PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Facultad de Educación

Importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde el sétimo ciclo de la EBR en el Perú.

Tesis para obtener el título profesional de Licenciado en Educación con especialidad en Educación para el Desarrollo que presenta:

Bermúdez Torres, Marco Antonio

Asesor:

LLaullipoma Romani, José Alberto

Lima, 2022

RESÚMEN

Actualmente el Estado peruano se encuentra inmerso, en lo que conocemos como sociedad de la información y sociedad del conocimiento, así mismo, viene propiciando a través de la Secretaría de Gobierno y Transformación Digital que pertenece a la Institución Pública de Perú denominada Presidencia del Consejo de Ministros (PCM), la implementación de la Transformación y Gobierno Digital en el Perú, y como consecuencia de ello viene realizando acciones orientadas a la gestión, implementación, difusión, entre otros de la temática de seguridad digital, seguridad de los datos y de la Información en las Instituciones y organizaciones peruanas, en este contexto el desarrollo de competencias digitales de seguridad desde el sétimo ciclo de la Educación Básica Regular (EBR) es un aspecto crucial en la formación básica ya que contribuirá en generar competencias para los ciudadanos digitales en temas y aspectos básicos pero relacionados con estándares de seguridad digital, seguridad de datos y de la información. Así mismo, tenemos la DigComp 2.2, que plantea 4 competencias digitales del área de seguridad, enmarcadas en lo siguiente: Protección de dispositivos digitales, protección y privacidad de los datos personales, protección de la salud y bienestar de las personas; y, protección del ecosistema medioambiental, las cuales comprenden competencias diversas relacionadas a aspectos de tecnologías que soportan diversas plataformas de información y comunicaciones, así como, de temas de seguridad digital, seguridad de los datos y de la información. En este marco, se requiere conocer cuál sería la importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2 en la EBR del nivel secundario, desde su sétimo ciclo, en el contexto peruano. En este sentido, la presente tesina tiene por objetivos: i) Describir las competencias digitales del área de seguridad del DigComp 2.2, relacionándolas con las competencias digitales del Currículo Nacional de la EBR; y, ii) Analizar la importancia de las competencias digitales del área de seguridad del DigComp 2.2. en la ciudadanía digital y para la seguridad digital, seguridad de los datos y de la información en el contexto peruano. Respecto, a la metodología utilizada, se tiene un enfoque cualitativo, utilizando el método de investigación documental, lo que ha permitido una aproximación y comprensión del

tema, a partir del uso de distintos tipos de fuentes documentales nacionales e internacionales. Se sustenta desarrollar las competencias digitales de seguridad del DigComp 2.2, ya que contribuirían en muchos aspectos de gestión, implementación, difusión, entre otros aspectos de las temáticas de seguridad digital, seguridad de los datos y de la información en las Instituciones públicas y organizaciones privadas, requeridos por el Estado peruano.

Palabras clave: Educación Básica Regular, competencias digitales de seguridad de la DigComp 2.2, ciudadanía digital, seguridad digital, seguridad de los datos y de la información.

ABSTRACT

Currently, the Peruvian State is immersed in what we know as the information society and knowledge society, likewise, it has been promoting through the Secretary of Government and Digital Transformation that belongs to the Public Institution of Peru called the Presidency of the Council of Ministers, the implementation of the Transformation and Digital Government in Peru, and as a consequence of this, it has been carrying out actions aimed at the management, implementation, dissemination, among others, of the subject of data and information security in institutions and organizations. Peruvians, in this context the development of digital security skills from the seventh cycle of Regular Basic Education (EBR) is a crucial aspect in basic training since it will contribute to generating skills for digital citizens in basic issues and aspects but related to security, data and information standards. Likewise, we have the DigComp 2.2, which proposes 4 digital competences in the security area, framed in the following: Protection of digital devices, protection and privacy of personal data, protection of the health and well-being of people; and, protection of the environmental ecosystem, which include various competencies related to aspects of technologies that support various information and communications platforms, as well as data and information security issues. In this framework, it is necessary to know what would be the importance of developing the digital security skills of DigComp 2.2 in the EBR at the secondary level, from its seventh cycle, in the Peruvian context. In this sense, this thesis has the following objectives: i) To describe the digital competences of the DigComp 2.2 security area, relating them to the digital competences of the EBR National Curriculum; and, ii) Analyze the importance of digital skills in the security area of DigComp 2.2. in digital citizenship and for data and information security in the Peruvian context. Regarding the methodology used, there is a qualitative approach, using the documentary research method, which has allowed an approximation and understanding of the subject, based on the use of different types of national and international documentary sources. It is supported to develop the digital security competencies of DigComp 2.2, since they would contribute in many aspects of management, implementation, dissemination, among other aspects of the topics of

digital security, data and information security in public institutions and private organizations, required by the Peruvian State.

Keywords: Regular Basic Education, DigComp 2.2 digital security skills, digital citizenship, digital security, data and information security.

DEDICATORIA

Dedico esta tesina a mis padres Pedro Gandhy (Digital Alien) y Teresa Emperatriz (Digital Inmigrant), a mi hermano Iván Omar y a mi esposa Lilia Marili (ambos Digital Adaptatives); pero especialmente a mi hija Nathalie Abigail (Digital Native) y a mi hijo Esteban Ludwig (Digital Avatar), dos seres extraordinariamente inteligentes inmersos en un uso intenso de tecnología digital como parte de este cambiante ecosistema digital, en un mundo donde la transformación digital con sus vertiginosos cambios disruptivos, les requerirá continuamente adquirir competencias digitales holísticas, para ser ciudadanos digitales plenos que puedan a través de las nuevas tecnologías de información y comunicación aplicarla en beneficio de la sociedad digital.

AGRADECIMIENTO

Un agradecimiento especial a mis asesores por su valioso tiempo, dedicación y apoyo durante este proceso. A la Facultad de Educación de la PUCP por la oportunidad de conseguir este nuevo objetivo académico. Finalmente, a los diferentes profesionales que me brindaron su apoyo con sus conocimientos ya sea de manera directa o a través de sus documentos que me sirvieron como referencias para la presente investigación.

ÍNDICE

Resumen 02

Abstract 04

Introducción 09

1. **Fundamentos de la Educación Básica Regular y de las competencias digitales** 12
   - 1.1. La Educación Básica Regular en el contexto peruano 12
   - 1.2. Competencias clave para el aprendizaje continuo 13
   - 1.3. Modelo conceptual de la DigComp 2.2 17
   - 1.4. Competencias digitales del área de seguridad de la DigComp 2.2 18
2. **Importancia de las competencias digitales del área de seguridad de la DigComp 2.2 en la ciudadanía digital y para la seguridad de la información en el contexto peruano** 21
   - 2.1. El Currículum Nacional de la Educación Básica Regular, las competencias digitales y la ciudadanía digital 22
   - 2.2. Las competencias digitales del área de seguridad de la DigComp 2.2 y el Currículum Nacional de la Educación Básica Regular 26
   - 2.3. Importancia en la ciudadanía digital y para la seguridad de la información 29
3. **Conclusiones** 45
4. **Recomendaciones** 49

Referencias 50

INTRODUCCIÓN

Actualmente la sociedad se encuentra viviendo en lo que conocemos como sociedad de la información y sociedad del conocimiento, cada día las diversas Instituciones y organizaciones peruanas trabajan con entornos digitales donde, la globalización y la innovación tecnológica tienen mucha influencia en sus actividades, generándose la necesidad de contar con nuevas habilidades que permitan integrar la cultura digital, siendo las competencias digitales un factor crítico para sobrevivir en este nuevo ecosistema digital, al mismo tiempo, en el caso peruano como se comentó anteriormente nos encontramos en un proceso de transformación digital y en el marco de la implementación de un gobierno digital.

Por otro lado, tenemos la DigComp 2.2, que hace referencia a diversas competencias clave, dentro de las cuales brinda un marco de 21 competencias digitales para la ciudadanía, dentro de las mismas presenta 4 competencias digitales del área de seguridad, enmarcadas en lo siguiente: Protección de dispositivos digitales, protección y privacidad de los datos personales, protección de la salud y bienestar de las personas; y, protección del ecosistema medioambiental. Estas competencias digitales del área de seguridad, comprenden competencias diversas, incluyendo competencias sobre el bienestar digital y sobre ciberseguridad, las cuales son transversales a diversos aspectos actuales que son necesarias para gestionar las tecnologías que soportan los aspectos informáticos, de información, comunicaciones, entre otros; así como, temas de seguridad digital, seguridad de datos y de la información.

Considerando este preámbulo, a través del presente trabajo, se busca conocer cuál sería la importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2 desde el sétimo ciclo en la EBR del nivel secundario en el contexto peruano. En este sentido, la presente investigación tiene por objetivos: i) Describir las competencias digitales del área de seguridad del DigComp 2.2, relacionándolas con las competencias digitales del Currículo Nacional de la EBR; y, ii) Analizar la importancia de las competencias digitales del área de seguridad del DigComp 2.2. en la ciudadanía digital y para la seguridad digital, seguridad de datos y seguridad de la información en el contexto peruano.

Se considero cómo metodología, el enfoque u orientación cualitativa, utilizando el método de investigación documental, lo que ha permitido una aproximación y comprensión de la temática estudiada, se sustentó a través del uso de distintos tipos de fuentes documentales nacionales e internacionales, en formato digital. Se realizó un análisis de documentos nacionales e internacionales, incluyendo artículos académicos, normas técnicas peruanas y estándares internacionales. Cabe precisar, que Revilla (2020), sostiene que para la investigación cualitativa se utiliza principalmente el método de investigación documental, el cual ayuda a que el investigador logre un acercamiento indirecto a la realidad estudiada, considerando fuentes secundarias accediéndose a su contenido sin cambiarlos o modificarlos.

Así mismo, de acuerdo al Reglamento que presenta el Comité de Ética de la Investigación de la Pontificia Universidad Católica del Perú (2011), se toman en cuenta los principios éticos de integridad científica, considerando que el presente trabajo de investigación fue elaborado íntegramente por el investigador, así mismo, que el análisis fue comunicado progresivamente durante el presente trabajo. Por otro lado, se trabajó con rigor académico respetando la autoría de los documentos utilizados, para lo cual se hizo uso del estilo de redacción APA 7ª.

La línea o área de investigación, está referida al tema de las competencias digitales en la educación básica, la cual se enmarca en el área de investigación de TIC y Educación. La presente investigación se estructura en dos capítulos, además de las conclusiones y referencias. En el primer capítulo se explica la organización, conceptos, niveles y ciclos de la EBR en el contexto peruano, así mismo, considera opiniones y conceptos relacionados a competencias digitales realizados por instituciones nacionales e internacionales, principalmente considerando lo propuesto en el Marco de Competencias Digitales para la Ciudadanía (DigComp 2.2). El segundo capítulo comprende: el currículum nacional peruano y su relación con las competencias digitales, posteriormente para ir bajando de nivel se trata el tema de las competencias digitales del área de seguridad de la DigComp y su relación con el currículum nacional de la EBR, a continuación se toca el tema de la importancia de desarrollar las competencias digitales del área de seguridad de la DigComp 2.2 desde el sétimo ciclo de la EBR, y por último se analiza sobre la importancia de estas competencias en la ciudadanía digital y su importancia de estas en la temática de

seguridad digital, seguridad de los datos y de la Información en el contexto peruano, considerando como parte del presente análisis algunas normas legales, normas técnicas peruanas y estándares internacionales aplicables referidos a transformación digital, seguridad digital, seguridad de datos y seguridad de la información.

