implicancia del aspecto recurso humano en la ciberdefensa del Estado peruano? 2.- Respecto a la ciberpersona, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 3.- Respecto al conocimiento, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 4.- Respecto a los sistemas de información, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 5.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 6.- Respecto al terreno, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 7.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

• **Problema Específico #2** ¿Cuál es la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	• **Objetivo Específico #2** Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	8.- Respecto a identidad digital, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 9.- Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano? 12.- ¿Cuál es la implicancia de la tecnología en la ciberdefensa del Estado peruano? 13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?
• **Problema Específico #3** ¿Cuál es la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	• **Objetivo Específico #3** Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	14.- ¿Cuál es la implicancia del aspecto normativo en la ciberdefensa del Estado peruano? 15.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital? 16.- Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano? 17.- Respecto a la arquitectura digital, ¿Cuál es la implicancia en la ciberdefensa del Estado peruano?

Anexo 3. Matriz de guía de preguntas al experto en gobierno digital.

Problema General	¿Cuál es la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano?		
Objetivo general	Analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano.		
Problemas específicos	**Objetivos específicos**	**Categoría**	**Preguntas al experto en gobierno digital**
• **Problema Específico #1** ¿Cuál es la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano? Las tecnologías avanzan muy rápido y avanzan	• **Objetivo Específico #1** Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	1.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano? 2.- Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 3.- Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 4.- Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 5.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 6.- Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 7.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

• **Problema Específico #2** ¿Cuál es la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	• **Objetivo Específico #2** Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	8.- Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 9.- Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano? 12.- ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano? 13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?
• **Problema Específico #3** ¿Cuál es la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano?	• **Objetivo Específico #3** Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.	**Categoría A:** Gobierno digital. **Categoría B:** Ciberdefensa.	14.- ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano? 15.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital? 16.- Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano? 17.- Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Anexo 4.

Guía de entrevista 1 – Experto en ciberdefensa

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mg. Manuel Antonio Pereyra Acosta		
Datos del entrevistado 01	Mg. Magister en doctrina y administración aeroespacial, 30 años de experiencia en el campo de ciberdenfesa para el Estado peruano.		
Fecha:	Hora:	Sexo: M	Edad: 52
Lugar: Reunión virtual	Duración:		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo, analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar ☐ No Acepto participar ☐

Preguntas a un experto en ciberdefensa.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

01.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano?

02.- ¿Cual es la implicancia del aspecto tecnología en el gobierno digital del Estado peruano?

03.- ¿Cual es la implicancia del aspecto normatividad en el gobierno digital del Estado

peruano?

04.- ¿Cuál es la implicancia de la tecnología en la ciberdefensa del Estado peruano?

05.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

06.- ¿Cuál es la implicancia del aspecto normativo en la ciberdefensa del Estado peruano?

07.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

OE 2: Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

08.- ¿Cuál es la importancia de mantener la confidencialidad de la información en el Estado peruano?

09.- ¿Cuál es la importancia de mantener la integridad de la información en el Estado peruano?

10.- ¿Cuál es la importancia de mantener la disponibilidad de la información en el Estado peruano?

11.- ¿Cuál es la implicancia del recurso humano en la ciberdefensa del Estado peruano?

12.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del Estado peruano?

13.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

Guía de entrevista 2 – Experto en gobierno digital.

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mg. Manuel Antonio Pereyra Acosta		
Datos del entrevistado 01	Mg. Magister en Política y Gobierno, 29 años de experiencia en el campo de las tecnologías de la información y comunicaciones para el Estado peruano. Comandante del Servicio de electronica de la FAP.		
Fecha:	Hora:	Sexo: M	Edad: 47
Lugar: Reunión virtual	Duración:		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar ☐ No Acepto participar ☐

Preguntas a un experto en gobierno digital.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

01.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano?

02.- Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

03.- Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

04.- Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

05.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

06.- Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

07.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

OE 2: Analizar la implicancia de los aspectos Confidencialidad, integridad y disponibilidad de la ciberdefensa del Estado peruano.

08.- Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

09.- Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano?

12.- ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano?

13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

OE 3: Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

14.- ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano?

15.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

16.- Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

17.- Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Anexo 5.

ENTREVISTA 01 DESARROLLADA Y CONSENTIMIENTO INFORMADO

Guía de entrevista 2 – Experto en ciberdefensa.

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mg. Manuel Antonio Pereyra Acosta		
Datos del entrevistado 01	Mg. Magister en ingeniería de sistemas, 29 años de experiencia en el campo de las tecnologías de la información y comunicaciones para el Estado peruano. Comandante del servicio de informática de la Fuerza Aérea del Perú.		
Fecha:	Hora:09:00 Hrs.	Sexo: M	Edad: 47
Lugar: Reunión virtual	Duración: 1 hora.		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar [X] No Acepto participar [ ]

Preguntas a un experto en ciberdefensa.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

01.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano?

RSP.

Tomando una mirada de seguridad digital (ciberdefensa), la implicancia del aspecto recurso humano es muy grande.

Kevin Mitnick (hackers, crackers y phreakers estadounidense más famosos de la historia) en una conferencia sobre ciberseguridad en Campus Party en Valencia el año 2011, indico lo siguiente: "….el ser humano que está ante el ordenador es siempre el eslabón más débil de la seguridad informática".

Otro alcance, según el informe sobre seguridad corporativa 2015, realizada por Kaspersky Lab y B2B Internacional, "cuando hablamos de seguridad, el eslabón más débil, siempre es el empleado".

El recurso humano es quien utiliza la tecnología, el recurso humano es quien utiliza el gobierno digital o las herramientas tecnológicas que el Estado nos brinda, para cumplir con la Ley de gobierno digital, pero conforme a lo que nos indican los expertos, ese recurso humano es débil y altamente vulnerable. El recurso humano decide a que páginas web ingresar, es quien decide si coloca un disco externo o una memoria externa contaminado con virus al computador o a la red del Estado, ese recurso humano es el que decide si utiliza una clave no robusta y fácil de robar. Por consiguiente, el recurso humano en el gobierno digital es muy importante, el estado peruano debería de tomar mucha consideración al recurso humano en el uso de las tecnologías implementadas por el gobierno digital.

El recurso humano dentro del gobierno digital podríamos ordenarlo de la siguiente manera: 1) Recurso humano usuario: Son los ciudadanos peruanos que utilizan las tecnologías ofrecidas por el Estado. A este recurso humano se los debería de capacitar en el uso adecuado de las tecnologías ofrecidas por el estado. 2) Recurso humano administrador de la tecnología: Son los expertos en la administración de las tecnologías implementadas por el Estado. En este grupo de ciudadanos podemos tener diferentes tipos de administradores, pueden ser administradores de las bases de datos de la institución, administradores del software, administradores del hardware y administradores de la infraestructura tecnológica como las redes, las comunicaciones o los lugares donde se alojan y funcionan toda esta tecnología del gobierno digital. Este grupo humano deben de estar capacitado y actualizado en la tecnología vigente del gobierno digital. Dentro de este grupo humano también deberíamos de considerar el grupo humano que realizaría las auditorias informáticas, en ciberdefensa podríamos hablar de auditores de ciberseguridad y en otras fuentes bibliográficas se hablarían de Ethical hacking. Asimismo, contar con un grupo humano que atienda de manera inmediata los problemas de cibeseguridad, como lo tiene actualmente la Presidencia del Consejo de Ministros, a través de la Secretaria de Gobierno Digital, llamado Equipo de respuesta ante incidentes de seguridad digital nacional (PECERT).

02.- Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

La ciberpersona es la identidad que toda persona tiene al usar la tecnología, necesaria para poder utilizar y validad su acceso al uso de la tecnología, entiéndase como tecnología a los sistemas que el Estado dispone para los ciudadanos de Perú, a los controles de acceso a las instituciones públicas (entiéndase como equipos de identificación biométrico o con tarjetas de identidad), a los controles de acceso a los cajeros electrónicos, a los servicios que ofrecen los bancos, entre muchos otros accesos que requieren de una clave o contraseña y de un usuario autorizado para utilizar las tecnologías implementadas por el gobierno digital. La Junta Interamericana de Defensa en su Guía de Ciberdefensa

Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar del año 2020, refiere a ciberpersona como la identidad que un usuario del ciberespacio establece en comunidades o actividades online. El gobierno digital debería de utilizar todas sus medidas de seguridad correspondientes, para proteger la confidencialidad de la ciberpersona, de esta manera podríamos estar seguros de la integridad de la información. En la actualidad, existen muchas formas de vulnerar la seguridad de la ciberpersona, se comenta muchos los robos de identidad digital con motivos de extorsión, robo económico, placer o reconocimiento, curiosidad, morbo, entre muchos otros impulsos de los ciberdelincuentes.

Un grupo de delincuentes informáticos, accedieron de forma fraudulenta a la página web del Bono Universal y robaron, se estima, cerca de un millón de soles. Dos expertos en ciberseguridad descubrieron los movimientos de esta banda de delincuentes y avisaron a la Policía Nacional de Perú, de lo que estaba ocurriendo. Así lo reveló un reportaje del programa de Juliana Oxenford, Al Estilo Juliana, transmitido por ATV el 29 de mayo del año 2020. La noticia provocó una gran indignación, pues los delincuentes aprovecharon sus conocimientos en tecnología para quedarse con dinero de cientos de personas en situación vulnerable que eran beneficiarias del Bono Universal. Esto es un ejemplo de lo que ocurre si es que el gobierno digital no se preocupa por proteger la identidad digital de los ciudadanos peruanos.

La ciberpersona tiene una implicancia muy fuerte dentro del gobierno digital y para ello se brinda las siguientes recomendaciones para proteger la identidad digital o a la ciberpersona: 1) Crear usuarios personalizados y propios, ya todos sabemos que los usuarios se crean con la primera letra del nombre, seguido por el primer apellido de la persona. Este trabajo lo deben de realizar los administradores de la tecnología en cada organización. 2) Las claves de acceso deben ser robustas, mínimo 8 caracteres y combinación de letras, números y símbolos. 3) Capacitación constante en temas de ciberseguridad a todas las ciberpersonas y administradores del gobierno digital. 4) Difusión constante de las nuevas modalidades de ataque informático y de dónde acudir en caso ocurra una vulneración a la ciberpersona.

03.- Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

El conocimiento es el conjunto de información almacenada mediante la experiencia y el aprendizaje. La importancia del conocimiento en la sociedad es reconocida como un gran desafío a nivel económico, político y cultural. En las sociedades actuales el conocimiento logra mayores niveles de desarrollo y calidad de vida. Cada sociedad cuenta con sus propios activos de conocimientos. Donde es fundamental conectar las diversas formas de conocimiento que ya se poseen con las nuevas formas de desarrollo adquisición y defunción del mismo.

El artículo escrito por José Martínez Rosas en noviembre del 2017, para MindSolutions, empresa dedicada a la capacitación, indica lo siguiente: El poder de un pueblo descansa en el desarrollo de sus inteligencias. Quizá nunca imaginamos porqué es importante para la vida de las sociedades el acopio de conocimientos, no sólo científicos sino de todo tipo de sabiduría que nuestra especie ha generado.

Sun Tzu en su obra “El arte de la Guerra” indica lo siguiente: “Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro. Si no conoces a los demás, pero te conoces a ti mismo, perderás una batalla y ganaras otra. Si no conoces a los demás ni te conoces a ti mismo, correrás peligro en cada batalla” Esta frase de Sun Tzu es muy usada por los responsables de la seguridad de la información y significa que debemos tener un total conocimiento de nuestra organización (fortalezas, debilidades, recursos humanos, infraestructura de información y comunicaciones, normatividad o reglas de la organización, infraestructura organizacional) y conocimiento de los aspectos del macro entorno (amenazas, oportunidades, aspectos legales o políticos, aspectos sociales y culturales, aspectos económicos, aspectos tecnológicos, aspectos medio ambientales). Cuanto mayor sea el conocimiento obtenido, mejor será la atención al ciudadano en el gobierno digital.

El conocimiento en el Estado peruano debe de estar al alcance de los ciudadanos para que puedan utilizarlo cuando lo requieran en cualquier tiempo y lugar, la tecnología puede salvar estas dificultades de tiempo y espacio.

Ese conocimiento en el Estado peruano, debe ser alimentado y actualizado por las instituciones públicas, por el personal de los tres niveles del Estado (estratégico, táctico y operativo), también debemos considerar los niveles ejecutivos, legislativos, judiciales, nivel regional y nivel local. El conocimiento es amplio y debe ser integrado y mostrado de manera fácil y segura por las instituciones del estado para la atención del ciudadano peruano.

04.- Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

Para Laudon y Laudon (1996), los sistemas de información son “conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución”; Stair y Reynolds (2000) comparten la definición anterior y agregan la retroalimentación como mecanismo de utilidad para el cumplimiento de un objetivo que de acuerdo con Oz (2000) debe ser el definido a nivel estratégico de la organización, mientras que para López (2000) debe estar dirigido a lograr la satisfacción de necesidades de información de una organización, contando para ello con la interrelación dinámica de recursos técnicos, humanos y económicos.

Respecto al gobierno digital, los sistemas de información contribuyen con la atención al ciudadano, agilizan los tiempos de respuesta de los procesos de las instituciones públicas y permiten la transparencia de la gestión del Estado. Estos sistemas de información requieren de gran cantidad de datos para que los sistemas de información procesen esos datos primarios y generen la información necesaria para la mejor toma de decisiones en la organización. La información generada por los sistemas de información es almacenada por las instituciones públicas y de esta manera se forma el conocimiento del Estado peruano.

Los sistemas de información tienen ciertas características que deben de ser consideradas en la implicancia con el gobierno digital del Estado peruano, 1) Todo sistema tiene un objetivo propio y particular, para eso son creados. 2) Todo sistema está conformado por diferentes elementos relacionados entre sí para lograr ese objetivo en común, mencionado en el párrafo anterior. 3) Todo sistema tiende a envejecer, gastarse, malograrse a fallar si no se le brinda un mantenimiento o actualización adecuado. La teoría general de sistemas lo llama ENTROPIA. 4) Todo sistema debe corregirse, arreglarse; La teoría general de sistemas lo llama HOMEOSTASIS. Es la corrección que se debe buscar a toda entropía.

Para tener un gobierno digital adecuado, se debe de gestionar y proteger los sistemas de información que el Estado peruano pone a disposición de los ciudadanos. De la gestión se debe de ordenar con las disposiciones de la Presidencia de Consejo de Ministros, a través de la secretaria de gobierno digital y de la protección, de acuerdo a ley de ciberdefensa, se responsabiliza a las fuerzas armadas.

05.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

La infraestructura TIC, se refiere al hardware, software, medios de transmisión y recepcion de información y comunicaciones, los ambientes donde trabajan y operan las TIC`s, el personal requerido para operar, gestionar y administrar las TIC`s.

El gobierno digital requiere contar con infraestructura TIC confiable, integra y disponible en todo momento y en todo lugar, no debe de haber límite para atender al ciudadano peruano.

La infraestructura TIC puede tener dos tipos de amenazas que podrían vulnerar la seguridad propia de las TIC; 1) amenazas naturales como terremotos, sismos, maremotos, huracanes, lluvias torrenciales, rayos, tormentas eléctricas, inundaciones, entre otros. 2) amenazas artificiales como delincuentes informáticos, terrorismo, robos, vandalismo, virus informático, malwares, bombas lógicas, engaño digital, muchas otras formas actuales que amenazan las TIC`s.

06.- Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

El terreno se refiere al medio ambiente donde el gobierno digital debe de llegar y atender.

Por ejemplo, el terreno de la región oriente (Iquitos, Madre de Dios, Pucallpa, Puerto Maldonado, entre otros), es el más inadecuado para operar y hacer llegar el gobierno digital. La señal de transmisión es muy lenta y demora en llegar. Para que la señal llegue de manera adecuada a esos terrenos alejados y agrestes se requiere de señal satelital (una manera muy cara para que las empresas de tecnología hagan llegar al ciudadano peruano los sistemas de información). de igual manera sucede en la señal que debe atravesar la cordillera de los andes o cualquier elemento que se coloque entre el emisor de señal y el receptor.

Existen muchos medios de transmisión, alámbricos o inalámbricos, cada uno tiene su particularidad de acuerdo al terreno donde se desarrollará.

07.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP.

No contamos con recurso humano capacitado en ciberdefensa. El recurso humano capacitado es escaso en Perú, la capacitación en ciberdefensa puede dividirse en tres niveles; 1) Nivel usuario, es el recurso humano que utiliza los sistemas de información del gobierno digital y deben de tener una capacitación básica en seguridad digital. 2) Nivel

defensa, son los responsables de defender la información del estado peruano y su infraestructura critica nacional. 3) Nivel explotación, son los capacitados en realizar operaciones de ciberdefensa. 4) Nivel de respuesta, son el personal capacitado en responder ante un ataque informático.

La capacitación en ciberdefensa no solo comprende estudiar y adquirir conocimiento, también corresponde la práctica y la ejecución de las operaciones de ciberdefensa o las operaciones de pruebas de vulnerabilidad a nuestras instituciones públicas del estado peruano, para corroborar el estado de seguridad de sus infraestructuras TIC`s o sistemas de información.

Otro aspecto de capacitación, es el compartir los conocimientos. El 5 de marzo de 1975 se reunieron por primera vez en un garaje, un grupo de entusiastas de electrónica y aficionados con inclinación técnica que recolectaban e intercambiaban partes, circuitos, información referente a la construcción de dispositivos computacionales. Fue iniciado por Gordon French y Fred Moore y se llamaron Homebrew Computer Club, en Silicon Valley. Ambos estaban interesados en mantener un foro abierto regular, para que la gente se reuniera para trabajar en hacer la fabricación de computadores más accesible a todo el mundo. El club se reunió hasta diciembre de 1986, donde dejaron de compartir información porque ya se habían formado más de 26 empresas propias y ya no les convenía compartir su información. Producto de esas reuniones, donde se comparten experiencias, ahora también se realizan foros y reuniones hackers y reuniones de ciberdefensa en muchos paises del mundo. Eventos conocidos como Ciso day de España, Cybertech en Europa o Black Hat en USA son famosos por conseguir compartir el conocimiento en ciberseguridad y los últimos ataques informáticos para proteger nuestras organizaciones.

OE 2: Analizar la implicancia del aspecto tecnología, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

08.- Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

La identidad digital es algo muy parecido a lo mencionado en ciperpersona. La identidad digital debe ser único y propio de cada persona, es la manera de acceder a los sistemas del gobierno digital. La identidad digital puede ser robada, alterada, modificada o vulnerada por delincuentes que desean hacer uso de una identidad que les permitan acceder a la información de los sistemas o cuentas bancarias o información de las infraestructuras criticas nacionales.

El Decreto Legislativo Nº 1412 del 13 de setiembre del 2018, en su artículo 10, nos brinda el concepto de identidad digital, “Identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales”. También nos indica que, los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

De acuerdo a un artículo publicado por Edgar Huaranga en HIPERDERECHO, el 8 de abril del 2021 en la página web de esta organización civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Huaranga define Identidad Digital como el conjunto de mecanismos utilizados para verificar la identidad de una persona en un entorno digital. Para

los ciudadanos, estos entornos serían principalmente páginas web o aplicaciones móviles. Entonces nos podríamos plantear las siguientes preguntas: ¿Qué me hace único como persona? y ¿quién decide o de quién depende afirmar que realmente soy yo la persona que está utilizando una web o aplicación? Existen características físicas y biológicas que nos diferencian de otras personas. Por ejemplo, podríamos pensar en nuestra estatura, color de ojos o algunas manchas en nuestra piel. Sin embargo, el problema con estas características es que, a pesar de parecer únicas en nuestro entorno, otras personas también las pueden tener. Por otro lado, existen características que realmente nos hacen únicos y que se utilizan en todo el mundo para identificar a personas de manera individual. Algunos ejemplos son nuestras huellas dactilares, nuestro rostro o nuestra voz. Estos conjuntos de características están clasificados como datos biométricos, que a pesar de no ser los únicos son los más utilizados por los sistemas computacionales a nivel global.

En el Perú, el Registro Nacional de Identificación y Estado Civil (RENIEC) es la institución encargada de organizar y mantener el registro único de identificación de las personas, y por lo tanto, se encarga también de emitir el Documento Nacional de Identidad (DNI) que acredita la identidad de las personas. La importancia de RENIEC en el contexto de identidad digital se debe a que también tiene la facultad de emitir certificados digitales para personas naturales o jurídicas que lo soliciten. Estos certificados digitales vendrían a ser un análogo del DNI o del pasaporte en un entorno digital; dándonos la seguridad de que el intercambio de información es entre personas o entidades que realmente son quien dicen ser y que la comunicación entre ellos estará segura y protegida. Este sistema de certificados digitales es válido y confiable porque es parte de una infraestructura más grande y compleja que involucra hardware, software, políticas y procedimientos de seguridad que tienen como base la criptografía asimétrica. Esta infraestructura se llama Infraestructura de Clave Pública PKI por sus siglas en inglés (Public Key Infraestructure). Con la tecnología de los últimos diez años y teniendo como referencia la implementación de identidad digital en otros países, en el Perú se desarrollaron diferentes plataformas o soluciones orientadas al ciudadano para acelerar procesos o trámites que en persona tomarían días o debían seguir un proceso burocrático muy lento y agotador. Esto aprovechando nuestros datos biométricos o certificados digitales en caso contemos con ellos.

Los proyectos que el Estado está desarrollando para ofrecer soluciones respecto a identidad digital orientado al ciudadano son: DNI electrónico, El portal del ciudadano y la plataforma de autenticación de la identidad digital nacional.

09.- Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia

en el gobierno digital del Estado peruano?

RSP.

En el capítulo V del Decreto Legislativo Nº 1412 del 13 de setiembre del 2018, nos indica que la Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.

El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el

ámbito de sus competencias, en la prestación de servicios digitales inter administrativos de valor para el ciudadano provisto a través de canales digitales.