Como resultado de este trabajo, se sustenta la relevancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde el sétimo nivel de la EBR, considerando que las citadas competencias digitales, contribuirían en muchos aspectos de seguridad digital, seguridad de los datos y de la información requeridos por el Estado peruano, como parte del proceso de transformación digital y en el marco de la implementación del gobierno digital en el cual se encuentra.

Así mismo, permitirá que los estudiantes de la EBR adquieran nuevas competencias diferentes a las tradicionales, que les permita ser más versátiles teniendo competencias digitales de seguridad que vayan más allá de las que les brinda actualmente el Currículo Nacional de la EBR, en este sentido desarrollar dichas competencias contribuiría con las competencias digitales requeridas por los ciudadanos digitales ante los cambios requeridos por las tecnologías que soportan diversas plataformas de información y comunicaciones.

CAPÍTULO 01

1. Fundamentos de la Educación Básica Regular y de las competencias digitales

Primero es necesario entender que actualmente la sociedad peruana se encuentra inmersa en lo que conocemos como sociedad de la información y sociedad del conocimiento, así mismo, nos encontramos en una época en la cual seguirán presentándose muchos cambios tecnológicos, formando parte el Perú de esta época de constantes cambios propiciados por el desarrollo tecnológico y el proceso de transformación digital en el marco de la implementación de un gobierno digital.

De acuerdo a lo explicado anteriormente, es necesario reemplazar los antiguos estándares educativos que son usados actualmente, los mismos, que combinan la adquisición de conocimientos tradicionales, por lo que ahora se debe enseñar habilidades y competencias además del conocimiento, con un enfoque en la metacognición, que incluya “aprender a aprender”, considerando que no podemos predecir las nuevas tecnologías del futuro, por lo que tenemos que aprender como sociedad a ser versátiles (Taguma y Lim, 2018).

En este marco, el capítulo 01 explica la organización, conceptos, niveles y ciclos de la Educación Básica Regular en el contexto peruano, así mismo, considera opiniones y conceptos relacionados a competencias digitales realizados por instituciones nacionales e internacionales, principalmente considerando lo propuesto en el Marco de Competencias Digitales para la Ciudadanía denominadas DigComp 2.2 (Vuorikari, 2022).

1.1. La Educación Básica Regular en el contexto peruano

En el Perú, la Ley General de Educación (Ley N°28044), en su Artículo 31°, literal c), hace mención que uno de los objetivos de la Educación Básica es desarrollar aprendizajes en varios campos de estudios, entre ellos menciona las ciencias, las humanidades, la técnica, la cultura y el arte, abarcando también los

estudios que contribuyan con el buen uso de las nuevas tecnologías, así mismo, en su Artículo 32º explica que la Educación Básica se organiza en: a) Educación Básica Regular, b) Educación Básica Alternativa, y c) Educación Básica Especial. Al respecto, en su Artículo 36º explica que la Educación Básica Regular involucra los niveles o escalas de Educación Inicial, Educación Primaria y Educación Secundaria, respecto a este último su literal c) plantea que la Educación Secundaria involucra su 3er nivel, con una duración de cinco años, y está orientada al desarrollo o adquisición de competencias en los alumnos que permitan acceder a conocimientos humanísticos, científicos y tecnológicos en permanente cambio, formando a los estudiantes para la vida, el trabajo y el ejercicio de la ciudadanía (Ministerio de Educación [MINEDU], 2003).

Por otro lado, el Reglamento de la Ley N° 28044, en su Artículo 50º brinda un mayor alcance sobre la Educación Básica Regular, dando a conocer que cuenta con un enfoque intercultural e inclusivo, así mismo, en su literal d) manifiesta que busca promover en los estudiantes el fortalecimiento de las competencias y la apropiación de nuevas tecnologías que les permitan la construcción permanente del conocimiento. En cuanto a su organización en su Artículo 70º describe que comprende cinco grados y se organiza en dos ciclos, siendo estos el sexto y el sétimo ciclo, por último, en su literal b) describe que en el sétimo ciclo de la Educación Básica Regular se profundiza la formación científica y tecnológica, promoviendo la construcción de conocimientos, la innovación e investigación para alcanzar aprendizajes complejos y continuar estudios superiores (MINEDU, 2012).

Es importante precisar que el alcance del presente análisis se enfoca en el sétimo ciclo o etapa de la Educación Básica Regular en el Perú y comprende los tres últimos grados de la Educación Secundaria, los mismos que se desarrollan en los tres últimos años de estudios.

1.2. Competencias clave para el aprendizaje continuo

Las competencias denominadas clave contribuyen en su conjunto de manera integral en la sociedad del conocimiento, considerando que estas en su

mayoría están interrelacionadas es decir que aspectos de una competencia clave apoyan otras competencias, las más básicas por ejemplo como lenguaje, comprensión lectora, buena escritura, matemáticas y cálculo; y, aspectos de tecnologías que soportan diversas plataformas de información y comunicaciones son el soporte del proceso de aprender continuamente, en el cual están inmersos los estudiantes, pero todas ellas se sustentan en la capacidad de poder aprender (por siempre) a aprender (European Comission, 2007). Entender primero el rol de las competencias llamadas clave en el proceso de aprendizaje continuo en la sociedad permite identificar su importancia en desarrollar estas capacidades en los estudiantes, de manera complementaria, así mismo, el pensamiento creativo, el desarrollo de servicios innovadores y de nuevas formas de trabajar, crear nuevos procesos, nuevos paradigmas de negocios y en general formas diferentes de pensar y vivir, son aspectos a considerar para el año 2030, los aspectos en que se basan estas nuevas competencias incluyen la adaptabilidad, la creatividad, la curiosidad y la mentalidad abierta (OECD, 2018). Para lograr que los estudiantes logren estos aspectos se debe orientar su educación a desarrollar nuevas competencias, por lo que es bueno precisar que según la European Comission cuando hablamos de competencias debemos entenderlas como la unión de diversos tipos de conocimientos, competencias, capacidades, aptitudes y actitudes, las mismas que están acondicionadas a un contexto específico. Estas competencias nombradas como clave son necesarias por la sociedad y las personas, ya que les son útiles para su realización, crecimiento, inserción social y desarrollo integral, así como para participar activamente de las actividades como ciudadano, permitiéndole su inclusión social y acceso a un trabajo (European Comission, 2007).

A su vez, el Currículo Nacional de Educación Básica entiende la competencia de la forma que pueden las personas combinar o agrupar diversas capacidades que le permitirán brindar soluciones a ciertos problemas, considerando que se deben tomar decisiones con pertinencia y ética (MINEDU, 2016).

Para lo cual se requieren identificar y desarrollar competencias clave que les permita a los alumnos del sétimo ciclo de la EBR un aprendizaje complejo,

continuo y contribuir con su realización personal de manera íntegra. Al respecto, Vuorikari (2022), señala: “La recomendación sobre las competencias clave para el aprendizaje permanente identifica las competencias clave que son esenciales para la ciudadanía para su realización personal, un estilo de vida saludable y sostenible, la empleabilidad, la ciudadanía activa y la inclusión social” (p. 6). La competencia digital, es considerada como competencia clave por varios autores, por ejemplo, la European Comission desde el año 2007 establece ocho competencias denominadas clave, las cuales no cambiaron a la fecha y fueron validadas en el año 2020 por la misma organización, dichas competencias se enmarcan en los siguientes aspectos: 1. Habilidades de comunicación en su lengua madre, 2. Habilidades de comunicación en lenguas foráneas o extranjeras, 3. Habilidades de competencia en ciencia básica, tecnología, matemáticas, cálculo, etc. 4. Habilidades de competencias digitales, 5. Lograr el aprendizaje permanente es decir poder aprender a aprender, 6. Habilidades de competencias de desenvolvimiento social y con valores cívicos, 7. Habilidades de liderazgo y con iniciativas empresariales, y 8. Lograr conciencia de temáticas culturales (European Comission, 2020).

Por otro lado, González-Fernández-Villavicencio (2015), señala que “La competencia digital se considera por tanto clave y se evidencia su adquisición incorporando el dominio de las nuevas tecnologías, la seguridad en la red y la valoración crítica de su impacto en la sociedad” (p. 31). Lo expuesto muestra como una competencia clave las competencias digitales, las mismas que de acuerdo al plan que contempla las acciones de educación digital de la Comisión Europea de enero del año 2018, debemos entenderlas como el uso seguro e importante de la tecnología digital, dirigida a la necesidad de estimular, respaldar e incrementar el uso correcto de buenas prácticas de educación digital, considerando temáticas innovadoras, siendo sus dos principales temas a considerar: 1) hacer un uso mejor de la tecnología digital para la enseñanza y el aprendizaje; y 2) desarrollar competencias y capacidades digitales pertinentes para la transformación digital (Agencia Ejecutiva Europea de Educación y Cultura [Eurydice], 2019).

Cabe precisar, que el segundo tema referido a desarrollar competencias y capacidades digitales pertinentes para la transformación digital, involucra transversalmente muchos temas de seguridad digital necesarios en la sociedad actual y en la Educación Básica Regular. En este contexto Gisbert y Esteve (como se citó en Muñoz-Repiso y Verónica, 2020) plantean que la competencia digital es la adición de muchas habilidades, experiencias, conocimientos, aptitudes y actitudes, en los rubros de las nuevas tecnologías, aspectos de comunicación e información y tecnología multimedia, propiciando una alfabetización holística y compleja.

Tenemos también que el aprendizaje continuo considera algunas competencias clave principales para la ciudadanía enfocándose en su realización personal, en mejorar su estilo de vida saludable y sostenible, así como, los aspectos de la empleabilidad, la ciudadanía activa y la inclusión social (Vuorikari, 2022). Estas competencias claves citadas en la DigComp 2.2 son las siguientes: 1) Ciencia, tecnología, ingeniería, matemáticas, 2) Lenguajes, 3) Alfabetización, 4) Conciencia y expresión cultural, 5) Emprendimiento, 6) Competencia civil, 7) Personales, sociales y aprender a aprender; y 8) Competencias digitales. Esta última competencia, está estructurada y enmarcada en las cinco áreas o espacios de competencia digital siguientes: Búsqueda y gestión de información y datos; Aspectos comunicativos y de colaboración; Contenidos y su creación en entornos digitales; Seguridad digital, seguridad de datos e información; y poder resolver problemas (Vuorikari, 2022).

De las cuales, nos centraremos en la competencia digital de seguridad, así mismo, hay que tener en cuenta que la formación en la educación básica regular de esta competencia ayudará a que los estudiantes y en general los ciudadanos adquieran esta competencia clave y se adapten a los cambios vigentes, en el marco del proceso de transformación digital y gobierno digital en la cual se encuentra inmerso el estado peruano. En general las competencias clave tienen una doble función, tanto social como económica, donde la educación desempeña un rol crucial para impulsar que los ciudadanos las adquieran y se adapten a los cambios actuales (European Comission, 2007).