En esta misma norma, nos indica ciertos aspectos sobre la gestión del marco de interoperabilidad del Estado Peruano, la cual se gestiona a través de los siguientes niveles: 1) Interoperabilidad a nivel organizacional: Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la administración pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias. 2) Interoperabilidad a nivel semántico: Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la administración pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información. 3) Interoperabilidad a nivel técnico: Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las oficinas de informática o las que hagan sus veces de las entidades de la administración pública, de acuerdo con los estándares definidos por el ente rector. 4) Interoperabilidad a nivel legal: Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la administración pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.

Como podemos ver, la interoperabilidad entre las entidades públicas, está considerada como un aspecto importante dentro de la Ley de gobierno digital y dicha norma lo considera en el Decreto Legislativo Nº 1412.

10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del

Estado peruano?

RSP.

La seguridad digital es otro de los aspectos considerados en la Ley de gobierno digital.

Dicha ley nos indica que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

El Marco de seguridad digital del Estado peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública.

Respecto a la gestión del marco de seguridad digital del Estado peruano, la Ley de gobierno digital indica los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la administración pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)

La Norma Técnica Peruana NTP-ISO/IEC 17799 ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Gestión de la Seguridad de la Información (SGSI), al igual que la norma internacional ISO 27001, ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.

Respecto a la articulación de la seguridad digital con la seguridad de la información, El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la

ciberdefensa del estado peruano?

RSP.

La ley de gobierno digital tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la administración pública en los tres niveles de gobierno (estratégico, táctico y operativo) hacia la atención del ciudadano de Perú. Esto quiere decir que el fin principal del gobierno digital es atender al ciudadano usando la tecnología; pero esa tecnología cada vez es más peligrosa y en la actualidad existen muchos riesgos en su uso y administración. Existen muchos delincuentes que utilizan la tecnología para producir daño, existen muchos paises que se han dado cuenta que vulnerando la tecnología pueden producir daño a su adversario, en vista que el mundo está totalmente automatizado, todo campo y toda persona utiliza hoy en día la tecnología, cualquier tipo de tecnología es vulnerable, no existe sistema seguro, la seguridad total no existe, los encargados de la ciberdefesa tienen la gran responsabilidad de proteger al gobierno digital para que puede operar y actuar de manera segura.

La Ley de ciberdefesa en Perú, tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Entonces el uso del gobierno digital influye en la ciberdefensa del estado peruano.

Para poder ser efectivos en la ciberdefensa debemos de conocer y evaluar los elementos que conforman el gobierno digital y la ciberdefensa. Los mencionamos a continuación:

Gobierno digital; -Identidad digital -Interoperabilidad entre entidades públicas -Seguridad digital -Datos para la toma de decisiones -Arquitectura digital.

Ciberdefensa; -Persona –Ciberpersonas –Conocimiento -Sistemas de información- Infraestructura TIC -Terreno.

Tener una mirada sistémica es saber reconocer las características propias de cada sistema, todo puede tener una mirada sistémica, los sistemas tienen un objetivo propio (Misión de la organización), está conformado por elementos que trabajan para cumplir el objetivo de la organización, siempre tiende a fallar o envejecer y siempre se podrá corregir esa falla. Asimismo, también podemos ordenar el trabajo de proteger al gobierno digital, reconociendo los aspectos recurso humano, normatividad, infraestructura física, comunicaciones, redes y tecnología.

12.- ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano?

RSP.

La tecnología es un elemento fundamental en el gobierno digital, sin tecnología no podríamos alcanzar tener un gobierno digital.

La tecnología es la aplicación de la ciencia a la resolución de problemas concretos.

Constituye un conjunto de conocimientos científicamente ordenados, que permiten diseñar y crear bienes o servicios que facilitan la adaptación al medio ambiente, así como la satisfacción de las necesidades individuales esenciales y las aspiraciones de la humanidad.

La Ley de gobierno digital define como Tecnologías Digitales, a las tecnologías de la información y la comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los

riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP.

La tecnología utilizada en ciberdefensa es muy importante para enfrentar todos los riesgos que se podrían presentar en el cumplimiento de la ley de gobierno digital. La tecnología contribuye con la supervisión, el control, el análisis y las operaciones en el ciberespacio. La tecnología utilizada en ciberdefensa se refiere al hardware, software, medios de comunicación y redes, equipos de protección y supervisión de las redes de información. Dicha tecnología requiere de actualización continua y capacitación del personal administrativo, técnico y usuarios propios. Lo complejo es la vigencia tecnológica, el cambio constante origina que la tecnología quede desactualizada en muy corto tiempo (6 meses aproximadamente); asimismo los delincuentes informáticos aprenden nuevas formas de atacar y vulnerar la tecnología utilizada en ciberdefensa.

De acuerdo a la Ley de ciberdefensa Nº 30999 del 27 de agosto del 2019, La ciberdefensa es la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

La tecnología es un elemento utilizado por la ciberdefensa para actuar frente a las amenazas o ataques realizados en y mediante el ciberespacio cuando afecten la seguridad nacional, esa seguridad nacional se refiere a los activos críticos nacionales.

El Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN), DECRETO SUPREMO N° 106-2017-PCM nos indica como Activo Crítico Nacional - ACN.- Son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin. La afectación, perturbación o destrucción de dichos activos no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación. El Sector Responsable. - Son los Ministerios que tienen la responsabilidad de adoptar las medidas necesarias para garantizar el normal funcionamiento de los Activos Críticos Nacionales – ACN. El Operador de los Activos Críticos Nacionales - ACN. - Es toda aquella entidad pública o privada que tiene a su cargo la administración o la operación de los Activos Críticos Nacionales – ACN; teniendo la obligación de adoptar todas aquellas medidas que resulten necesarias para garantizar su normal funcionamiento, de acuerdo al marco jurídico vigente.

OE 3: Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

14.- ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano?

RSP.

La normatividad en el gobierno digital también es muy importante, porque rigen el accionar formal dentro del cumplimiento en el Estado, su implicancia es directa. El gobierno digital cuenta con las siguientes normas del Estado:

- DL Nº 1412 del jueves 13 de setiembre de 2018, Decreto Legislativo que aprueba la Ley de gobierno digital.

– Ley de ciberdefensa Nº 30999 del 27 de agosto del 2019

- Decreto Supremo N.º 066-PCM del 2011, Agenda digital 2.0, Decreto Supremo que ofrece el Plan de Desarrollo de la Sociedad de la Información en el Perú.

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

15.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP.

No contamos con normatividad apropiada en ciberdefensa, recién el año 2019 se promulgo la Ley de ciberdefensa, actualmente no contamos con el reglamento a dicha ley.

La ciberdefensa en Perú es un campo nuevo, no está establecido de manera formal, se desconoce mucho sobre este nuevo campo de acción y no esta ordenado de manera formal en las instituciones públicas, existe mucho desorden y duplicidad de funciones en este nuevo campo llamado ciberdefensa.

Las normas que podrían contribuir y ser consideradas dentro de la normatividad de cibedefensa podrían ser la Ley del delito informático, Ley Nº 30096 del 21 de octubre del 2013. La Norma Técnica Peruana 17799.

16.- Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el

gobierno digital del Estado peruano?

RSP.

Los datos son los principales elementos que se requieren para tener información. Estos datos son los referentes que se requieren para generar información, mientras mayor cantidad de datos se tenga mejor es el proceso para generar información. Los datos por sí mismo no constituye información, es el procesamiento de estos datos los que nos proporciona la información. La Lay de gobierno digital nos indica en su capítulo V respecto a gobernanza de datos, que los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación.

Las entidades de la administración pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

Estos datos se deben de proteger y cuidar por su importancia para generar información.

El artículo 24 de la Ley indica que La Infraestructura Nacional de Datos se define como el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública.

Y el articulo 25 indica, El Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

17.- Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del

Estado peruano?

RSP.

La Ley de gobierno digital indica que la arquitectura digital es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

La misma Ley indica que las tecnologías digitales se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

La gestión y administración de una adecuada arquitectura digital depende de las propias instituciones del estado, ellas serán las responsables de adquirir, mantener, actualizar y proteger el cumplimiento de las disposiciones de la PCM respecto al gobierno digital.

Muchas gracias

ENTREVISTA 02 DESARROLLADA Y CONSENTIMIENTO INFORMADO

Guía de entrevista 2 – Experto en ciberdefensa.

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mag. Manuel Pereyra		
Datos del entrevistado 02	Bachiller en Ciencias de la administración Aeroespacial, 09 años de experiencia en el campo de las tecnologías de la información y comunicaciones para el Estado peruano		
Fecha:	Hora:18:00 Hrs.	Sexo: M	Edad: 37
Lugar: Reunión virtual	Duración: 1.5 horas.		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar [X] No Acepto participar [ ]

Preguntas a un experto en ciberdefensa.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

01.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano?

RSP.

La Influencia del recurso Humano en el aspecto de la ciberseguridad es la más grande flaqueza para lograr una seguridad autónoma.

Javier Chistik, en una entrevista dada por ForcePoint una de las empresas más grandes en seguridad “el factor humano como parte de la seguridad informática, siendo este el eslabón más débil de la cadena y sobre cómo la industria financiera es la más vulnerable.”

Otro alcance, según el informe sobre seguridad corporativa 2015, realizada por Kaspersky Lab y B2B Internacional, “cuando hablamos de seguridad, el eslabón más débil, siempre es el empleado”.

Las personas son el medio por el cual es estado hace uso de la Tecnología, esto está dividido o categorizado ya que podemos ver una persona que utiliza los recursos de una entidad como usuario, como administrador, técnico y otras ramas, pero todas están convergen o llegan al mismo punto, son las más fáciles de corromper, de equivocarse o de pasar por alto la normatividad para llegar a las buenas prácticas en el uso de la Tecnología.

Por otro lado, el recurso humano en la actualidad es irremplazable de la misma forma como es la parte más débil de la cadena es el actor principal para la mitigación de riesgos ya que es este recurso humano quien tiene que realizar el estudio para la implementación de las políticas.

Asimismo, contar con un grupo humano que atienda de manera inmediata los problemas de cibeseguridad, como lo tiene actualmente la Presidencia del Consejo de Ministros, a través de la Secretaria de Gobierno Digital, llamado Equipo de respuesta ante incidentes de seguridad digital nacional (PECERT).

02.- Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.

La ciberpersona o identidad digital hace referencia a la existencia de una persona física dentro de la red de datos, esto no quiere decir que necesariamente esta persona tenga que tener una cuenta para loguearse a un sistema específico la ciberpersona o identidad digital está compuesta por varios recursos y se va construyendo con la información recabada o que se pueda encontrar en la red, no es uniforme o un formulario que se pueda completar se acuerdo a lo requerido.

Ejemplo, Algunas tecnologías exponenciales, como ‘**blockchain**’, la **inteligencia artificial** y las **tecnologías DLT** (siglas en inglés de Distributed Ledger Technology) o la **biometría**, son capaces de contribuir a la construcción de servicios de identidad segura, en particular a gobiernos e instituciones financieras.