1.3. Modelo conceptual de la DigComp 2.2

La DigComp 2.2 hace referencia al Marco de Competencias Digitales para la Ciudadanía, según Vuorikari (2022):

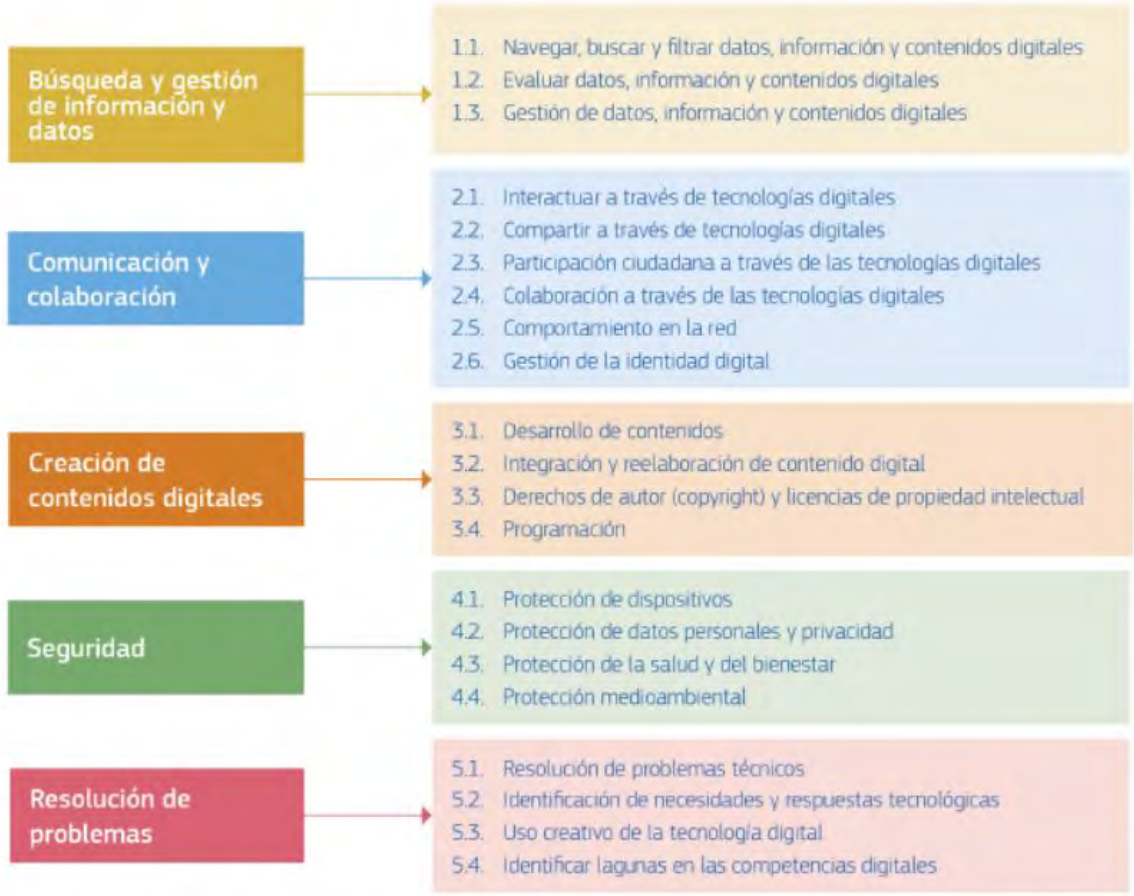
> (…) proporciona un lenguaje común para identificar y describir las áreas clave de las competencias digitales. Se trata de una herramienta a escala de la UE para mejorar la competencia digital de la ciudadanía, ayudar a los responsables políticos a formular políticas que apoyen el desarrollo de la competencia digital y planificar iniciativas de educación y formación para mejorar las competencias digitales de grupos específicos. (p. 2)

Lo descrito anteriormente, se relaciona a la educación digital, la cual contempla dos perspectivas, por un lado, el desarrollo de competencias digitales por parte de los alumnos y profesores; y por otro ángulo el uso pedagógico de las nuevas tecnologías en entornos digitales para mejorar los aprendizajes de los alumnos, la enseñanza y la evaluación, así mismo es bueno indicar que la mayoría de los países europeos cuentan con estrategias nacionales relacionadas a educación digital orientadas a que los estudiantes desarrollen sus destrezas digitales, entre otros aspectos. Otro factor importante, es la actual perspectiva del mercado laboral que exige altos niveles de destrezas digitales, por lo que la educación digital considera un reto el desarrollo y mejora de las competencias digitales en los alumnos (Eurydice, 2019).

La DigComp 2.2 con su actualización 2.2 no cambia los enunciados de las competencias ni sus descriptores del modelo conceptual de la DigComp, solo adiciona ejemplos de conocimientos, habilidades y actitudes aplicables a cada una de sus 21 competencias digitales; el modelo conceptual se presenta en la figura siguiente:

Figura 1

Modelo de referencia conceptual de la DigComp



Nota. La figura muestra las 5 áreas de competencia y las 21 competencias digitales del Modelo de referencia conceptual de la DigComp. Fuente: Vuorikari (2022).

1.4. Competencias digitales del área de seguridad de la DigComp 2.2

Las competencias digitales del área de la competencia de seguridad, comprenden competencias diversas, incluyendo competencias sobre el bienestar digital y sobre ciberseguridad, las cuales son transversales a diversos temas que soportan las plataformas de información y comunicaciones.

Cabe precisar, que la competencia digital alberga el uso seguro, vital o crítico y responsable de las tecnologías digitales para un entorno de aprendizaje, ya sea en el trabajo o en su rol en la sociedad, también incluye la interacción bidireccional con estas tecnologías. Esta concepción considera la búsqueda y gestión de información y datos, la comunicación y la colaboración, la creación e

innovación de contenidos o repositorios digitales (incluyendo criterios de programación), la seguridad digital, seguridad de datos e información (comprendiendo el bienestar o salud digital y las competencias direccionadas con la ciberseguridad y seguridad informática); así como la capacidad de entender y poder resolver problemas (Vuorikari, 2022).

En cuanto, al área de competencia de seguridad, está formada por cuatro competencias digitales, que de acuerdo a Vuorikari (2022) comprenden:

Protección de dispositivos:

- Proteger los dispositivos y los contenidos digitales, y comprender los riesgos y las amenazas en los entornos digitales.
- Conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad.

Protección de datos personales y privacidad

- Proteger los datos personales y la privacidad en los entornos digitales.
- Entender cómo utilizar y compartir la información personal identificable, siendo capaz de protegerse a sí mismo y a los demás de los daños.
- Entender que los servicios digitales utilizan una “política de privacidad” para informar sobre el uso de los datos personales.

Protección de la salud y del bienestar digital

- Capacidades a la hora de evitar riesgos para la salud tanto física como mental en el uso de las tecnologías digitales.
- Capacidad a la hora de protegerse uno mismo y a otros ante los riesgos de los entornos digitales (por ejemplo: cyberbullying).

Protección medioambiental

- Ser consciente del impacto de las tecnologías digitales y su uso. (pp. 35-41)

En relación, con lo descrito anteriormente la educación tiene un rol fundamental en proporcionar a las personas, las habilidades, conocimientos y actitudes necesarias para prosperar en sus vidas a nivel personal y profesional. Considerando que el mundo está cada vez más digitalizado, el sistema educativo debe adaptarse y evolucionar para aprovechar las herramientas y las fortalezas de las nuevas tecnologías, al tiempo que aborda las inquietudes sobre posibles abusos, como el fraude, el robo de identidad o el ciberacoso (OECD, 2019). En el sentido relacionado a que las personas son actores cruciales en el proceso educativo, el actual Proyecto Educativo Nacional (PEN 2036) (Consejo de Educación [CNE] 2020) expresa:

> La acción educativa debe ser concebida desde las personas, reconociendo la centralidad del aprendizaje en función de sus necesidades, características y aspiraciones, y que este se suscita en diversos contextos y a lo largo de la vida, produciéndose diferentes trayectorias que deben ser reconocidas y fortalecidas, poniendo el sistema educativo y su operación al servicio de esta finalidad. (p. 27)

CAPÍTULO 02

2. Importancia de las competencias digitales del área de seguridad de la DigComp 2.2 en la ciudadanía digital y para la seguridad de la información en el contexto peruano

Las competencias digitales de seguridad, que propone el modelo DigCom comprenden las temáticas de: protección de dispositivos digitales, protección de datos personales y privacidad de datos, protección de la salud y del bienestar digital; y protección medioambiental por el impacto de las tecnologías. Estas competencias juegan un rol vital en los procesos actuales de gestión de la seguridad digital, seguridad de datos e información y ciberseguridad en las organizaciones públicas y privadas de la sociedad peruana, por lo que dichas competencias y capacidades digitales de seguridad son importantes desarrollar en los estudiantes, ya que se encuentran enmarcadas en los estándares internacionales de gestión de seguridad digital, seguridad de datos e información, que son aplicables al contexto peruano como parte del proceso de transformación digital e implementación de un gobierno digital en que la sociedad peruana se encuentra inmersa, lo señalado anteriormente permitirá brindar nuevas opciones a los estudiantes y ciudadanos en general pero más aún a los ciudadanos digitales.

En este sentido, las capacidades se entienden como recursos para que los estudiantes actúen de manera competente, los mismos que se refieren a los conocimientos, experiencias, habilidades, aptitudes y actitudes que los alumnos utilizarán para lograr solucionar problemas. A su vez, dichas capacidades involucran actividades u operaciones simples comprendidas en las competencias, que son actividades u operaciones de mayor complejidad (MINEDU, 2016).

En este contexto, el capítulo 02 comprende: el currículum nacional peruano y su relación con las competencias digitales, posteriormente para ir bajando de nivel se trata el tema de las competencias digitales del área de seguridad de la DigComp y su relación con el currículum nacional de la EBR, a

continuación se toca el tema de la importancia de desarrollar las competencias digitales del área de seguridad de la DigComp 2.2 desde el sétimo ciclo de la EBR, y por último se analiza sobre la importancia de estas competencias en la ciudadanía digital y para la seguridad de la información en el contexto peruano.

2.1. El Currículum Nacional de la Educación Básica Regular, las competencias digitales y la ciudadanía digital

El Ministerio de Educación publicó en el año 2016, la versión vigente del Currículo Nacional de Educación Básica, que actualmente es de uso obligatorio en el Estado peruano, para el cual, los valores, la ética, la educación cívica y ciudadana de los alumnos son un aspecto fundamental, que servirá posteriormente para viabilizar en la sociedad tanto sus derechos y deberes como ciudadanos, así mismo, el desarrollo y mejora de sus competencias les permitan atender e insertarse ante las actividades actuales de diversos temas en el entorno mundial tan cambiante, estando entre una de ellas las actividades que soportan diversas plataformas de información y comunicaciones, estando por consecuencia muchos aspectos de seguridad digital, seguridad de datos e información relacionados; por otro lado, reconoce que vivimos en una época inmersa en una transformación fundamental del trabajo, y ante la incertidumbre de nuevas destrezas aplicables al siglo XXI, cuya consecuencia es que el ámbito del conocimiento vive y vivirá un futuro de agitación y renovación permanente, hecho muy ligado al avance de la tecnología y, por supuesto, por la masificación de las tecnologías en entornos digitales, así mismo, hay que considerar que el uso masivo de estas tecnologías y la conexión en tiempo real usando Internet, nos presenta un mundo diverso, en el cual cultura digital y la ciudadanía digital requieren ciudadanos formados que puedan desenvolverse exitosamente en un futuro de cambios profundos y constantes (MINEDU, 2016).

De manera complementaria a lo indicado, anteriormente en cuanto al perfil de egreso de la Educación Básica el Ministerio de Educación plantea que los estudiantes se orienten a poder de una manera ética y responsable hacer un uso correcto de las tecnologías que soportan diversas plataformas de información y comunicaciones, interacción que permitirá al alumno a conseguir datos,

información, construir conocimientos, gestionar su proceso de aprendizaje y lograr afianzar su comunicación en su entorno. También propone que el estudiante tenga la capacidad de depurar y sistematizar información de forma interactiva; a su vez que pueda crear y modificar materiales digitales lo que le permitirá afianzar su proceso comunicativo; logrará respecto a las aplicaciones informáticas poder escoger las que requiera, poder instalarlas y usarlas de acuerdo a sus requerimientos y su entorno. Podrá escoger que interfaces usar y como conseguirlas de acuerdo a sus necesidades o de su entorno social. También se señala que tendrá la capacidad de participar e interactuar con responsabilidad en diversas redes sociales y ecosistemas virtuales, a través de comunicaciones bidireccionales enmarcados en proyectos colaborativos. Adicionalmente, logra las actividades nombradas mediante la capacidad de autorregulación de sus actos (MINEDU, 2016).

Así mismo, el Currículo Nacional de Educación Básica peruano vigente, considera 29 competencias nacionales que los estudiantes deben adquirir y desarrollar, este documento incluye sus niveles esperados por ciclo, nivel y modalidad, a su vez, muestra un enfoque transversal inspirado en principios educativos, como la conciencia ambiental, la democracia, la igualdad de género, entre otros (MINEDU, 2016).

En el citado documento el MINEDU en su competencia 28, plantea para su competencia digital que el alumno logre entender, conceptualizar, interpretar, y por lo tanto hacer cambios y mejoras a los entornos virtuales que formen parte de su desarrollo y proceso en sus actividades de aprendizaje, así como, en actividades sociales en este entorno. Lo señalado, considera el ensamblaje de diversos procesos como recopilación, selección o disgregación y evaluación de datos e información; también se considera aspectos de modificación, innovación y creación de materiales digitales, materiales comunicacionales, que permitan que los alumnos puedan tener un rol participativo e, comunidades virtuales, por último, se considera que los alumnos sepan adaptarse a entornos nuevos en función de cómo lo vayan requiriendo para un adecuado comportamiento social (MINEDU, 2016).

Por otro lado, respecto a las competencias digitales y la ciudadanía digital, actualmente los procesos de digitalización de la información se vienen dando de manera intensa en todo tipo de organizaciones, este cambio profundo genera nuevos paradigmas cualitativos y cuantitativos en nuevos entornos y ecosistemas digitales, los mismos que engloban lo involucrado con la temática de competencias digitales (Levano et al., 2019). Las competencias digitales se refieren al adecuado uso de las tecnologías que soportan diversas plataformas de información y comunicaciones desde una perspectiva integral en las tareas de la vida de los ciudadanos.

Sobre este concepto para un mayor alcance, puede entenderse en el sentido que la competencia digital por su naturaleza intrínseca requiere un uso seguro de los datos e información, este uso seguro es un criterio importante a considerar para las tecnologías que soportan diversas plataformas de información y comunicaciones, también para el trabajo diario en estos entornos digitales y para actividades recreativas y comunicativas en estos entornos digitales. Lo citado, tienen como sustento que las competencias básicas en materia de nuevas tecnologías como, por ejemplo: el uso de computadoras, laptops u otro dispositivo para recopilar, analizar, resguardar o almacenar, crear o producir, divulgar o presentar e intercambiar datos e información, y por último comunicarse y ser participe activo en redes sociales de colaboración a través de Internet (European Comission, 2007).

En este marco, las competencias digitales y la ciudadanía digital deben entenderse como conceptos relacionados entre sí, un punto a considerar es que para lograr ser ciudadanos digitales se requiere que los ciudadanos cuenten con competencias digitales, en este sentido Bustamante (2021) explica:

> La formación de la ciudadanía digital será el resultado de una intencionalidad que debe plantearse claramente desde las políticas educativas en conjunto con diversos sectores de la sociedad, a quienes esta responsabilidad atañe de modo más directo. Así, educar para una ciudadanía plena implica que, desde la educación, se trabaje de manera conjunta con otros

> sectores de la sociedad para potenciar el desarrollo de la ciudadanía digital en todos los peruanos. (p. 92)

En cuanto a las competencias digitales, los conocimientos, capacidades y actitudes esenciales, requieren comprender conocimientos sobre las TSI y que sean aplicables a la vida diaria ya sea privada y laboral, en consecuencia, se necesita conocimiento actualizado de las TIC y de temas de seguridad de la información, los estudiantes deben comprender sobre las oportunidades que ofrecen las TIC en la creatividad e innovación en su desarrollo profesional, considerando los principios legales y éticos (European Comission, 2007). En este sentido, la ciudanía digital requiere un trabajo integral desde la perspectiva educativa y desde las políticas nacionales, por este motivo es que se plantea que el desarrollo de competencias digitales, específicamente las competencias digitales de seguridad del DigComp 2.2, deben propiciarse en los estudiantes peruanos desde el sétimo ciclo de la EBR.

Al respecto, Bustamante (2021), señala:

> En vista de que la ciudadanía plena empieza a señalarse como una dimensión nueva la de la ciudadanía digital, es necesario pensar y considerar cómo se puede preparar a los ciudadanos del presente y del futuro próximo para que lleguen a ejercerla a cabalidad. Este es un ejercicio que corresponde inicialmente a la academia, pero también a quienes diseñan las políticas de la educación nacional. (p. 92)

A su vez, para la DigComp, la competencia de ciudadanía se entiende como la capacidad de los ciudadanos de poder participar en la vida cívica y social, existiendo una interconexión complementaria entre los conocimientos, habilidades y actitudes de las competencias digitales y la ciudadanía digital (Vuorikari, 2022). Esta aplicación de las competencias digitales por parte de los ciudadanos en su vida diaria y en situaciones reales requiere sea concebida desde la EBR.

En este sentido, respecto al currículo nacional de la educación básica peruana, cabe señalar que este documento inserta una mirada desde las competencias, esto con el objetivo de agrupar los conceptos y contenidos, buscando entorno a casos o situaciones de descripciones reales brindarles un contexto. También se especifica y busca normalizar o estandarizar aprendizajes buscando adaptarlos a cada contexto y que conversen con las capacidades que los alumnos necesiten para resolver problemas en su vida diaria (Mateus y Suárez-Guerrero, 2017).

Respecto a las capacidades necesarias de las competencias digitales, están comprenden buscar, recopilar u obtener; y, tratar analíticamente la información, considerando los riesgos de seguridad digital, seguridad de los datos e información, los estudiantes deben ser capaces de utilizar las tecnologías que soportan diversas plataformas de información y comunicaciones, también de poder crear, mostrar; y, entender y procesar mentalmente información compleja, para luego lograr acceder y usar servicios digitales a través de Internet (European Comission, 2007).

2.2. Las competencias digitales del área de seguridad de la DigComp 2.2 y el Curriculum Nacional de la Educación Básica Regular

Así mismo, a través del Currículo Nacional, el Perú incide en promover el pensamiento complejo, temática necesaria para las competencias digitales ya que permitirá que los estudiantes observen el mundo holísticamente y no desde una perspectiva individualizada, este pensamiento como un sistema interrelacionado requiere entender la complejidad de la realidad a través de sus competencias digitales (MINEDU, 2016). Esta perspectiva del Ministerio se alinea con lo requerido por las competencias digitales de seguridad que propone la DigCom que tiene un planteamiento desde diversas dimensiones; lo cual puede apreciarse en el detalle del área de competencia de seguridad del modelo de referencia conceptual de la DigComp, que está formada por las cuatro competencias digitales siguientes. Primero, tenemos a la **protección de dispositivos**, que contempla la protección de los dispositivos y los contenidos digitales, así mismo busca comprender los riesgos y las amenazas en los

entornos digitales; esta competencia también se orienta a conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad. En segundo lugar, se propone la **protección de datos personales y privacidad**, que considera proteger los datos personales y la privacidad en los entornos digitales; así como, entender cómo utilizar y compartir la información personal identificable, siendo capaz de protegerse a sí mismo y a los demás de los daños; esta competencia también busca entender que los servicios digitales utilizan una "política de privacidad" para informar sobre el uso de los datos personales. En tercer lugar, trata sobre la **protección de la salud y del bienestar**, que incluye las capacidades a la hora de evitar riesgos para la salud tanto física como mental en el uso de las tecnologías digitales; y la capacidad a la hora de protegerse uno mismo y a otros ante los riesgos de los entornos digitales. Y, por último, tenemos a la **protección medioambiental**, competencia que apunta a que los estudiantes sean conscientes del impacto de las tecnologías digitales y su uso (Vuorikari, 2022). En este sentido, el PEN 2036, refiere que se requiere el uso amplio y constante de las tecnologías digitales como recursos educativos que permitan contribuir las labores de enseñanza-aprendizaje, para mejorar el progreso de cada persona que aprende (CNE, 2020).

Por otro lado, como se citó anteriormente para el MINEDU su competencia 28, plantea para su competencia digital diversos temas interesantes, primero cita que los alumnos puedan comprender, conceptualizar, analizar e interpretar, y por lo tanto lograr mejoras y cambios significativos en los entornos virtuales que forma parte y que comprenden su desarrollo y proceso en sus actividades de aprendizaje, así mismo, en actividades y grupos sociales en este entorno digital. Lo que se explicó en el párrafo precedente, ayuda a lograr que diversos procesos como la recopilación, selección o disgregación y evaluación de datos e información puedan funcionar integrados; otro aspecto importante, es que se menciona criterios de modificación, innovación y creación de materiales digitales, materiales comunicacionales, que dirigidos a que los estudiantes participen en interactúen en comunidades virtuales, finalmente, los alumnos deberían tener competencias de adaptación a entornos diferentes en función de cómo lo vayan requiriendo para un adecuado comportamiento social (MINEDU, 2016).

Dicha competencia, se orienta a que el estudiante, **se desenvuelve o desempaña sus actividades en los entornos virtuales originados por las tecnologías que soportan diversas plataformas de información y comunicaciones, estas actividades las realiza con responsabilidad y ética**, esta competencia se enmarca en los cuatro aspectos siguientes: El alumno podrá personalizar los entornos virtuales en los que se desenvuelve, gestionará datos e información de los entornos virtuales, logrará interactuar en los citados entornos virtuales, y por último tiene la capacidad de idear y crea diferentes tipos de objetos virtuales usando formatos variados (MINEDU, 2016).

Al respecto, el MINEDU, se refiere a que estos aspectos requieren la combinación por parte del estudiante de las siguientes capacidades: Primero, en lo concerniente a que el alumno podrá personalizar los entornos virtuales en los que se desenvuelve, lo cual involucra que el alumno de forma sistemática y ordenada logre para diversos entornos virtuales, crearlos a medida seleccionándolos, siempre considerando los principios éticos, la cultura y los valores. En segundo lugar, en cuanto a que gestionará datos e información de los entornos virtuales, está relacionado con analizar, estructurar, organizar y sistematizar datos e información accesible en los entornos virtuales, para lo cual hay que considerar tomando en cuenta su importancia, los variados procedimientos y formatos digitales. En tercer lugar, en relación a que el alumno logrará interactuar en los citados entornos virtuales, se considera la participación del alumno en otros en espacios o entornos virtuales colaborativos, esta participación que comprende su comunicación, establecimiento y creación de lazos de nuevos vínculos sociales se de en un contexto social seguro considerando los principios éticos, la cultura y los valores. Por último, lo señalado a que tiene la capacidad de idear y crea diferentes tipos de objetos virtuales usando formatos variados, consiste en que, como parte de un proceso iterativo de mejora continua en el marco de sus necesidades y su vida cotidiana, el estudiante pueda crear, construir, idear nuevos materiales para entornos digitales, los mismos, que pueden tener varios propósitos (MINEDU, 2016).

De manera complementaria a lo detallado en los párrafos precedentes, el PEN 2036 recoge en su Cuadro 30 denominado: “Tecnología, información e

interconexión de datos para que la política pública vea a las personas y no solo procesos desde quien presta el servicio", varios aspectos relacionados y que muestran la importancia de las competencias digitales del área de seguridad de la DigComp 2.2 en la educación básica regular, entre los más relevantes tenemos que se citan las nuevas tecnologías digitales, el almacenamiento y procesamiento de grandes cantidades de información, la computación en la nube, el aumento del ancho de banda para transmitir datos, los flujos de información generados por tecnologías digitales, entre otros temas, como parte de las tendencias de la transformación digital que atravesamos como sociedad, en las cuales las competencias de seguridad ya citadas juegan un rol vital (CNE, 2020).