La ciberpersona tiene una implicancia muy fuerte dentro del gobierno digital y para ello se brinda las siguientes recomendaciones para proteger la identidad digital o a la ciberpersona: 1) Crear usuarios personalizados y propios, ya todos sabemos que los usuarios se crean con la primera letra del nombre, seguido por el primer apellido de la persona. Este trabajo lo deben de realizar los administradores de la tecnología en cada organización. 2) Las claves de acceso deben ser robustas, mínimo 8 caracteres y combinación de letras, números y símbolos. 3) Capacitación constante en temas de ciberseguridad a todas las ciberpersonas y administradores del gobierno digital. 4) Difusión constante de las nuevas modalidades de ataque informático y de dónde acudir en caso ocurra una vulneración a la ciberpersona.

03.- Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. El conocimiento en el gobierno digital del estado peruano está variando sustancialmente en todos los sentidos y en todos los ámbitos de la vida pedagógica. No solo se asiste a una auténtica revolución dentro de las aulas, sino que además el individuo indaga, busca, investiga (y a menudo hasta encuentra) información siguiendo patrones esencialmente distintos.

04.- Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP.Para Laudon y Laudon (1996), los sistemas de información son "conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución"; Stair y Reynolds (2000) comparten la definición anterior y agregan la retroalimentación como mecanismo de utilidad para el cumplimiento de un objetivo que de acuerdo con Oz (2000) debe ser el definido a nivel estratégico de la organización, mientras que para López (2000) debe estar dirigido a lograr la satisfacción de necesidades de información de una organización, contando para ello con la interrelación dinámica de recursos técnicos, humanos y económicos.

Respecto al gobierno digital, los sistemas de información contribuyen con la atención al ciudadano, agilizan los tiempos de respuesta de los procesos de las instituciones públicas y permiten la transparencia de la gestión del Estado. Estos sistemas de información requieren de gran cantidad de datos para que los sistemas de información procesen esos datos primarios y generen la información necesaria para la mejor toma de decisiones en la organización. La información generada por los sistemas de información es almacenada por las instituciones públicas y de esta manera se forma el conocimiento del Estado peruano.

Los sistemas de información tienen ciertas características que deben de ser consideradas en la implicancia con el gobierno digital del Estado peruano, 1) Todo sistema tiene un objetivo propio y particular, para eso son creados. 2) Todo sistema está conformado por diferentes elementos relacionados entre sí para lograr ese objetivo en común, mencionado en el párrafo anterior. 3) Todo sistema tiende a envejecer, gastarse, malograrse a fallar si no se le brinda un mantenimiento o actualización adecuado. La teoría general de sistemas lo llama ENTROPIA. 4) Todo sistema debe corregirse, arreglarse; La teoría general de sistemas lo llama HOMEOSTASIS. Es la corrección que se debe buscar a toda entropía.

Para tener un gobierno digital adecuado, se debe de gestionar y proteger los sistemas de información que el Estado peruano pone a disposición de los ciudadanos. De la gestión se debe de ordenar con las disposiciones de la Presidencia de Consejo de Ministros, a través de la secretaria de gobierno digital y de la protección, de acuerdo a ley de ciberdefensa, se responsabiliza a las fuerzas armadas.

05.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. La infraestructura TIC, se refiere al hardware, software, medios de transmisión y recepcion de información y comunicaciones, los ambientes donde trabajan y operan las TIC`s, el personal requerido para operar, gestionar y administrar las TIC`s.

El gobierno digital requiere contar con infraestructura TIC confiable, integra y disponible en todo momento y en todo lugar, no debe de haber límite para atender al ciudadano peruano.

La infraestructura TIC puede tener dos tipos de amenazas que podrían vulnerar la seguridad propia de las TIC; 1) amenazas naturales como terremotos, sismos, maremotos, huracanes, lluvias torrenciales, rayos, tormentas eléctricas, inundaciones, entre otros. 2) amenazas artificiales como delincuentes informáticos, terrorismo, robos, vandalismo, virus informático, malwares, bombas lógicas, engaño digital, muchas otras formas actuales que amenazan las TIC`s.

06. Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. El comercio electrónico, telesalud, educación virtual y el teletrabajo vienen ganando más terreno que nunca. Y es que en tiempos de cuarentena se ha hecho cada vez más estrecha la relación de las Tecnologías de Información y Comunicaciones (TIC) con las actividades cotidianas y la forma de hacer los negocios.

El 93,9% de los hogares en el Perú cuenta con al menos una TIC, que comprende telefonía fija, telefonía celular, internet, televisión y radio. Asimismo, dicho porcentaje es mayor en hogares cuyo jefe de hogar cuenta con educación superior universitario (100%), en comparación a aquellos hogares cuyo jefe tiene educación primaria (85,1%). Esta información se desprende del informe Estadísticas de las Tecnologías de Información y Comunicación en los Hogares, elaborado por el Instituto Nacional de Estadística e Informática (INEI) correspondiente al cuarto trimestre del 2019.

Sin embargo, el bajo acceso a internet resta la posibilidad de aprovechar en mayor medida de los beneficios en el uso de las TIC.

A nivel nacional, solo el 38,8% de los hogares cuenta con internet; con una mayor cobertura en Lima Metropolitana (LM), donde el 59,6% de los hogares tiene este servicio. No obstante, la brecha de disposición tecnológica es mucho más marcada al comparar el área urbana (excluyendo LM) con la rural: en el área urbana, 41 de cada 100 hogares disponen del servicio de internet. En el extremo opuesto, se ubican las familias del área rural, donde solo 6 de cada 100 hogares cuentan con dicho servicio.

En el campo de la educación, el auge repentino de la enseñanza no presencial nos lleva a evaluar el acceso a internet y a los dispositivos con los que tienen las familias para hacer frente a esta tendencia global. Por ejemplo, el 48,3% que tiene acceso a internet lo hace a través de su teléfono móvil.

Es preocupante que solo el 34,2% de los hogares a nivel nacional tenga acceso a una computadora y dentro de este conjunto de hogares, tres de cada cuatro hogares cuentan con una sola. La disposición de computadoras sube en Lima Metropolitana (48,7%), en el área urbana, sin incluir, la capital se alcanza el 39,7% y en las zonas rurales se reduce a 6,7%.

Así, tenemos que el uso de internet que hacen los niños y adolescentes que cursan la educación básica regular (primaria y secundaria) difiere según grupos de edad. Para la población de 6 a 11 años, el uso de internet alcanzó el 42,7%, contrastando con el 80,1% en el rango entre 12 a 18 años.

Respecto al uso de internet, es importante señalar que la educación y capacitación en red se ha mantenido aún precaria, tal es así que alrededor del 8,9% de la población mayor de 6 años utiliza internet para fines de educación formal y actividades de capacitación frente al 91% que lo utilizó para obtener información y el 89,8% para comunicarse. Esto revela la escasa costumbre y formación en el uso de las TIC aplicadas a la educación virtual en nuestro país.

Sobre la tenencia de dispositivos, los hogares con presencia de niños y adolescentes menores de 16 años que poseen al menos una computadora representan el 34,2%. Pese a este bajo porcentaje, si el COVID-19 y sus repercusiones hubiesen llegado en el 2008 habrían encontrado que en promedio solo el 18% de los hogares con hijos en edad escolar poseía una computadora.

Por otro lado, el creciente uso de las TIC ha mejorado las operaciones en la banca y generado modernos espacios para la compra y venta de productos y servicios. Por ejemplo, la banca electrónica pasó de representar el 5,5% del uso de internet en el año 2014 a 13,8% en el último trimestre de 2019.

Similar tendencia ha mostrado la compra de productos en línea con un salto de 4,2% en el año 2014 a 12,7% en el último trimestre de 2019. Estos indicadores se incrementarán en los próximos meses tomando en cuenta que la reanudación de actividades.

07. ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP. Yo creo que sí, el tema es que estamos un poco desordenados y las instituciones armadas deben estandarizar la capacidad de Ciberdefensa.

OE 2: Analizar la implicancia de los aspectos Confidencialidad, integridad y disponibilidad de la ciberdefensa del Estado peruano.

08. Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. El objetivo de identidad digital es permitir la autenticación en línea de la identidad de las personas peruanas y extranjeras cuando necesiten acceder a los servicios digitales brindados por las entidades públicas. También, proporciona el servicio de autenticación de la identidad digital a todas las instituciones públicas cuando desarrollen un servicio digital.

Atributos de la Identidad Digital

Son aquellos datos que en conjunto individualizan y caracterizan al ciudadano en el entorno digital. Se clasifican en inherentes y complementarios.

Atributos inherentes: permiten distinguir a un ciudadano digital distinto de otro en un determinado ámbito. Para los peruanos, estos datos son administrados por el Reniec y para el caso de extranjeros, por la Superintendencia Nacional de Migraciones. Son los siguientes:

Código único de identificación (CUI) para peruanos

Código único de extranjero (CUE) para extranjeros

Nombre y apellidos

Fecha de nacimiento

Lugar de nacimiento

Nacionalidad

Dirección

Correo electrónico o número de teléfono celular

Atributos complementarios: son aquellos atributos, que en conjunto con los atributos inherentes, permiten la caracterización de una persona desde una determinada perspectiva social, económica, judicial, entre otras. Por ejemplo: calificación como contribuyente, profesión, etc.

Asimismo, son gestionados por los Proveedores de Atributos de Identidad Complementarios (PAI), que son todas las entidades de la administración pública.

Documento Nacional de Identidad Digital (DNId)

Es el documento emitido por el Reniec en dispositivos digitales que acredita la identidad de la persona en entornos presenciales y no presenciales. Además, permite al ciudadano crear firmas digitales y puede ser usado para el ejercicio de voto electrónico en los procesos electorales organizados por la Oficina Nacional de Procesos Electorales (ONPE).

El DNId es una de las credenciales de autenticación que puede utilizar el ciudadano para demostrar que es quien dice ser en la Plataforma ID Gob.pe.

09. Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. La Plataforma Nacional de Interoperabilidad es una infraestructura tecnológica administrada por la Secretaría de Gobierno Digital que permite la implementación de servicios públicos en línea por medios electrónicos, y el intercambio electrónico de datos entre entidades del Estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles.

Se inauguró el 18 de octubre de 2011, mediante Decreto Supremo N° 083-2011-PCM. Actualmente es utilizada por más de 450 entidades del Poder Ejecutivo, gobiernos regionales y locales.

Beneficios

- Agiliza la realización de trámites por el ciudadano o usuario.
- Cooperación entre instituciones de la administración pública, sin distinción de su nivel de desarrollo tecnológico.
- Facilita la simplificación administrativa y los procesos de negocio de las instituciones.
- Reducción de los costos gracias a la reutilización de datos y funcionalidades.

10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del

Estado peruano?

RSP.

La seguridad digital es otro de los aspectos considerados en la Ley de gobierno digital.

Dicha ley nos indica que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

El Marco de seguridad digital del Estado peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública.

Respecto a la gestión del marco de seguridad digital del Estado peruano, la Ley de gobierno digital indica los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la administración pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)

La Norma Técnica Peruana NTP-ISO/IEC 17799 ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Gestión de la Seguridad de la Información (SGSI), al igual que la norma internacional ISO 27001, ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.