2.3. Importancia en la ciudadanía digital y para la seguridad de la información

Las competencias digitales de seguridad del DigComp 2.2, descritas anteriormente son importantes para la ciudadanía digital y deben desarrollarse desde el sétimo ciclo de la educación básica regular por muchos motivos, al respecto la National Institute of Standards and Technology (NIST) explica que, el entrenamiento en temas de seguridad digital, seguridad de datos e información, está orientado a desarrollar habilidades que permitan a una persona a realizar actividades específicas, habilidades que se construyen usando conceptos, teorías y buenas prácticas de seguridad digital, seguridad de datos e información (NIST, 2015). Las citadas buenas prácticas de seguridad digital, seguridad de datos e información, se basan en estándares internacionales usados a nivel mundial por todas las organizaciones por lo que comprenden básicamente todos los temas de seguridad citados por la DigComp.

También tenemos el Convenio de Budapest o convenio sobre la ciberdelincuencia, que presenta la importancia para la ciudadanía digital de ser competentes en temas de seguridad, este convenio es un instrumento internacional que trata aspectos de ciberseguridad, contemplando de manera general: (i) actividades que tienen como objetivo los sistemas informáticos y sus datos; (ii) la falsificación informática; (iii) los fraudes informáticos; (iv) el uso de

la tecnología computacional para la creación, distribución y procesamiento de pornografía infantil; y (v) el uso de la tecnología computacional para infringir reglas sobre la propiedad intelectual. Por otro lado, sugiere que los Estados adopten una legislación que permita: (i) la preservación y producción de evidencia electrónica; (ii) la búsqueda e incautación legal de sistemas informáticos; y (iii) la recolección de datos de tráfico y de contenido por parte de las autoridades. Para lo cual exige, que las partes colaboren en las siguientes temáticas: (i) la extradición de los delincuentes; (ii) el intercambio de información; y (iii) la preservación, acceso, interceptación y relación de datos de tráfico y contenido, asignando un punto de contacto que sea responsable de asegurar una asistencia inmediata en investigaciones y procedimientos relacionados a los ciberdelitos (Gálvez Reyes & Gálvez Pacheco, 2020).

Toda esta temática mostrada en el párrafo precedente demuestra lo pertinente de considerar para la sociedad peruana y la ciudadanía digital, en empezar a desarrollar las competencias digitales de seguridad del DigComp 2.2, desde la educación básica regular. Se precisa, que el término ciberseguridad no es sinónimo de la seguridad de la información, debe entenderse que la seguridad de la información tiene una visión mayor que la ciberseguridad, en este caso la información también abarca lo verbal y escrito mientras que la ciberseguridad básicamente se dirige a proteger la información en formato digital y los sistemas de información interconectados que procesan, transmiten o almacenan información, mientras que, la seguridad de la información de manera general considera políticas, esquemas de seguridad desde una perspectiva holística, directrices, métodos de gestión de riesgos, capacitación, sensibilización, buenas prácticas, aseguramiento y técnicas a usarse para proteger los activos de las organizaciones (Mario & Correa, 2018).

Otro argumento importante, que explica la importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde la educación básica regular, lo encontramos en el Manual de Tallin 2.0, elaborado por el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCD COE de la OTAN) con sede en Tallin, Estonia, que en su versión 2.0 del año 2017 está referido al derecho internacional aplicable a las ciberoperaciones que

tienen lugar en el ciberespacio. A diferencia del Convenio de Budapest, este Manual no es un documento vinculante para los Estados, pero si brinda la doctrina acordada por los especialistas más competentes a nivel mundial, su objetivo es desarrollar el derecho internacional aplicable a las ciberoperaciones a juicio de los expertos, brindando asistencia legal a los asesores jurídicos de los Estados sobre diversos temas relevantes para elaborar un proyecto de ley aplicable a las ciberoperaciones en sus respectivos Estados (Gálvez Reyes & Gálvez Pacheco, 2020). Las consideraciones de este Manual demuestran también lo importante de la temática de las competencias de seguridad ya citadas.

Así mismo, en el contexto peruano algunos argumentos que explican la importancia de las competencias digitales de seguridad para la ciudadanía digital, tienen que ver, que el Perú cuenta con el Sistema Nacional de Transformación Digital creado en enero del 2020, mediante el Decreto de Urgencia Nº 006-2020, y posteriormente mediante el Decreto de Urgencia Nº 007-2020, se establece el Marco de Confianza Digital que presenta las medidas para aumentar la confianza de las personas en su interacción con los servicios digitales brindados por entidades públicas y organizaciones del sector privado, lo señalado anteriormente evidencia que los temas de seguridad de la información y ciberseguridad en el Perú debe ser parte de una estrategia integral y desde una mirada holística. Debiendo considerarse la ciberseguridad con énfasis en la protección de la infraestructura crítica, la lucha contra el ciberdelito y la mejora de la competencia en seguridad de la información (Pacheco Araoz, 2020). Lo argumentado, justifica que se incluya las competencias digitales de seguridad en el tema educativo desde el sétimo ciclo de la educación básica regular, a fin de preparar con las competencias requeridas por los ciudadanos digitales.

De manera complementaria, el PEN 2036 explica que la transformación digital y el camino hacia un gobierno digital es trascendente, requiriéndose afianzar las competencias de los servidores públicos en todos los niveles de Gobierno, que les permita interactuar a través de medios digitales, así mismo, detalla que el gobierno digital está dirigido a que los servicios públicos

contribuyan al ejercicio de la ciudadanía de las personas. El tránsito hacia un gobierno digital propicia que los servidores públicos desarrollen aprendizajes desde los espacios de la educación, para de esta manera, generar capacidades y poder acceder información; es importante recalcar que la importancia de las TIC en la vida de las personas conlleva que no acceder a ella pueda ser motivo de exclusión a diversas actividades (CNE, 2020). Por lo que, para incentivar que las TIC favorezcan la inclusión se debe pensar desarrollar capacidades de las competencias digitales de seguridad, desde el sétimo ciclo de la educación básica regular.

Así mismo, para entender y explicar de cómo el hecho de poder desarrollar las competencias digitales de seguridad del DigComp 2.2 desde la educación básica regular serían fundamentales para mejorar la seguridad digital, seguridad de los datos e información en el contexto peruano, primero es bueno explicar lo que implica y comprende un Sistema de Gestión de Seguridad de la Información (SGSI), esto es importante entender porque un SGSI nos brinda el paraguas genérico de toda la temática de seguridad digital, seguridad de datos e información en cualquier organización a nivel mundial, incluyendo las instituciones y organizaciones peruanas; en este sentido, además son aspectos normalizados en los diferentes estándares internacionales de la familia ISO 27000 que justamente estandariza a nivel mundial estas áreas de conocimiento, por lo que se precisa que un SGSI comprende: las políticas generales y específicas, procedimientos del sistema de gestión y los controles de seguridad digital, seguridad de datos e información que ayuden a coadyubar la administración de la información, la cual está orientada a las criterios siguientes: preservación de la confidencialidad, integridad y disponibilidad de la información de las instituciones y organizaciones peruanas. Al respecto: La confidencialidad implica el acceso a la información por parte únicamente de quienes están autorizados, la integridad conlleva el mantenimiento de la exactitud y totalidad de la información y sus métodos de procesamiento, y la disponibilidad está referida al acceso de la información por parte de los usuarios autorizados en el momento que lo requieran (Organización Internacional de Normalización, 2013).

En este sentido, el SGSI, involucra a la organización de manera integral y a los procesos que afectan su seguridad digital, seguridad de los datos e información, teniendo como finalidad conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información desde una visión general, brindando confianza a las instituciones y organizaciones peruanas que los requisitos de seguridad serán cumplidos (Organización Internacional de Normalización, 2018).

Así mismo, se debe considerar que la información es un activo muy valioso que sirve como insumo para todos los procesos de las organizaciones, incluyendo la toma de decisiones en todos los niveles organizacionales y del cual depende el adecuado funcionamiento de las instituciones y organizaciones peruanas, en consecuencia, mantener su integridad, confidencialidad y disponibilidad es esencial. La seguridad digital, seguridad de los datos e información tiene que ver con cuidar y proteger los activos de información críticos o más importantes para el éxito de las instituciones y organizaciones peruanas, se debe considerar que, a diario, estamos amenazados por riesgos que mantienen en alerta la integridad, confidencialidad y disponibilidad de la información, y que provienen no sólo desde el exterior de las instituciones y organizaciones, sino también desde el interior (Organización Internacional de Normalización, 2017).

Para proteger las organizaciones e instituciones de las amenazas constantes que se presentan en los entornos digitales y en general a nivel mundial, primero se requiere saber de ellas o conocerlas, para luego pensar en estrategias de como contenerlas o superarlas de la manera más eficiente y eficaz, para ello se debe establecer procedimientos e implementar controles integrales de seguridad basados, controles que deben basarse en una evaluación integral de los riesgos y luego en una medición continua de su eficacia (Organización Internacional de Normalización, 2022).

Por lo expuesto anteriormente se sustenta la relevancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde la educación básica regular, ya que serían la base de toda la temática expuesta de seguridad

de la información y contribuiría en las competencias digitales de los ciudadanos digitales. Así mismo, cabe precisar, que los citados estándares internacionales mencionados en los párrafos anteriores, son aplicables al Estado Peruano y en consecuencia a las instituciones y organizaciones peruanas, esto queda evidenciado por que dichos estándares cuentan con una Norma Técnica Peruana equivalente, documentos que se muestran a continuación.

Al respecto el Instituto Nacional de Calidad (INACAL) a través del Comité N° 21 “Codificación e Intercambio Electrónico de Datos”, tomando como base los estándares internacionales de la Organización Internacional de Estandarización (en inglés International Organization for Standardization (ISO)), analizó, adoptó y aprobó Normas Técnicas Peruanas, que son usadas por el Estado Peruano, siendo las que refiero a continuación, las principales referidas a la implementación de un SGSI:

Primero veremos a la Norma Técnica Peruana NTP-ISO/IEC 27001-2014. Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2° Edición, de 20 de noviembre del 2014, equivalente a la ISO/IEC 27001:2013, esta es la principal norma de la familia ISO/IEC 27000, la cual contiene los requisitos obligatorios para la implementación de un SGSI y en su Anexo A, presenta una lista de los objetivos o lineamientos de control y una serie controles de seguridad de la información que deben implementarse (Norma Técnica Peruana, 2014).

Este estándar básicamente presenta los aspectos necesarios o requisitos para que una organización de todo tipo a nivel mundial logre implementar su SGSI, ya sean empresas transnacionales, pequeñas empresas o entidades públicas; estos requisitos se basan en buenas prácticas internacionales sobre seguridad de la información, entre los requisitos más importantes podemos citar los siguientes: (i) conocer la organización y su contexto el cual está orientado a que los objetivos de la seguridad de la información consideren los objetivos propios de la empresa u entidad pública, (ii) el liderazgo es otro aspecto considerado, el cual tiene que ver con el compromiso continuo de los directivos de la organización o entidad pública en la implantación

de un SGSI, especialmente apoyando y consolidando la cultura de seguridad de la información dentro de las organizaciones, (iii) también tenemos los requisitos relacionados a definir la metodología de gestión de riesgos de seguridad de la información, la identificación de los activos de información con sus correspondientes amenazas y vulnerabilidades de la seguridad de la información, la evaluación de riesgos de seguridad de la información (que comprende identificación del riesgo, análisis del riesgo y valoración del riesgo), los criterios de asignación y el tratamiento de riesgos de seguridad de la información, la selección de los controles aplicables del listado general de controles señalados en el Anexo A, y el plan de gestión de riesgos de seguridad de la información, (iv) respecto a las revisiones del desempeño del SGSI este estándar presenta como requisitos las auditorías internas de seguridad de la información, y el proceso de revisión por parte de la dirección. Lo manifestado previamente, muestra que es importante que las competencias digitales de seguridad, que propone el modelo DigCom 2.2 que comprenden las temáticas de: protección de dispositivos digitales, protección de datos personales y privacidad de datos, protección de la salud y del bienestar digital; y protección medioambiental por el impacto de las tecnologías, se desarrollen desde el sétimo ciclo de la educación básica regular ya que formarán a los estudiantes en competencias críticas enmarcadas en los requisitos de la NTP-ISO/IEC 27001-2014 e ISO/IEC 27001:2013.

También, tenemos la Norma Técnica Peruana NTP-ISO/IEC 27002-2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, de 27 de diciembre del 2017, equivalente a la ISO/IEC 27002:2013, que es una guía de buenas prácticas en la cual se presentan recomendaciones para la implementación de cada uno de los objetivos o lineamientos de control y controles de seguridad de la información que son el detalle de lo citado en el Anexo A mencionado en la NTP-ISO/IEC 27001-2014 (Norma Técnica Peruana, 2017).

En este caso se debe precisar que a nivel internacional ya se cuenta con la nueva versión de este estándar que fue publicada en el año 2022, estamos hablando de la ISO/IEC 27002:2022 que actualmente no tiene una Norma

Técnica Peruana equivalente; la ISO 27002:2013 presentaba 114 controles, mientras que la actual versión del 2022 considera 93 controles, agrupados en 4 cláusulas, subdivididos en 37 controles organizativos, 8 controles sobre personas, 14 controles físicos y 34 controles relacionados a temas tecnológicos, estas buenas prácticas que brinda este estándar internacional engloban temas como gobierno de seguridad de la información, gestión de activos, protección de la información, seguridad de los recursos humanos, seguridad física, seguridad de sistemas y redes, seguridad de las aplicaciones, configuración segura, gestión de la identidad y del acceso, gestión de amenazas y vulnerabilidades, continuidad, seguridad de las relaciones con los proveedores, cumplimiento legal, gestión de eventos de seguridad de la información y aseguramiento de la información. Las citadas buenas prácticas de seguridad de la información proporcionadas por este estándar a través de sus controles manifestados en el párrafo precedente, proporcionan evidencias que las competencias digitales de seguridad, que propone el modelo DigCom, que comprenden las temáticas de: protección de dispositivos digitales, protección de datos personales y privacidad de datos, protección de la salud y del bienestar digital; y protección medioambiental por el impacto de las tecnologías, son importantes a ser estudiados desde el sétimo ciclo de la educación básica regular ya que formarán a los estudiantes en competencias fundamentales enmarcadas en las buenas prácticas de la NTP-ISO/IEC 27002-2017 e ISO/IEC 27002:2022.

Así mismo, contamos con la Norma Técnica Peruana NTP-ISO/IEC 27003-2019. Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Orientación, de 18 de diciembre del 2019, equivalente a la ISO/IEC 27003:2017, que proporciona orientación sobre los requisitos para un SGSI, que se especifican en la NTP-ISO/IEC 27001-2014 (Norma Técnica Peruana, 2019).

Sobre lo referido en el párrafo anterior, encontramos el detalle de los requisitos para implementar un SGSI, brindando orientaciones para definir el alcance y aprobación del SGSI, muestra orientaciones sobre los límites y políticas de un SGSI, así mismo, brinda orientaciones respecto a la evaluación de los requerimientos de seguridad de la información; y un aspecto crucial que

especifica este estándar se refiere al proceso de evaluación de riesgos y el plan de tratamiento de riesgos requeridos como parte de la implementación de un SGSI. Dichas orientaciones de seguridad de la información del presente estándar, cómo en los casos anteriores, también nos indican que las competencias digitales de seguridad, que propone el modelo DigCom, son importantes considerarlas desde la etapa de la educación básica regular en el Estado peruano ya que involucran temáticas inmersas en la NTP-ISO/IEC 27003-2019 e ISO/IEC 27003:2017.

Como se mencionó al analizar las normas o estándares anteriores, un aspecto vital durante la implementación de un SGSI es lo relacionado al proceso de gestión de riesgos, para lo cual se cuenta con la Norma Técnica Peruana NTP-ISO/IEC 27005-2018. Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información, de 28 de diciembre del 2018, equivalente a la ISO/IEC 27005:2018, la misma que proporciona una guía sobre la gestión de riesgos para ayudar a cumplir con los requisitos específicos de la NTP-ISO/IEC 27001-2014, y que también indica que se puede utilizar múltiples enfoques o metodologías de gestión del riesgo (Norma Técnica Peruana, 2018).

Cabe precisar que la citada Norma Técnica Peruana se complementa y enmarca en la Norma Técnica Peruana NTP-ISO/IEC 31000-2018. Gestión del riesgo. Directrices, de 27 de junio del 2018, equivalente a la ISO 31000:2018, estructurada en tres (3) elementos: los principios para la gestión de riesgos, la estructura de soporte cuyo objetivo es integrar el proceso de gestión de riesgos con la alta dirección; y, el proceso de gestión de riesgos que consta de tres (3) etapas: establecimiento del contexto, evaluación de riesgos y tratamiento de los mismos (Norma Técnica Peruana, 2018).

En cuanto a estos dos estándares sobre riesgos y específicamente sobre gestión de riesgos de seguridad de la información, debe entenderse que su proceso consiste en: establecer el contexto para la identificación de riesgos, realizar la evaluación del riesgo (identificar, analizar y valorar el riesgo), tratamiento del riesgo, comunicar el riesgo de manera continua; y por último

hacer el seguimiento y revisión del riesgo de seguridad de la información, si nos enfocamos en la identificación y análisis de los riesgos de seguridad de la información (cómo parte de la evaluación del riesgo), se tendrán que identificar las amenazas, vulnerabilidades y sus riesgos asociados para los activos de información, por lo que a continuación de acuerdo a lo señalado por la ISO/IEC 27005:2018 se presentan ejemplos de amenazas y vulnerabilidades relacionadas a las competencias digitales de seguridad, que propone el modelo DigCom y que resaltan su importancia para que los estudiantes peruanos desde el sétimo ciclo de la EBR puedan desarrollarlas.

Algunos ejemplos de amenazas y vulnerabilidades que identifica la ISO/IEC 27005:2018 son las siguientes: a) Amenazas (i) respecto a compromiso de información: Interceptación de señales de interferencias comprometidas, espionaje remoto, escucha secreta, robo de medios o documentos, datos de fuentes poco fiables, manipulación con hardware y software, (ii) en cuanto a fallas técnicas: falla de equipo, mal funcionamiento de software, brecha de mantenimiento del sistema de información, (iii) referidas a acciones no autorizadas: uso no autorizado de equipo, copia fraudulenta de software, uso de software falsificado o copiado, corrupción de datos, procesamiento ilegal de datos, (iv) compromiso de las funciones: error en uso, abuso de derechos, falsificación de derechos, negación de acciones y brecha de disponibilidad de personal. b) Vulnerabilidades (i) hardware: mantenimiento insuficiente e instalación defectuosa de medios de almacenamiento, falta de esquemas periódicos de reemplazo, sensibilidad a radiación electromagnética, falta de control eficiente de cambio de configuración, susceptibilidad a radiación electromagnética, falta de control eficiente de cambio de configuración, susceptibilidad a variaciones de voltaje, susceptibilidad a variaciones de temperatura, almacenamiento no protegido, falta de cuidado en eliminación, copiado no controlado, (vi) software: falta o insuficiente prueba de software, fallas bien conocidas en el software, no se cierra la sesión cuando se abandona la estación de trabajo, eliminación o reutilización de medios de almacenamiento sin borrado apropiado, falta de seguimiento de auditoria, incorrecta asignación de derechos de acceso, software ampliamente distribuido, aplicación de programas de aplicación a datos erróneos en términos de tiempo, complicada interfaz de

usuario, falta de documentación, establecer parámetros incorrectos, fechas incorrectas, falta de mecanismos de identificación y autenticación como autenticación de usuario, tablas de contraseñas no protegidas, manejo deficiente de contraseñas, habilitación de servicios innecesarios, software nuevo o inmaduro, especificaciones poco claras o incompletas para desarrolladores, falta de control de cambio efectivo, descarga y uso no controlado de software, falta de copias de respaldo, falta de protección física del edificio, puertas y ventanas y falla en producir reportes de gestión.

Las amenazas y vulnerabilidades mencionadas y necesarias durante la evaluación de riesgos de seguridad de la información que presenta la NTP-ISO/IEC 27005-2018 e ISO/IEC 27005:2018, que forman parte de la implementación de los SGSI, de acuerdo a la ISO/IEC 27001:2013 y NTP-ISO/IEC 27001-2014, en las organizaciones privadas y entidades públicas del Estado peruano respectivamente; así como, el contenido analizado de las Normas Técnicas Peruanas y estándares internaciones siguientes: NTP-ISO/IEC 27001-2014, ISO/IEC 27001:2013, NTP-ISO/IEC 27002-2017, ISO/IEC 27002:2022, NTP-ISO/IEC 27003-2019 e ISO/IEC 27003:2017, demuestran que las competencias digitales de seguridad, que propone el modelo DigCom 2.2, que abarcan la protección de dispositivos digitales, la protección de datos personales y privacidad de datos, la protección de la salud y del bienestar digital; y la protección medioambiental por el impacto de las tecnologías; son competencias digitales que deben ser adquiridas y estudiadas desde el sétimo ciclo de la educación básica regular para ir formando a los estudiantes peruanos en estos temas vigentes e importantes y para contribuir con sus competencias de ciudadanos digitales; por lo que deberían ser consideradas como parte del Currículum Nacional de la Educación Básica Regular del MINEDU.

Teniendo en cuenta, lo mencionado anteriormente es bueno tener presente que la competencia 28 del Currículo Nacional de Educación Básica vigente, sólo señala de manera genérica para el ámbito de la competencia digital que el alumno logre entender, conceptualizar, interpretar, y por lo tanto hacer cambios y mejoras a los entornos virtuales que formen parte de su desarrollo y proceso en sus actividades de aprendizaje, así como, en actividades sociales en

este entorno (MINEDU, 2016). Por lo que, es necesario que los estudiantes obtengan competencias digitales más detalladas y profundas, debido a lo explicado anteriormente, así mismo, porque el Estado peruano se encuentra propiciando el desarrollo de la transformación digital, el gobierno digital y la gestión de la seguridad de la información, en este sentido como parte de este proceso el Estado peruano cuenta actualmente con normativa importante, como Leyes y Reglamentos, Decretos Legislativos, Decretos Supremos, Decretos de Urgencia, entre otros documentos orientados específicamente a temas que engloban holísticamente las competencias digitales de seguridad en el marco de la seguridad digital, seguridad de datos y seguridad de la información; algunas de estas normas relevantes son las siguientes:

Primero es importante mencionar la Ley de Gobierno Digital, aprobada mediante Decreto Legislativo N° 1412 el 12 de setiembre de 2018 por la PCM, la cual establece el Marco General del Gobierno Digital para los temas de gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y seguridad de datos; así mismo, considera aspectos legales aplicables a las tecnologías digitales para los procesos de digitalización y respecto a la prestación de servicios digitales; este documento establece el Marco de Seguridad Digital del Estado peruano, precisándolo como una agrupación de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares con la finalidad de preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital y que es administrado por las entidades públicas. Otro punto importante de esta norma es que indica que las entidades públicas deben establecer, mantener y documentar un SGSI, y aclara las principales diferencias entre seguridad de la información y seguridad digital, indicando que para la seguridad de la información debe conceptualizarse a la información, en todos sus formatos (físico, oral, digital), mientras que la seguridad digital tiene un enfoque acotado solo a un entorno digital (PCM, 2018).