Respecto a la articulación de la seguridad digital con la seguridad de la información, El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar

confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano?

RSP.

La ley de gobierno digital tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la administración pública en los tres niveles de gobierno (estratégico, táctico y operativo) hacia la atención del ciudadano de Perú. Esto quiere decir que el fin principal del gobierno digital es atender al ciudadano usando la tecnología; pero esa tecnología cada vez es más peligrosa y en la actualidad existen muchos riesgos en su uso y administración. Existen muchos delincuentes que utilizan la tecnología para producir daño, existen muchos paises que se han dado cuenta que vulnerando la tecnología pueden producir daño a su adversario, en vista que el mundo está totalmente automatizado, todo campo y toda persona utiliza hoy en día la tecnología, cualquier tipo de tecnología es vulnerable, no existe sistema seguro, la seguridad total no existe, los encargados de la ciberdefesa tienen la gran responsabilidad de proteger al gobierno digital para que puede operar y actuar de manera segura.

La Ley de ciberdefesa en Perú, tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Entonces el uso del gobierno digital influye en la ciberdefensa del estado peruano.

Para poder ser efectivos en la ciberdefensa debemos de conocer y evaluar los elementos que conforman el gobierno digital y la ciberdefensa. Los mencionamos a continuación:

Gobierno digital; -Identidad digital -Interoperabilidad entre entidades públicas -Seguridad digital -Datos para la toma de decisiones -Arquitectura digital.

Ciberdefensa; -Persona –Ciberpersonas –Conocimiento -Sistemas de información-Infraestructura TIC -Terreno.

Tener una mirada sistémica es saber reconocer las características propias de cada sistema, todo puede tener una mirada sistémica, los sistemas tienen un objetivo propio (Misión de la organización), está conformado por elementos que trabajan para cumplir el objetivo de la organización, siempre tiende a fallar o envejecer y siempre se podrá corregir esa falla. Asimismo, también podemos ordenar el trabajo de proteger al gobierno digital, reconociendo los aspectos recurso humano, normatividad, infraestructura física, comunicaciones, redes y tecnología.

12.- ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano?

RSP.

La tecnología es un elemento fundamental en el gobierno digital, sin tecnología no podríamos alcanzar tener un gobierno digital.

La tecnología es la aplicación de la ciencia a la resolución de problemas concretos.

Constituye un conjunto de conocimientos científicamente ordenados, que permiten diseñar y crear bienes o servicios que facilitan la adaptación al medio ambiente, así como la satisfacción de las necesidades individuales esenciales y las aspiraciones de la humanidad.

La Ley de gobierno digital define como Tecnologías Digitales, a las tecnologías de la información y la comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los

riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

OE 3: Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

14 ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano?

RSP. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

Uno de los objetivos del gobierno digital es normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

15 ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP. La ley No 30999 tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley y tiene como finalidad de defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

16 Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector tiene las siguientes atribuciones:

a) Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.
b) Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.
c) Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.
d) Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.
e) Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.
f) Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.
g) Definir los alcances del marco normativo en materia de gobierno digital.
h) Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.
i) Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.
j) Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.
k) Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.
l) Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.

17 Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, debiendo para tal efecto:

a) Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.
b) Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.
c) Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.
d) Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.
e) Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.
f) Considerar la implementación de pagos a través de canales digitales.
g) Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.
h) Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.
i) Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Muchas gracias

ENTREVISTA 03 DESARROLLADA Y CONSENTIMIENTO INFORMADO

Guía de entrevista 2 – Experto.

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mg. Manuel Antonio Pereyra Acosta		
Datos del entrevistado 01	Mg. Magister en Administración y Doctrina Aeroespacial, 15 años de experiencia en el campo de las tecnologías de la información y comunicaciones para el Estado peruano. Jefe del Departamento de Ingeniería de Software del Servicio de Informática de la FAP.		
Fecha:	Hora: 19:00	Sexo: M	Edad: 41
Lugar: Reunión virtual	Duración: 2 Hrs.		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar [x] No Acepto participar [ ]

Preguntas a un experto en ciberdefensa.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

01.- ¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del Estado peruano?

Según el D.L 1412 el Gobierno digital, como uso estratégico de tecnologías las digitales y datos en la Administración Pública para la creación de valor público, se sustenta en ciudadanos y actores del sector público o los recursos humanos del Estado, motivo por el cual podemos afirmar que la implicancia del aspecto humano en el gobierno digital es significativa y positiva. Cada Institución del Estado debe establecer una estrategia para atraer, desarrollar y retener recursos humanos con el conjunto necesario de capacidades

y habilidades para apoyar la transformación digital de su entidad, más allá de los incentivos económicos, porque no hay transformación digital posible sin especialistas digitales para llevarla adelante y sin que todos los servidores públicos puedan implementar correctamente las nuevas tecnologías. La relación entre la agenda digital y la gestión del recurso humano es indiscutible e ineludible.

02.- Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Según Hillis Miller en su ensayo the poetics of ciberspace: Two ways to get life, estamos en la era de la cibercultura y las ciberpersonas y asimismo estas son las identidades digitales del ciudadano de hoy (Ecija, 2019). La relación entre las ciberpersonas y el gobierno digital del Estado es positiva, toda vez que, el Perú garantiza el uso seguro y fiable del ciberespacio protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico, es por ello que el gobierno digital utilizara todas sus medidas de seguridad correspondientes, para proteger la confidencialidad de la ciberpersona, de esta manera podríamos estar seguros de la integridad de la información. En la actualidad, existen muchas formas de vulnerar la seguridad de la ciberpersona, se realizan robos de identidad digital para extorsión, así como robos económicos, de reconocimiento, curiosidad, morbo, entre muchos otros impulsos de los ciberdelincuentes cometen.

03.- Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

En su sentido más general, la palabra conocimiento alude a la información acumulada sobre un determinado tema o asunto. En un sentido más específico, el conocimiento es definido como el conjunto de habilidades, destrezas, procesos mentales e información adquiridos por el individuo, cuya función es ayudarle a interpretar la realidad, resolver problemas y dirigir su comportamiento. La implicancia del gobierno digital en las sociedades del conocimiento es muy significativa, toda vez que, impacta positivamente en las personas mediante las Tecnologías de Información y Comunicación (TIC), que tienen el poder de transformar las economías y las sociedades. Motivo por el cual las sociedades del conocimiento en un gobierno digital se apoyan en la libertad de expresión, el acceso universal a la información y al conocimiento, el respeto a la diversidad cultural y lingüística, y una educación de calidad para todos

04.- Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Un sistema de información es un conjunto de datos que interactúan entre sí con un fin común, su importancia radica en la eficiencia de la correlación de una gran cantidad de datos ingresados a través de procesos diseñados para cada área con el objetivo de producir información válida para la posterior toma de decisiones. El gobierno digital tiene una implicancia positiva en los sistemas de información, ya que eleva la eficiencia operativa del gobierno mediante el uso de las tecnologías de la información y las comunicaciones (TIC), de igual forma a través de un marco normativo, asegurar la administración y operación de las tecnologías de la información y las comunicaciones (TIC) y finalmente

ayuda a fomentar el desarrollo del gobierno digital mediante la vinculación con organismos nacionales e internacionales, industrias, academias y la sociedad.

05.- Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

La infraestructura de tecnología de la información y comunicación (TIC) hace referencia a los elementos necesarios para operar y gestionar entornos de TI empresariales. La infraestructura de TI puede implementarse en un sistema de cloud computing o en las instalaciones de las entidades públicas. Estos elementos incluyen el hardware, el software, los elementos de red, un sistema operativo y el almacenamiento de datos. Todos ellos se utilizan para ofrecer servicios y soluciones de TI. Los productos de infraestructura de TIC se pueden descargar como aplicaciones de software que se ejecutan sobre los recursos de TI actuales (por ejemplo, el almacenamiento definido por software) o como soluciones en línea que ofrecen los proveedores de servicios. Dicho lo anterior, la infraestructura TIC tiene una implicancia positiva, ya que incentiva buenas practicas del gobierno digital para cerrar la brecha tecnológica actual.

06.- Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

El medio ambiente o terreno es el sitio gubernamental donde se accede a la información sobre medio ambiente y la organización de la misma refleja qué tipo de jerarquía le otorga el gobierno en cuestión a la información a procesar. Las provincias representan alrededor del 50% de las operaciones en línea en el país, y Lima la otra mitad. Mientras que el 79.9% de hogares en Lima Metropolitana tienen conexión a Internet, solo 25.5% de los hogares rurales lo hacen; esto se debe a que las zonas rurales todavía son menos atractivas para que los inversionistas privados desplieguen de redes de telecomunicaciones, dado que la menor densidad de clientes potenciales dificulta la recuperación de la inversión. Es en el contexto mencionado que el gobierno digital tiene importancia positiva, dado que ayudara a reducir la brecha digital del Estado Peruano.

07.- ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

Entendemos como Ciberdefensa al conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos. En el Perú, según la Secretaria de Gobierno Digital, existe una carencia en recursos humanos capacitados en ciberdefensa para cumplir lo estipulado líneas arriba, es por eso que el Estado, mediante sus diversas Instituciones públicas deben procurar la constante formación de sus cuadros en mencionada especialidad, es decir fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado, cada vez más importante para poder cumplir la ley de gobierno digital.

OE 2: Analizar la implicancia de los aspectos Confidencialidad, integridad y disponibilidad de la ciberdefensa del Estado peruano.

08.- Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

La identidad digital es la versión en internet de la identidad física de una persona. Está compuesta por una gran cantidad de datos que proporcionamos en la red, más allá de nuestro correo electrónico y dirección: incluye nuestras fotos, datos bancarios, preferencias a la hora de compra. En el Perú la Ley de Gobierno Digital y su reglamento establecen el Marco de Identidad Digital del Estado Peruano, siendo uno de sus componentes la Plataforma Nacional de Identificación y Autenticación de la Identidad Digital. Su objetivo es permitir la autenticación en línea de la identidad de las personas peruanas y extranjeras cuando necesiten acceder a los servicios digitales brindados por las entidades públicas. También, proporciona el servicio de autenticación de la identidad digital a todas las instituciones públicas cuando desarrollen un servicio digital. La implicancia de la identidad digital es positiva y significativa en el gobierno digital ya que fomenta la modernización del Estado y permite la interoperabilidad entre las diversas instituciones públicas.

09.- Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Uno de los principales retos de la Administración Pública es asegurar que la interacción y colaboración entre las entidades públicas sea segura, eficiente y ajustada a la normativa vigente; más aún, se debe asegurar que dichos esfuerzos sean adecuadamente articulados y gestionados para generar valor al ciudadano. Es así, que, con el devenir del tiempo, las Tecnologías de la Información y Comunicaciones (TIC) han habilitado a las organizaciones a que la llamada “colaboración” se materialice entre estas usando una característica de los Sistemas de Información denominada “Interoperabilidad”, mecanismo por medio del cual éstas pueden intercambiar datos e información, independientemente de la plataforma de desarrollo que las soporte o hagan uso. La implicancia de la interoperabilidad es positiva en el gobierno digital y muestra de eso es el despliegue de esfuerzos para la digitalización de la Administración Pública con miras a lograr un Estado al servicio del ciudadano; lo cual se consolida con la dación de un conjunto de dispositivos legales, en particular, los Decretos Legislativos N° 1246 y N° 1310, mediante los cuales se dictan medidas para la simplificación administrativa, siendo uno de los mecanismos para lograr tal fin el uso intensivo de la interoperabilidad y, sobre todo, de la Plataforma de Interoperabilidad del Estado (PIDE), la cual debe habilitar el intercambio de datos e información entre las entidades.