Otra norma legal importante es el Reglamento de la Ley de Gobierno Digital, aprobado por la PCM el 18 de febrero de 2021 a través del Decreto Supremo N° 029, el cual regula o reglamenta detalladamente las actividades de la Ley de Gobierno Digital, así mismo, presenta el Modelo de Identidad Digital

del Estado que abarca los siguientes componentes: i) Principios, ii) Ciudadanos digitales, iii) Gestores de la identidad digital, iv) Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (ID GOB.PE), v) Atributos de identidad digital, vi) Proveedores de atributos de identidad complementarios; y, vii) Credenciales de autenticación; vemos que como parte de este modelo se involucra al ciudadano digital, con los siguientes requisitos: i) Tienen atributos de identidad propios, ii) Cuentan con una casilla única electrónica, iii) Cuentan con credenciales de autenticación emitidas, entregadas y/o habilitadas dentro del marco del presente reglamento; y a su vez se establecen las siguientes obligaciones para el ciudadano digital: i) Desenvolverse en el entorno digital de acuerdo con las normas del derecho común y buenas costumbres, ii) Facilitar a las entidades públicas información oportuna, veraz, completa y adecuada, asumiendo responsabilidad sobre ello, iii) Resguardar, custodiar y utilizar sus credenciales de autenticación de manera diligente y manteniendo el control de éstas, iv) No afectar la disponibilidad de los servicios digitales, ni alterarlos, ni hacer uso no autorizado o indebido de los mismos, v) Respetar las políticas de seguridad y privacidad de la información establecida por los servicios digitales, vi) Ejercer la responsabilidad sobre el uso de sus datos y acciones en su interacción con las entidades públicas en el entorno digital, y vii) Otros que establezca la PCM. También presenta y explica el Modelo de Seguridad Digital, que esta formado por: i) Responsables de los ámbitos del Marco de Seguridad Digital, ii) Centro Nacional de Seguridad Digital, iii) Redes de confianza en Seguridad Digital, iv) Oficial de Seguridad Digital, v) Sistemas de Gestión de Seguridad de la Información, vi) Ciudadano o persona en general, vii) Autoridad (PCM, 2021).

Una tercera norma legal, es el Decreto de Urgencia N° 0006-2020 que fue aprobado por la PCM el 8 de enero de 2020 y que crea el Sistema Nacional de Transformación Digital, cuya finalidad es propiciar la transformación digital de las organizaciones privadas y entidades públicas, así como, afianzar el uso de las tecnologías y servicios digitales, en los ciudadanos peruanos; otra finalidad es fortalecer el ejercicio de la ciudadanía digital con deberes y derechos digitales de los ciudadanos, también busca apoyar la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital, por

otro lado, este el Sistema Nacional de Transformación Digital tiene entre sus principios uno sobre las competencias digitales, el cual propone que la transformación digital necesita afianzar las competencias digitales, las habilidades y destrezas digitales, los servicios digitales, seguridad digital y la arquitectura digital (PCM, 2020).

Complementaria a la norma legal anterior, el Estado peruano cuenta con el Reglamento del Sistema Nacional de Transformación Digital, el cual mediante Decreto Supremo N° 157-2021-PCM DE 24 de setiembre de 2021, fue aprobado por la PCM, documento que regula o reglamenta detalladamente el Sistema Nacional de Transformación Digital, que comprende temas como gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital, confianza digital, salud digital, justicia digital, talento digital, comercio electrónico, entre otras, además un aspecto importante de esta norma es la definición que muestra sobre ciudadanía digital, explicándola como la capacidad de los ciudadanos en poder desarrollarse a nivel holístico en un entorno digital, considerando importante el desarrollo de competencias digitales, para ejecutar trámites, operaciones financieras, operaciones de comercio electrónico, actividades de entretenimiento, actividades de comunicación, así como, para buscar y obtener datos e información usando Internet (PCM, 2021).

Otra norma legal, considerada en esta investigación es el Decreto Supremo N° 050-2018-PCM, aprobado por la PCM el 14 de mayo de 2018, que define la seguridad digital en el ámbito nacional, al respecto la seguridad digital debe entenderse como el estado de confianza en el entorno digital, producto de que las organizaciones privadas y entidades públicas luego de un proceso integral de evaluación de riesgos de seguridad de la información (que comprende identificación del riesgo, análisis del riesgo y valoración del riesgo), se gestión estos riesgos aplicando cuando corresponda hacerlo los controles o medidas que afectan la seguridad ya sea de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en el entorno digital (PCM, 2018).

La penúltima norma legal, revisada es el Decreto de Urgencia 007-2020 aprobada el 8 de enero de 2020 por la PCM, que establece el marco de confianza digital y dispone medidas para su fortalecimiento; cuyo objeto es establecer las medidas que brinden confianza en los ciudadanos cuando utilicen los servicios digitales de las organizaciones privadas y entidades públicas; así mismo, referente al concepto de confianza digital, se refiere al estado resultante que surge de las interacciones digitales, este resultado puede ser veraz, predecible, ético, proactivo, transparente, seguro, inclusivo y confiable. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital. Por otro lado, entorno digital se entiende como el dominio o ámbito en el cual las tecnologías y dispositivos digitales, operan interconectados a través de diversas plataformas de información y comunicaciones; esta norma enmarca la ciberseguridad, como la capacidad tecnológica de mantener operativas las redes y comunicaciones, los sistemas informáticos, y en general todos los activos de tecnologías de información y comunicación, protegiéndolos de amenazas y vulnerabilidades en entornos digitales (PCM, 2020).

Por último, tenemos la Ley N° 3099 aprobada por la PCM el 09 de agosto de 2019, que aprueba la Ley de Ciberdefensa, respecto al concepto de ciberdefensa debe entenderse como la capacidad militar del Estado peruano, de actuar frente a amenazas o ataques realizados en el entorno del ciberespacio ante situaciones que afecten la seguridad nacional. Otro aspecto importante se refiere a que este documento recuerda la importancia de crear contenidos curriculares de educación superior sobre seguridad digital, incluyendo los temas de ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pregrado y postgrado (PCM, 2019).

Finalmente, luego de analizar las normas legales más importantes del Estado peruano, que enfocan desde diversas perspectivas muchas competencias digitales de seguridad necesarias actualmente por los ciudadanos y que engloban aspectos como gobierno digital, transferencia digital, entorno

digital, seguridad digital, seguridad de datos, seguridad de la información, seguridad digital, confianza digital, ciberguerra, ciberseguridad, entre otros temas importantes, se corrobora que es necesario que los estudiantes desarrollen desde el sétimo ciclo de la EBR competencias digitales de seguridad, que abarquen un mayor espectro que la competencia 28 del Currículo Nacional de Educación Básica vigente que es muy general, es decir que las competencias digitales de seguridad que propone el modelo DigCom 2.2, que abarcan la protección de dispositivos digitales, la protección de datos personales y privacidad de datos, la protección de la salud y del bienestar digital; y la protección medioambiental por el impacto de las tecnologías; son competencias digitales que deben ser adquiridas y estudiadas desde el sétimo ciclo de la EBR para ir formando a los estudiantes peruanos en estos temas vigentes e importantes y para contribuir con sus competencias de ciudadanos digitales en toda la amplitud de temas desarrollados en el presente trabajo de investigación; por lo que deberían ser consideradas como parte del Currículum Nacional de la Educación Básica Regular del MINEDU.

CONCLUSIONES

1. Respecto a la importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2 en la EBR del nivel secundario, desde su sétimo ciclo en el contexto peruano, se sustenta la relevancia de desarrollar dichas competencias digitales, considerando que estas propiciaran que los estudiantes de la EBR adquieran nuevas competencias diferentes a las tradicionales, que les permita ser más versátiles al obtener competencias digitales de seguridad enmarcadas en la temática de seguridad digital, seguridad de los datos y de la Información, hoy en día criterios fundamentales para la gestión de las Instituciones públicas y organizaciones privadas peruanas desde una perspectiva holística de la seguridad de la información, tomando en cuenta diversas Normas Técnicas Peruanas y estándares internacionales sobre seguridad de la información; así mismo, es bueno precisar que estas competencias digitales de seguridad del DigComp 2.2 son más específicas y abarcan un mayor espectro de las que brinda actualmente el Currículo Nacional de la EBR a través de su competencia número 28, por lo que desarrollarlas desde etapas tempranas de la formación de los estudiantes busca lograr competencias futuras que les permita desenvolverse en este nuevo ecosistema digital que nos trae el proceso de transformación digital que se encuentra actualmente inmerso el Estado peruano como parte del gobierno digital que impulsa la PCM a través de la Secretaría de Gobierno Digital; en este sentido se concluye que las competencias digitales de seguridad, que propone el modelo DigCom 2.2, que abarcan la protección de dispositivos digitales, la protección de datos personales y privacidad de datos, la protección de la salud y del bienestar digital; y la protección medioambiental por el impacto de las tecnologías, deben ser consideradas y estudiadas desde el sétimo ciclo de la EBR para ir formando a los estudiantes peruanos en estos temas vigentes e importantes y para de esta manera contribuir con sus competencias como futuros ciudadanos digitales; por lo que debería analizarse su inclusión como parte del Currículum Nacional de la Educación Básica Regular del MINEDU ya que contribuirían con las competencias digitales requeridas por los ciudadanos digitales ante los cambios constantes de las tecnologías que soportan diversas plataformas de información y comunicaciones.

2. En referencia a describir las competencias digitales del área de seguridad del DigComp 2.2, relacionándolas con las competencias digitales del Currículo Nacional de la EBR, tenemos que el área de competencia de seguridad del DigComp 2.2, es mucho más amplia que la competencia digital número 28 del Currículo Nacional de Educación Básica Regular, presentándose de manera estructurada y cubriendo mayores temas de seguridad digital, seguridad de datos e información, los cuales son temas vigentes y requeridos actualmente por el Estado peruano, como parte del proceso de transformación digital y en el marco de la implementación del gobierno digital ya señalado, las 4 competencias digitales del DigComp 2.2 son: (i) **Protección de dispositivos:** Proteger los dispositivos y los contenidos digitales; y, comprender los riesgos y las amenazas en los entornos digitales, conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad, (ii) **Protección de datos personales y privacidad:** Proteger los datos personales y la privacidad en los entornos digitales, entender cómo utilizar y compartir la información personal identificable, siendo capaz de protegerse a sí mismo y a los demás de los daños; y, entender que los servicios digitales utilizan una “política de privacidad” para informar sobre el uso de los datos personales, (iii) **Protección de la salud y del bienestar:** Capacidades a la hora de evitar riesgos para la salud tanto física como mental en el uso de las tecnologías digitales; y, capacidad a la hora de protegerse uno mismo y a otros ante los riesgos de los entornos digitales (por ejemplo: cyberbullying); y, (iv) **Protección medioambiental:** Ser consciente del impacto de las tecnologías digitales y su uso.