10.- Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

Según el Decreto Supremo N° 050 – 2018 PCM, la Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos de la confianza en el entorno digital y los riesgos en el entorno digital o riesgo de seguridad digital. En

mencionado contexto, la implicancia en el gobierno digital es muy positiva dado que la entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

11.- ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano?

Se entiende como ciberdefensa a todos aquellos usos de conocimiento, habilidades, y medios para realizar operaciones en y mediante el ciberespacio. En el Peru el Poder Ejecutivo oficializó la Ley de Ciberdefensa, cuyo objetivo es proteger la soberanía, los intereses nacionales y los recursos claves del Perú ante amenazas o ataques cibernéticos, cuando estos afecten la seguridad nacional. La planificación y ejecución de las operaciones de ciberdefensa están a cargo del Comando Conjunto de las Fuerzas Armadas bajo la supervisión del Ministerio de Defensa. El cumplimiento de la ley de gobierno digital tiene una fuerte implicancia en la ciberdefensa ya que permite establecer, norma, supervisa y evalúa las normas en materia de ciberdefensa; que el Comando Conjunto de las Fuerzas Armadas que están a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional; y que es la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros quien establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la ley

12.- ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano?

La tecnología es un componente de la Sociedad de la Información de un gobierno digital, parte del concepto que se tiene de esta sociedad, En el Perú no sólo hemos incorporado esa tecnología en el campo, sino que también se han convertido en una herramienta para la optimización en la gestión de todo el sistema sanitario; la reducción de las desigualdades en el acceso a servicios de salud; el acceso al ciudadano a información y contenidos sobre prevención de enfermedades y buenas prácticas en materia de salud; y, la integración de las personas discapacitadas a la sociedad. Para los países en vías de desarrollo como el Perú, es tratar de acortar la brecha digital e incorporar la tecnología y la modernidad en espacios que permitan mejorar la calidad de los productos y buscarles nuevos mercados. Es por ello que el Estado Peruano, afronta el gran reto de impulsar el desarrollo de la tecnología en una situación en el que mayormente la población cuenta con niveles socioeconómicos bajos, escasos niveles de bancarización, reducidos niveles de alfabetización digital especialmente en las zonas rurales y alejadas , escaso presupuesto para invertir en tecnologías de información y comunicaciones en las Entidades Estatales y casi una nula integración de sus sistemas informáticos, impidiendo esto último, la operación horizontal del Estado, así como la creación de ventanillas únicas, focalizadas en servicios sectoriales.

13.- ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

Lastimosamente no se cuenta con las tecnologías apropiadas para la ciberdefensa. Se afirma que la estructura social y política del estado-nación actual es una respuesta a la seguridad, que necesariamente implica estar en condiciones de defenderse de amenazas, riesgos y peligros. Por ello, seguridad y defensa son inherentes a la supervivencia y desarrollo del hombre y la sociedad. En suma, el desarrollo de un Estado está íntimamente ligado a su condición de seguridad y a las acciones que se ejecuten para mantener esa condición, es decir, su capacidad de defensa. Las vulnerabilidades a los ciberataques se continúan ampliando, no solo porque internet se expande rápidamente con más servicios y usuarios, sino también porque el número y la sofisticación de los ciberataques aumenta en una proporción mayor, es por eso que actualmente no se podría cumplir la ley de gobierno digital.

OE 3: Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

14.- ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano?

En las últimas cuatro décadas lo que ha revolucionado a la historia de la humanidad, por la influencia, magnitud y rapidez de su implementación, han sido las Tecnologías de la Información y la Comunicación (TIC), que han dado forma a lo que hoy designamos como Revolución Digital. La disrupción digital, es un fenómeno que viene transformando irreversiblemente al mundo hace ya algunas décadas, y en los últimos meses, debido a la pandemia COVID-19, se ha acelerado este proceso de digitalización ante la necesidad de adaptarse a las nuevas condiciones de bioseguridad y a los grandes cambios económicos, sociales y políticos que se vislumbran en el mediano y largo plazo, sin embargo el desarrollo de normas en el Perú aun sigue siendo escaso, el mismo que genera un brecha de aspectos normativos. El aspecto normativo tiene una gran implicancia en las normas, ya que, permite establecer las bases formales para la actuación correcta de las instituciones púbicas a fin de brindar un buen servicio al ciudadano con respecto a las transformaciones de las TICs mencionadas líneas arriba.

15.- ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

En la actualidad no se cuenta con la normatividad suficiente en el ámbito para la ciberdefensa para dar cumplimiento de la ley de gobierno digital. A la fecha, solo se cuenta con la Ley Nº 309999 “Ley de ciberdefensa”, la misma que tiene por objeto objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia y cuya finalidad es defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. Sin embargo, aún está pendiente la elaboración del Reglamento de la Ley, donde se detallará acciones más específicas para las Fuerzas Armadas y su responsabilidad con el ciberespacio.

16.- Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

El proceso de identificación de un problema u oportunidad y la selección de una alternativa de acción entre varias existentes, es una actividad conocida como toma de decisiones, y esta tiene una alta implicancia en el gobierno digital. Es fundamental que las decisiones se tomen con sabiduría y que las acciones que implemente cada sujeto y organización publica, cuenten con cimientos sólidos. Recordemos que las decisiones son muy importantes, ya que los resultados trascenderán a lo largo del presente y el futuro de las organizaciones y de los ciudadanos. El gobierno digital ha evolucionado desde la década de los noventa como herramienta de apoyo estatal para desarrollar su función de servicio a los ciudadanos. Dentro de la creciente tendencia por aplicar conceptos clásicos de la gestión privada en el ámbito público, es clave identificar las Tecnologías de la Información y las Comunicaciones (TIC) como elemento de apoyo y no como un fin, de tal manera que soporten el proceso de toma de decisiones ejecutado por los gestores públicos.

17.- Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

La arquitectura digital mediante modelados de computadora, programación, simulación e imágenes para crear formas virtuales y estructuras físicas está permitiendo al gobierno digital de una Estado poder lograr sus objetivos con respecto a la satisfacción de sus cuidados. El uso de arquitecturas digitales en el Estado está haciendo posible que gobiernos, instituciones y empresas, puedan esconder menos su información, los está volviendo más abiertos, más transparentes. La importancia de definir un marco o modelo de arquitectura permite la gobernanza y esto hace que las organizaciones gubernamentales o no gubernamentales entiendan la importancia estratégica de las TIC, por su capacidad de comunicación, universalidad y de conocimiento colaborativo que solo es posible mediante el uso de las TIC, por ello con base a las nuevas tendencias en educación superior se demanda una preparación del profesionista acorde con las necesidades de su entorno, apoyado en una formación basada en competencias para el desarrollo de nuevas habilidades para la utilización de un modelo gobernanza digital, el cual establece las estructuras que sirven de enlace entre los recursos y los procesos de TIC con la planeación estratégica de la organización y que permite institucionalizar las prácticas de organización, planeación, operación y entrega de bienes y/o servicios de la organización de que se trate, en donde la gobernanza se refiere a la estructura de control y establece una organización para dirigir, evaluar y vigilar la efectividad organizativa, procurando la transparencia y la participación colectiva para mejorar continuamente lo establecido, mediante políticas y lineamientos.

Muchas gracias

ENTREVISTA 04 DESARROLLADA Y CONSENTIMIENTO INFORMADO

Guía de entrevista 2 – Experto.

Titulo:	La Ley de gobierno digital y su implicancia en la ciberdefensa del Estado peruano, 2021		
Línea de investigación:	Reforma y modernización del estado		
Nombre:	Mg. Manuel Antonio Pereyra Acosta		
Datos del entrevistado 01	Mg. Magister en Seguridad de la información, 10 años de experiencia en el campo de las tecnologías de la información y comunicaciones para el Estado peruano. Centro de seguridad de la información.		
Fecha:	Hora: 9:00 Hrs.	Sexo: M	Edad: 38
Lugar: Reunión virtual	Duración: 2 Hrs		

Saludos cordiales.

Quien lo saluda es el Magister Manuel Antonio Pereyra Acosta, le quiero dar las gracias por su tiempo y por estar dispuesto a participar en esta entrevista que forma parte de la investigación que vengo realizando. El estudio que estoy realizando tiene como objetivo analizar la implicancia de la Ley de gobierno digital en la ciberdefensa del Estado peruano. Utilizando el diseño metodológico el caso de ciberguerra en un país totalmente automatizado producto del cumplimiento de la ley de gobierno digital; por lo que las respuestas que Ud. me brinde en esta oportunidad serán grabadas para cuidar todos los detalles de la información; en ese sentido le pido la autorización para proceder así mismo le comunico que los datos que usted me brinde se mantendrán en estricta confidencialidad, y me servirán como insumo para poder desarrollar la presente investigación.

Acepto participar [X] No Acepto participar [ ]

Preguntas a un experto en ciberdefensa.

OE 1: Analizar la implicancia del aspecto recurso humano, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

1. **¿Cuál es la implicancia del aspecto recurso humano en el gobierno digital del estado peruano?**

RSP. Los momentos de crisis, parece que nos bloquean, pero una vez superada esa fase, nos sirven para parar y ser conscientes de la situación, de los retos que tenemos, a los que tenemos que enfrentarnos para avanzar. En Recursos Humanos, ahora más que nunca, debemos entender cuáles son en esta era digital en la que vivimos, para sacar el mejor provecho.

La era digital nos obliga a contar con un equipo que se adapte. Tener a personas en el gobierno digital que sepan cual es el propósito y que puedan adaptarse a los cambios siendo flexibles, es vital para el estado peruano.

2. **Respecto a la ciberpersona, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?**

RSP. Es importante que todo peruano tenga acceso a la tecnología ya que se considera un servicio importante para la persona. La tecnología se refiere a la colección de herramientas que hacen más fácil usar, crear, administrar e intercambiar información. En el inicio de los tiempos, los seres humanos hacían uso de ella para el proceso de descubrimiento del mundo y evolución. La tecnología es el conocimiento y la utilización de herramientas, técnicas y sistemas con el fin de servir a un propósito más grande como la resolución de problemas o hacer la vida más fácil y mejor. Su importancia para los seres humanos es enorme porque les ha ayudado a adaptarse al entorno.

3. **Respecto al conocimiento, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?**

RSP El conocimiento en el gobierno digital del estado peruano está variando sustancialmente en todos los sentidos y en todos los ámbitos de la vida pedagógica. No solo se asiste a una auténtica revolución dentro de las aulas, sino que además el individuo indaga, busca, investiga (y a menudo hasta encuentra) información siguiendo patrones esencialmente distintos.

4. **Respecto a los sistemas de información, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?**

RSP Durante los últimos años los sistemas de información constituyen uno de los principales ámbitos de estudio en el estado peruano. El entorno donde las organizaciones desarrollan sus actividades se vuelve cada vez más complejo. La creciente globalización, el proceso de internacionalización del estado, el incremento de la competencia en los mercados de bienes y servicios, la rapidez en el desarrollo de las tecnologías de información, el aumento de la incertidumbre en el entorno y la reducción de los ciclos de vida de los productos originan que la información se convierta en un elemento clave para la gestión, así como para la supervivencia y crecimiento del país. Si los recursos básicos analizados hasta ahora eran tierra, trabajo y capital, ahora la información aparece como otro insumo fundamental a valora el estado.

5. **Respecto a la infraestructura TIC, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?**

RSP Respecto a la infraestructura de las TIC podemos denotar cómo ha evolucionado el uso de las TIC en donde pensábamos que no iba a ser menos y que a su vez se puede ir incentivando y actualmente se puede observar como los profesionales en este ámbito utilizan estas nuevas TIC en el desarrollo cotidiano de Labor como docentes con muy buenos resultados. En la Conferencia Internacional de Educación celebrada en Ginebra en 2001 denominada “La educación para todos para aprender a vivir juntos” ya se hacía referencia a la importancia que iban a tener estas nuevas TIC en el ámbito educativo acorde a los cambios que están experimentando nuestras

sociedades modernas. Se observa un notable interés en la comunidad educativa en el uso docente de estas TIC.

6. Respecto al terreno, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. El comercio electrónico, telesalud, educación virtual y el teletrabajo vienen ganando más terreno que nunca. Y es que en tiempos de cuarentena se ha hecho cada vez más estrecha la relación de las Tecnologías de Información y Comunicaciones (TIC) con las actividades cotidianas y la forma de hacer los negocios.

El 93,9% de los hogares en el Perú cuenta con al menos una TIC, que comprende telefonía fija, telefonía celular, internet, televisión y radio. Asimismo, dicho porcentaje es mayor en hogares cuyo jefe de hogar cuenta con educación superior universitario (100%), en comparación a aquellos hogares cuyo jefe tiene educación primaria (85,1%). Esta información se desprende del informe Estadísticas de las Tecnologías de Información y Comunicación en los Hogares, elaborado por el Instituto Nacional de Estadística e Informática (INEI) correspondiente al cuarto trimestre del 2019.

Sin embargo, el bajo acceso a internet resta la posibilidad de aprovechar en mayor medida de los beneficios en el uso de las TIC.

A nivel nacional, solo el 38,8% de los hogares cuenta con internet; con una mayor cobertura en Lima Metropolitana (LM), donde el 59,6% de los hogares tiene este servicio. No obstante, la brecha de disposición tecnológica es mucho más marcada al comparar el área urbana (excluyendo LM) con la rural: en el área urbana, 41 de cada 100 hogares disponen del servicio de internet. En el extremo opuesto, se ubican las familias del área rural, donde solo 6 de cada 100 hogares cuentan con dicho servicio.

En el campo de la educación, el auge repentino de la enseñanza no presencial nos lleva a evaluar el acceso a internet y a los dispositivos con los que tienen las familias para hacer frente a esta tendencia global. Por ejemplo, el 48,3% que tiene acceso a internet lo hace a través de su teléfono móvil.

Es preocupante que solo el 34,2% de los hogares a nivel nacional tenga acceso a una computadora y dentro de este conjunto de hogares, tres de cada cuatro hogares cuentan con una sola. La disposición de computadoras sube en Lima Metropolitana (48,7%), en el área urbana, sin incluir, la capital se alcanza el 39,7% y en las zonas rurales se reduce a 6,7%.

Así, tenemos que el uso de internet que hacen los niños y adolescentes que cursan la educación básica regular (primaria y secundaria) difiere según grupos de edad. Para la población de 6 a 11 años, el uso de internet alcanzó el 42,7%, contrastando con el 80,1% en el rango entre 12 a 18 años.

Respecto al uso de internet, es importante señalar que la educación y capacitación en red se ha mantenido aún precaria, tal es así que alrededor del 8,9% de la población mayor de 6 años utiliza internet para fines de educación formal y actividades de capacitación frente al 91% que lo utilizó para obtener información y el 89,8% para comunicarse. Esto revela la escasa costumbre y formación en el uso de las TIC aplicadas a la educación virtual en nuestro país.

Sobre la tenencia de dispositivos, los hogares con presencia de niños y adolescentes menores de 16 años que poseen al menos una computadora representan el 34,2%. Pese a este bajo porcentaje, si el COVID-19 y sus repercusiones hubiesen llegado en el 2008 habrían encontrado que en promedio solo el 18% de los hogares con hijos en edad escolar poseía una computadora.

Por otro lado, el creciente uso de las TIC ha mejorado las operaciones en la banca y generado modernos espacios para la compra y venta de productos y servicios. Por ejemplo, la banca electrónica pasó de representar el 5,5% del uso de internet en el año 2014 a 13,8% en el último trimestre de 2019.

Similar tendencia ha mostrado la compra de productos en línea con un salto de 4,2% en el año 2014 a 12,7% en el último trimestre de 2019. Estos indicadores se incrementarán en los próximos meses tomando en cuenta que la reanudación de actividades.

7. ¿Contamos con recurso humano capacitado en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP. Yo creo que sí, el tema es que estamos un poco desordenados y las instituciones armadas deben estandarizar la capacidad de Ciberdefensa.

OE 2: Analizar la implicancia de los aspectos Confidencialidad, integridad y disponibilidad de la ciberdefensa del Estado peruano.

8. Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. El objetivo de identidad digital es permitir la autenticación en línea de la identidad de las personas peruanas y extranjeras cuando necesiten acceder a los servicios digitales brindados por las entidades públicas. También, proporciona el servicio de autenticación de la identidad digital a todas las instituciones públicas cuando desarrollen un servicio digital.

Atributos de la Identidad Digital

Son aquellos datos que en conjunto individualizan y caracterizan al ciudadano en el entorno digital. Se clasifican en inherentes y complementarios.

Atributos inherentes: permiten distinguir a un ciudadano digital distinto de otro en un determinado ámbito. Para los peruanos, estos datos son administrados por el Reniec y para el caso de extranjeros, por la Superintendencia Nacional de Migraciones. Son los siguientes:

Código único de identificación (CUI) para peruanos

Código único de extranjero (CUE) para extranjeros

Nombre y apellidos

Fecha de nacimiento

Lugar de nacimiento

Nacionalidad

Dirección

Correo electrónico o número de teléfono celular

Atributos complementarios: son aquellos atributos, que en conjunto con los atributos inherentes, permiten la caracterización de una persona desde una determinada perspectiva social, económica, judicial, entre otras. Por ejemplo: calificación como contribuyente, profesión, etc.

Asimismo, son gestionados por los Proveedores de Atributos de Identidad Complementarios (PAI), que son todas las entidades de la administración pública.

Documento Nacional de Identidad Digital (DNId)

Es el documento emitido por el Reniec en dispositivos digitales que acredita la identidad de la persona en entornos presenciales y no presenciales. Además, permite al ciudadano crear firmas digitales y puede ser usado para el ejercicio de voto electrónico en los procesos electorales organizados por la Oficina Nacional de Procesos Electorales (ONPE).

El DNId es una de las credenciales de autenticación que puede utilizar el ciudadano para demostrar que es quien dice ser en la Plataforma ID Gob.pe.

9. Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. La Plataforma Nacional de Interoperabilidad es una infraestructura tecnológica administrada por la Secretaría de Gobierno Digital que permite la implementación de servicios públicos en línea por medios electrónicos, y el intercambio electrónico de datos entre entidades del Estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles.

Se inauguró el 18 de octubre de 2011, mediante Decreto Supremo N° 083-2011-PCM. Actualmente es utilizada por más de 450 entidades del Poder Ejecutivo, gobiernos regionales y locales.

Beneficios

- Agiliza la realización de trámites por el ciudadano o usuario.
- Cooperación entre instituciones de la administración pública, sin distinción de su nivel de desarrollo tecnológico.
- Facilita la simplificación administrativa y los procesos de negocio de las instituciones.
- Reducción de los costos gracias a la reutilización de datos y funcionalidades.

10. Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. Según el decreto Supremo No 050-2018-PCM la definición de Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en

la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes:

a) Nota 1: La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.
b) Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.
c) Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego.
d) Nota 4: La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.

11. ¿Cuál es la implicancia del cumplimiento de la ley de gobierno digital en la ciberdefensa del estado peruano?

RSP. La finalidad de la ley de Ciberdefensa es Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. Los órganos ejecutores son las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

12. ¿Cuál es la implicancia de la tecnología en el gobierno digital del Estado peruano?

RSP.

13. ¿Contamos con tecnología apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP. Si, cada instituto armado (Marina, Ejercito, Fuerza Aérea y Comando Conjunto) cuenta con una organización para mitigar los riesgos en el ciberespacio de acuerdo a su ámbito de su competencia.

La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la ley No 30999, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y

el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables.

OE 3: Analizar la implicancia del aspecto normativo, de la Ley de gobierno digital, en la ciberdefensa del Estado peruano.

14. ¿Cuál es la implicancia del aspecto normativo en el gobierno digital del Estado peruano?

RSP. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

Uno de los objetivos del gobierno digital es normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

15. ¿Contamos con normatividad apropiada en ciberdefensa, para enfrentar todos los riesgos que se podrían presentar en cumplimiento de la Ley de gobierno digital?

RSP. La ley No 30999 tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley y tiene como finalidad de defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

16. Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector tiene las siguientes atribuciones:

m) Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.

n) Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.
o) Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.
p) Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.
q) Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.
r) Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.
s) Definir los alcances del marco normativo en materia de gobierno digital.
t) Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.
u) Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.
v) Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.
w) Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.
x) Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.

17. Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?