   Mientras que por otro lado, el Currículo Nacional de Educación Básica Regular, considera una sola competencia digital, que es la número 28, que plantea para su competencia digital diversos temas de carácter general: primero cita que los alumnos puedan comprender, conceptualizar, analizar e interpretar, y por lo tanto lograr mejoras y cambios significativos en los entornos virtuales que forma parte y que comprenden su desarrollo y proceso en sus actividades de aprendizaje, así mismo, en actividades y grupos sociales en este entorno digital. Lo que se explicó en el párrafo precedente, ayuda a lograr que diversos procesos como la recopilación, selección o disgregación y evaluación de datos e información puedan funcionar integrados. Otro aspecto, es que se menciona criterios de modificación, innovación y creación de materiales digitales, materiales

comunicacionales, dirigidos a que los estudiantes participen e interactúen en comunidades virtuales, finalmente, los alumnos deberían tener competencias de adaptación a entornos diferentes en función de cómo lo vayan requiriendo para un adecuado comportamiento social (MINEDU, 2016). Se observa que, dicha competencia sólo se describe de manera genérica, brindando orientaciones enmarcadas en los cuatro aspectos siguientes: El alumno podrá personalizar los entornos virtuales en los que se desenvuelve, gestionará datos e información de los entornos virtuales, logrará interactuar en los citados entornos virtuales, y por último tiene la capacidad de idear y crear diferentes tipos de objetos virtuales usando formatos variados (MINEDU, 2016).

3. Respecto a la importancia de las competencias digitales del área de seguridad del DigComp 2.2. en la ciudadanía digital y para la seguridad de la información en el contexto peruano, se sustenta la importancia de desarrollar estas competencias digitales por que contribuirían en muchos aspectos de la seguridad digital, seguridad de datos e información requeridos por el Estado peruano, como parte del proceso de transformación digital y en el marco de la implementación del gobierno digital en el cual nos encontramos y por el cual se vienen realizando diversas actividades referidas a la temática de seguridad de la información, principalmente en el marco de la implementación de los SGSI de acuerdo al estándar internacional ISO/IEC 27001:2013 y a la Norma Técnica Peruana NTP-ISO/IEC 27001-2014, en las organizaciones privadas y entidades públicas del Estado peruano respectivamente; en este sentido se precisa que para la implementación de los SGSI se requiere de Normas Técnicas Peruanas y estándares internaciones complementarios como: NTP-ISO/IEC 27002-2017, ISO/IEC 27002:2022, NTP-ISO/IEC 27003-2019 e ISO/IEC 27003:2017, NTP-ISO/IEC 27005-2018 e ISO/IEC 27005:2018; que en todos sus casos requieren de competencias digitales de seguridad, prioritariamente durante la evaluación de riesgos de seguridad de la información que requiere la NTP-ISO/IEC 27005-2018 e ISO/IEC 27005:2018 durante la identificación y análisis de amenazas y vulnerabilidades a los activos de información. Adicionalmente, luego de analizar las normas legales más importantes del Estado peruano, que enfocan desde diversas perspectivas muchas competencias digitales de seguridad necesarias actualmente por los ciudadanos y que engloban aspectos como gobierno digital,

transferencia digital, entorno digital, seguridad digital, seguridad de datos, seguridad de la información, seguridad digital, confianza digital, ciberguerra, ciberseguridad, entre otros temas importantes, se concluye que es necesario que los estudiantes desarrollen desde el sétimo ciclo de la EBR competencias digitales de seguridad, que abarquen un mayor espectro que la competencia 28 del Currículo Nacional de Educación Básica vigente que es muy general, es decir que las competencias digitales de seguridad que propone el modelo DigCom 2.2, que comprenden la protección de dispositivos digitales, la protección de datos personales y privacidad de datos, la protección de la salud y del bienestar digital; y la protección medioambiental por el impacto de las tecnologías; son competencias digitales que deben ser adquiridas y estudiadas desde el sétimo ciclo de la EBR para ir formando a los estudiantes peruanos en estos temas vigentes e importantes y para contribuir con sus competencias de ciudadanos digitales en toda la amplitud de temas desarrollados en el presente trabajo de investigación.

RECOMENDACIONES

Por último, se recomienda, considerar para próximas investigaciones otros niveles del Currículo Nacional de la EBR, a los docentes de la EBR, así como, tomar en cuenta otras competencias clave del modelo de la DigComp 2.2 como por ejemplo: 1) Ciencia, tecnología, ingeniería, matemáticas, 2) Lenguajes, 3) Alfabetización, 4) Conciencia y expresión cultural, 5) Emprendimiento, 6) Competencia civil; y, 7) Personales, sociales y aprender a aprender; así mismo, para brindar un alcance aún mayor y con más profundidad de la importancia del modelo de la DigComp 2.2 se puede analizar otros estándares internacionales de Seguridad de la Información como la ISO/IEC 27017:2015, “Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, basado en ISO/IEC 27002 para los servicios de la nube”, la ISO/IEC 27035-1:2016, “Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidencias”, la ISO/IEC 27035-2:2016, “Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 2: Directrices para planificar y prepararse para la respuesta a incidentes”, la ISO/IEC 27103:2018, “Tecnología de la información. Técnicas de seguridad. Ciberseguridad”, entre otros. Y analizar adicionalmente normas legales sobre estos temas de otros países. Adicionalmente, se recomienda se realice una comparación o análisis de los próximos resultados con los presentados en el presente trabajo.

REFERENCIAS

Agencia Ejecutiva Europea de Educación y Cultura, Eurydice. (2019). *La educación digital en los centros educativos en Europa.* Oficina de Publicaciones. https://data.europa.eu/doi/10.2797/33210

Consejo Nacional de Educación-CNE. (2020). *Proyecto Educativo Nacional–2036. El Reto de la Ciudadanía Plena.* Lima: CNE. https://www.cne.gob.pe/uploads/publicaciones/2020/proyecto-educativo-nacional-al-2036.pdf

European Comission. (2007). *Competencias clave para un aprendizaje a lo largo de la vida un marco de referencia europeo. Bélgica: Comunidades Europeas.* https://www.educacionyfp.gob.es/dctm/ministerio/educacion/mecu/movilidad-europa/competenciasclave.pdf?documentId=0901e72b80685fb1

European Commission, Directorate-General for Education, Youth, Sport and Culture, McGrath, C., Frohlich Hougaard, K., O'Shea, M. (2020). *Supporting key competence development: learning approaches and environments in school education: input paper*, Publications Office. https://data.europa.eu/doi/10.2766/8227

García-Valcárcel, A., Casillas, M, S. y Basilotta Gómez-Pablos, V. M. (2020). *Validación de un modelo de indicadores (INCODIES) para evaluar la competencia digital de los estudiantes de Educación Básica*. Journal of New Approaches in Educational Research, *9(1),* 116-132. https://doi.org/10.7821/naer.2020.1.459

González-Fernández-Villavicencio, N. (2015). *DigComp o la necesaria adecuación al marco común de referencia en competencias digitales.* Anuario ThinkEPI, 9, 030–035. https://doi.org/10.3145/thinkepi.2015.04

Instituto Nacional de Calidad. (2014). *Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2°*

Edición (NTP 27001). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2017). *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información* (NTP 27002). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2019). *Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Orientación* (NTP 27003). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2018). *Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información* (NTP 27005). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2018). *Gestión del Riesgo. Directrices* (NTP 31000). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Lévano-Francia, L., Sánchez, S., Guillén-Aparicio, P., Tello-Cabello, S., Herrera-Paico, N., y Collantes-Inga, Z. (2019). *Competencias digitales y educación. Propósitos y Representaciones,* 7(2), 569-588. doi: http://dx.doi.org/10.20511/pyr2019.v7n2.329

Mario, J. y Correa, A. (2018). *Adaptación del modelo de madurez en ciberseguridad basado en C2M2, para la industria manufacturera del sector textil que utiliza sistemas SCADA.* Instituto Tecnológico Metropolitano. https://repositorio.itm.edu.co/handle/20.500.12622/4681

Mateus, J. C. y Suárez-Guerrero, C. (2017). *La competencia TIC en el nuevo currículo peruano desde la perspectiva de la educación mediática. Edmetic,* 6(2), 129-147. https://doi.org/10.21071/edmetic.v6i2.6908

Ministerio de Educación de Perú. (2003). *Ley General de Educación Ley N° 28044.* http://www.minedu.gob.pe/p/ley_general_de_educacion_28044.pdf

Ministerio de Educación de Perú. (2012). *Reglamento de la Ley General de Educación Ley N° 28044*. http://www.minedu.gob.pe/files/3896_201207100937.pdf

Ministerio de Educación de Perú. (2016). *Currículo Nacional de Educación Básica Regular.* http://www.minedu.gob.pe/curriculo

National Institute of Standards and Technology. (2015). *NIST Special Publication 800-16.* Obtenido de Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-16/800- 16.pdf

OECD (2019). *Trends Shaping Education 2019.* OECD Publishing. DOI: 10.1787/trends_edu-2019-en.

OECD (2018). *The future of education and skills. Education 2030: the future we want* (position paper). OECD Publishing. https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf

Organización Internacional de Normalización. (2013). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos* (ISO 27001). https://www.iso.org/store.html

Organización Internacional de Normalización. (2013). *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información* (ISO 27002). https://www.iso.org/store.html

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información* (ISO 27002). https://www.iso.org/store.html

Organización Internacional de Normalización. (2017). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Orientación* (ISO 27003). https://www.iso.org/store.html

Organización Internacional de Normalización. (2018). *Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de seguridad de la información* (ISO 27005). https://www.iso.org/store.html

Organización Internacional de Normalización. (2018). *Gestión del Riesgo. Directrices* (ISO 31000). https://www.iso.org/store.html

Pacheco A, E. J. (2020). *Oportunidades de Ciberdiplomacia para la Política Exterior del Perú*. http://repositorio.adp.edu.pe/handle/ADP/143

Presidencia del Consejo de Ministros. (2018). *Ley de Gobierno Digital*. http://www.minedu.gob.pe/files/3896_201207100937.pdf

Presidencia del Consejo de Ministros. (2018). *Decreto Supremo N° 050-2018-PCM que aprueba la definición de seguridad digital en el ámbito nacional.* https://busquedas.elperuano.pe/normaslegales/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1/

Presidencia del Consejo de Ministros. (2019*). Ley 3099 Ley de Ciberdefensa.* https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

Presidencia del Consejo de Ministros. (2020*). Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.* https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2/

Presidencia del Consejo de Ministros. (2020). *Decreto de Urgencia N° 0006-2020 que crea el Sistema Nacional de Transformación Digital.* https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-crea-el-sistema-nacional-de-transfor-decreto-de-urgencia-n-006-2020-1844001-1/

Presidencia del Consejo de Ministros. (2021). *Reglamento de la Ley de Gobierno Digital.* https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-del-decreto-legisl-decreto-supremo-n-029-2021-pcm-1929103-3/

Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 157-2021-PCM que aprueba el Reglamento del Sistema Nacional de Transformación Digital.* https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-del-decreto-de-urg-decreto-supremo-n-157-2021-pcm-1995486-1/

Reyes, M. y Gálvez Pacheco, R. (2020).*La recepción e incorporación del principio de cooperación internacional en materia de ciberseguridad en el derecho chileno.* Universidad de Chile. http://repositorio.uchile.cl/handle/2250/176706

Revilla F., D. y Sime P, L. (Eds.) (2021). *Perspectivas y reflexiones sobre el Proyecto Educativo Nacional al 2036.* Pontificia Universidad Católica del Perú, Facultad de Educación, Departamento Académico de Educación y Centro de Investigaciones y Servicios Educativos (CISE). págs.87-95. https://repositorio.pucp.edu.pe/index/handle/123456789/180968

Taguma, M., Feron, E. y Lim, M. H. (2018). *Future of education and skills 2030: Conceptual learning framework.* Organization of Economic Cooperation and Development.

Vuorikari, R., K, S. y Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes.* Oficina de Publicaciones de la Unión Europea. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415