RSP. Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, debiendo para tal efecto:

j) Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.
k) Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.
l) Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.
m) Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio

la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.

n) Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.
o) Considerar la implementación de pagos a través de canales digitales.
p) Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.
q) Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.
r) Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Muchas gracias

Anexo 6. MATRIZ DE ANÁLISIS DE DATOS

CATEGORIA	SUBCATEGORIA	PREGUNTA	RESPUESTA EXPERTO 01	RESPUESTA EXPERTO 02	RESUMEN
Gobierno digital	Identidad digital	Respecto a identidad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?	La identidad digital es algo muy parecido a lo mencionado en ciperpersona. La identidad digital debe ser único y propio de cada persona, es la manera de acceder a los sistemas del gobierno digital. La identidad digital puede ser robada, alterada, modificada o vulnerada por delincuentes que desean hacer uso de una identidad que les permitan acceder a la información de los sistemas o cuentas bancarias o información de las infraestructuras criticas nacionales. El Decreto Legislativo Nº 1412 del 13 de setiembre del 2018, en su artículo 10, nos brinda el concepto de identidad digital, "Identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales". También nos indica que, los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo. De acuerdo a un artículo publicado por Edgar Huaranga en HIPERDERECHO, el 8 de abril del 2021 en la página web de esta organización civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Huaranga define Identidad Digital como el conjunto de mecanismos utilizados para verificar la identidad de una persona en un entorno digital. Para los ciudadanos, estos entornos serían principalmente páginas web o aplicaciones móviles. Entonces nos podríamos plantear las siguientes preguntas: ¿Qué me hace único como persona? y ¿quién decide o	El objetivo de identidad digital es permitir la autenticación en línea de la identidad de las personas peruanas y extranjeras cuando necesiten acceder a los servicios digitales brindados por las entidades públicas. También, proporciona el servicio de autenticación de la identidad digital a todas las instituciones públicas cuando desarrollen un servicio digital. Atributos de la Identidad Digital Son aquellos datos que en conjunto individualizan y caracterizan al ciudadano en el entorno digital. Se clasifican en inherentes y complementarios. Atributos inherentes: permiten distinguir a un ciudadano digital distinto de otro en un determinado ámbito. Para los peruanos, estos datos son administrados por el Reniec y para el caso de extranjeros, por la Superintendencia Nacional de Migraciones. Son los siguientes: Código único de identificación (CUI) para peruanos Código único de extranjero (CUE) para extranjeros Nombre y apellidos Fecha de nacimiento Lugar de nacimiento Nacionalidad Dirección Correo electrónico o número de teléfono celular Atributos complementarios: son aquellos atributos, que en conjunto con los atributos inherentes, permiten la caracterización de una persona desde una determinada perspectiva social, económica, judicial, entre otras. Por ejemplo: calificación como contribuyente, profesión, etc. Asimismo, son gestionados por los Proveedores de Atributos de Identidad Complementarios (PAI), que son todas las entidades de la administración pública. Documento Nacional de Identidad Digital (DNId) Es el documento emitido por el Reniec en dispositivos digitales que acredita la identidad de la	La identidad digital tiene una implicancia directa en el gobierno digital del Estado peruano, en vista que es el conjunto de atributos que individualizan y permiten la identificacion de una persona en los entornos digitales del Estado peruano, a traves de las instituciones publicas. La identidad digital permite ingresar de manera confiable y segura, a la persona al gobierno digital y de esta manera poder utilizar los sistemas, portales, paginas web y herramientas tecnologicas ofrecidas por el Estado.

			de quién depende afirmar que realmente soy yo la persona que está utilizando una web o aplicación? Existen características físicas y biológicas que nos diferencian de otras personas. Por ejemplo, podríamos pensar en nuestra estatura, color de ojos o algunas manchas en nuestra piel. Sin embargo, el problema con estas características es que, a pesar de parecer únicas en nuestro entorno, otras personas también las pueden tener. Por otro lado, existen características que realmente nos hacen únicos y que se utilizan en todo el mundo para identificar a personas de manera individual. Algunos ejemplos son nuestras huellas dactilares, nuestro rostro o nuestra voz. Estos conjuntos de características están clasificados como datos biométricos, que a pesar de no ser los únicos son los más utilizados por los sistemas computacionales a nivel global. En el Perú, el Registro Nacional de Identificación y Estado Civil (RENIEC) es la institución encargada de organizar y mantener el registro único de identificación de las personas, y por lo tanto, se encarga también de emitir el Documento Nacional de Identidad (DNI) que acredita la identidad de las personas. La importancia de RENIEC en el contexto de identidad digital se debe a que también tiene la facultad de emitir certificados digitales para personas naturales o jurídicas que lo soliciten. Estos certificados digitales vendrían a ser un análogo del DNI o del pasaporte en un entorno digital; dándonos la seguridad de que el intercambio de información es entre personas o entidades que realmente son quien dicen ser y que la comunicación	persona en entornos presenciales y no presenciales. Además, permite al ciudadano crear firmas digitales y puede ser usado para el ejercicio de voto electrónico en los procesos electorales organizados por la Oficina Nacional de Procesos Electorales (ONPE). El DNId es una de las credenciales de autenticación que puede utilizar el ciudadano para demostrar que es quien dice ser en la Plataforma ID Gob.pe.	

			entre ellos estará segura y protegida. Este sistema de certificados digitales es válido y confiable porque es parte de una infraestructura más grande y compleja que involucra hardware, software, políticas y procedimientos de seguridad que tienen como base la criptografía asimétrica. Esta infraestructura se llama Infraestructura de Clave Pública PKI por sus siglas en inglés (Public Key Infraestructure). Con la tecnología de los últimos diez años y teniendo como referencia la implementación de identidad digital en otros países, en el Perú se desarrollaron diferentes plataformas o soluciones orientadas al ciudadano para acelerar procesos o trámites que en persona tomarían días o debían seguir un proceso burocrático muy lento y agotador. Esto aprovechando nuestros datos biométricos o certificados digitales en caso contemos con ellos. Los proyectos que el Estado está desarrollando para ofrecer soluciones respecto a identidad digital orientado al ciudadano son: DNI electrónico, El portal del ciudadano y la plataforma de autenticación de la identidad digital nacional.		

	Interoperabilidad entre entidades publicas	Respecto a la interoperabilidad entre las entidades públicas, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?	En el capítulo V del Decreto Legislativo Nº 1412 del 13 de setiembre del 2018, nos indica que la Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información. El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter administrativos de valor para el ciudadano provisto a través de canales digitales. En esta misma norma, nos indica ciertos aspectos sobre la gestión del marco de interoperabilidad del Estado Peruano, la cual se gestiona a través de los siguientes niveles: 1) Interoperabilidad a nivel organizacional: Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la administración pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias. 2) Interoperabilidad a nivel semántico: Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser	La Plataforma Nacional de Interoperabilidad es una infraestructura tecnológica administrada por la Secretaría de Gobierno Digital que permite la implementación de servicios públicos en línea por medios electrónicos, y el intercambio electrónico de datos entre entidades del Estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles. Se inauguró el 18 de octubre de 2011, mediante Decreto Supremo N° 083-2011-PCM. Actualmente es utilizada por más de 450 entidades del Poder Ejecutivo, gobiernos regionales y locales. Beneficios • Agiliza la realización de trámites por el ciudadano o usuario. • Cooperación entre instituciones de la administración pública, sin distinción de su nivel de desarrollo tecnológico. • Facilita la simplificación administrativa y los procesos de negocio de las instituciones. • Reducción de los costos gracias a la reutilización de datos y funcionalidades.	La interoperabilidad entre las instituciones publicas ayudan al gobierno digital en alcanzar lo siguiente: -Mejor atencion de tramites al ciudadano y a las instituciones publicas usuarias. (atencion con mayor rapidez y menor burocracia) - Cooperacion entre las instituciones publicas en el manejo de los datos, informacion y conocimiento. - Simplifica los procesos administrativos de las organizaciones publicas. - Reduccion de costos, tiempo y distancia con el uso de la tecnologia.

			intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la administración pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información. 3) Interoperabilidad a nivel técnico: Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las oficinas de informática o las que hagan sus veces de las entidades de la administración pública, de acuerdo con los estándares definidos por el ente rector. 4) Interoperabilidad a nivel legal: Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la administración pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia. Como podemos ver, la interoperabilidad entre las entidades públicas, está considerada como un aspecto importante dentro de la Ley de gobierno digital y dicha norma lo considera en el Decreto Legislativo Nº 1412.		

	Seguridad digital	Respecto a la seguridad digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?	La seguridad digital es otro de los aspectos considerados en la Ley de gobierno digital. Dicha ley nos indica que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas. El Marco de seguridad digital del Estado peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública. Respecto a la gestión del marco de seguridad digital del Estado peruano, la Ley de gobierno digital indica los siguientes ámbitos: a. Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa. b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia. c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder	Según el decreto Supremo No 050-2018-PCM la definición de Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes: a) Nota 1: La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas. b) Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital. c) Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego. d) Nota 4: La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.	La seguridad digital es el aspecto de proteccion de la informacion del gobierno digital, sin el se perderian los datos, la informacion y el conocimiento del ciudadano y del Estado y se podrian comprometer con las amenazas y riesgos existentes. La seguridad digital tiene que considerar principios, modelos, politicas, procesos, roles, tecnologias y estandares minimos. Se procura preservar la confidencialidad, disponibilidad e integridad de la informacion. Se requiere de la participacion de actores del sector publico, sector privado y otros que apoyen en la implementacion de controles, acciones y medidas.

			Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia. d. Institucional: Las entidades de la administración pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI) La Norma Técnica Peruana NTP-ISO/IEC 17799 ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Gestión de la Seguridad de la Información (SGSI), al igual que la norma internacional ISO 27001, ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones. Respecto a la articulación de la seguridad digital con la seguridad de la información, El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.		

	Datos para la toma de decisiones	Respecto a los datos para la toma de decisiones, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?	Los datos son los principales elementos que se requieren para tener información. Estos datos son los referentes que se requieren para generar información, mientras mayor cantidad de datos se tenga mejor es el proceso para generar información. Los datos por sí mismo no constituye información, es el procesamiento de estos datos los que nos proporciona la información, con esta informacion se toma las decisiones. La Ley de gobierno digital nos indica en su capítulo V respecto a gobernanza de datos, que los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación. Las entidades de la administración pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante. Estos datos se deben de proteger y cuidar por su importancia para generar información para la mejor toma de decisiones. El artículo 24 de la Ley indica que La Infraestructura Nacional de Datos se define como el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación,	La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, **datos,** seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector tiene las siguientes atribuciones: a) Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital. b) Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital. c) Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital. d) Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital. e) Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales. f) Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales. g) Definir los alcances del marco normativo en materia de gobierno digital. h) Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital. i) Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía	Los datos para la toma de decisiones se requieren de manera masiva, estos datos ayudaran a la mejor toma de decisiones en el gobierno digital. El el Peru, la Presidencia del consejo de ministros a traves de la secretaria de gobierno digital tienen la responsabilidad de procesar, almacenar, comunicar e interpretar los datos de las instituciones publicas y de las personas que utilizan el gobierno digital.

			almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública. Y el articulo 25 indica, El Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.	digital. j) Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda. k) Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales. l) Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.	

	Arquitectura digital	Respecto a la arquitectura digital, ¿Cuál es la implicancia en el gobierno digital del Estado peruano?	La Ley de gobierno digital indica que la arquitectura digital es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital. La misma Ley indica que las tecnologías digitales se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital. La gestión y administración de una adecuada arquitectura digital depende de las propias instituciones del estado, ellas serán las responsables de adquirir, mantener, actualizar y proteger el cumplimiento de las disposiciones de la PCM respecto al gobierno digital.	Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, debiendo para tal efecto: a) Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley. b) Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia. c) Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital. d) Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley. e) Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional. f) Considerar la implementación de pagos a través de canales digitales. g) Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales. h) Garantizar la conservación de las comunicaciones y documentos generados a través	El gobierno digital requiere, para su buen funcionamiento, de una adecuada arquitectura digital. La arquitectura digital no solo es las TICs, tambien estan comprometidas las normas o politicas, los procedimientos, los componentes digitales, los recursos humanos adecuados para su utilizacion y los elementos que interrrelacionados cumplen un fin en comun propio de la institucion publica y de las responsabilidades del gobierno digita.

				de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales. i) Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.	