

UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO

**Maestría en Educación
Mención Educación y Creatividad**

**Línea de investigación
Pedagogía creativa, didáctica, currículo y tecnología.**

**Programa:
Gestión pedagógica en el aula desde las competencias digitales docentes.**

MODALIDAD

Artículos profesionales de alto nivel

Título del Artículo Científico

**Seguridad informática: Competencia digital docente en la gestión pedagógica
de aula**

**Autora
Marjorie Silvana Delgado Santana**

**Tutora
Sonia Monserrate Párraga Muñoz**

**Investigación presentada como requisito para la obtención del título de
Magister en Educación, mención Educación y Creatividad**

Portoviejo, 20 de mayo del 2022



Seguridad informática: Competencia digital docente en la gestión pedagógica de aula
Computer security: Teaching digital competence in classroom pedagogical management

Lcda. Marjorie Silvana Delgado Santana

e.msdelgados@sangregorio.edu.ec

Universidad San Gregorio de Portoviejo, Manabí, Ecuador

<https://orcid.org/0000-0002-8928-4059>

Mg. Sonia Monserrate Párraga Muñoz

smparraga@sangregorio.edu.ec

Universidad San Gregorio de Portoviejo, Manabí, Ecuador

<https://orcid.org/0000-0003-3964-7736>

I. Resumen

La gestión pedagógica en las instituciones educativas es una clave fundamental del proceso de transformación en la educación. El propósito del presente trabajo de investigación es analizar la gestión pedagógica de aula a partir de la competencia digital docente desde la aplicabilidad de la seguridad informática en las Unidades Educativas de la provincia de Manabí, república del Ecuador. Para ello, se propone abordar este problema a partir de un enfoque metodológico cualitativo y cuantitativo, participaron como informantes en la recolección de datos docentes, directivos de las instituciones educativas y dos expertos, utilizando como herramienta la encuesta y entrevista. Los resultados señalan que los docentes tienen un bajo interés en usar recursos tecnológicos para desarrollar las habilidades en la tecnología por lo que no están totalmente capacitados y se exponen a riesgos tecnológicos que, si no son identificados y aminorados de manera apropiada, pueden afectar la seguridad de la información. Se concluye que los docentes tienen limitados conocimientos sobre los riesgos que implican los diferentes ataques informáticos y no saben actuar adecuadamente ante estas situaciones, lo que pone en evidencia la vulnerabilidad a la que se enfrentan al hacer uso de medios tecnológicos.

Palabras claves

Gestión pedagógica; competencia digital; vulnerabilidad; seguridad informática.

Abstract

Pedagogical management in educational institutions is a fundamental key to the transformation process in education. The purpose of this research work is to analyze the pedagogical management of the classroom based on the digital teaching competence from the applicability of computer security in the Educational Units of the province of Manabí, Republic of Ecuador. To do this, it is proposed to address this problem from a qualitative and quantitative methodological approach, teachers, directors of educational institutions and two experts participated as informants in the data collection, using the survey and interview as a tool. The results indicate that teachers have a low interest in using technological resources to develop technology skills, so they are not fully trained and are exposed to technological risks that, if not identified and mitigated appropriately, can affect the security of their teaching information. It is concluded that teachers have limited knowledge about the risks involved in different computer attacks and do not know how to act appropriately in these situations, which highlights the vulnerability they face when using technological means.

Keywords

Pedagogical management; digital competence; Vulnerability; Informatic security.

II. Introducción

La sociedad actual, caracterizada por un contexto de globalización y por el rápido crecimiento de las Tecnologías de la Información y la Comunicación (TIC), ha impulsado

la creación de mecanismos para la incorporación de diferentes avances tecnológicos en variados sectores económicos y sociales, fortaleciendo tales escenarios en cuanto a su eficiencia y dinamismo.(De la Hoz Franco et al., 2018)Y el sector educativo no se escapa de esta realidad porque en muchas ocasiones es mal aprovechada a causa del desconocimiento existente en los docentes.

En este estudio se considera que la integración de las TIC en el aula requiere de personas capacitadas en el uso técnico de las tecnologías, pero, sobre todo, en el empleo pedagógico de las mismas. Debido a que existe limitados conocimientos por parte de los docentes frente a escenarios de seguridad informática que incide en la seguridad de la información es necesario que exista una buena gestión pedagógica para que facilite, oriente y coordine las acciones que desarrollan los docentes en los diferentes niveles, y adquieran competencias digitales para no enfrentarse con amenazas graves en los sistemas informáticos.

Desde la posición de (Laje, 2020, p.66) “La Competencia Digital es conocida como un conjunto de habilidades y destrezas que las personas deben obtener al finalizar su formación, para poder estar inmerso en la sociedad actual como lo es la era de la tecnología”

Las competencias entendidas desde el panorama educativo, según lo manifestado por (Lévano-Francia et al., 2019,) son asumidas a manera de instrumentos de gran utilidad permitiendo la movilización de actitudes, conocimientos y procesos; los cuales los estudiantes adquieren habilidades para facilitar la transferencia de conocimientos y generar innovación.

La investigación hace referencia a que existe una alternativa metodológica. En este sentido, (Julio Delgado & Sánchez, 2020, pp,1-13) sostuvo al respecto que la modalidad educativa B-aprendizaje, dirigido a perfeccionar la preparación en seguridad informática del docente, donde se ofrece una estructuración de contenidos en seguridad informática de forma presencial y a distancia con el empleo de Entornos Virtuales de Enseñanza Aprendizaje ayuda a mantener la información segura.

En otra investigación se evidenció que “los proveedores de internet no poseen dispositivos con seguridad para proteger la privacidad de los datos personales” (De la Rosa Rodríguez, 2021, pp,20). Es por eso que el gobierno debe promover una cultura en los ciudadanos e impulsar acciones de protección proporcionándoles el conocimiento necesario para proteger la información que ingresen en la red.

En otro estudio se identificó las prácticas de seguridad de la información en una comunidad universitaria, donde se destaca que tanto los profesores como estudiantes tienen un aceptable conocimiento sobre seguridad de la información, pese a no recibir capacitación significativa por entidades gubernamentales. (David Estrada-Esponda et al., 2021) Estos resultados denotan que la institución realiza un esfuerzo institucional para combatir ese tipo de delitos generando estrategias de sensibilización para promover una mejor higiene digital.

Los estudios señalados sirvieron de base para sustentar la investigación en la importancia que tiene en la actualidad desarrollar, promover, fortalecer, proteger la información digital de los y las docentes de manera continua, por tal razón las instituciones educativas deben contar con un laboratorio implementado con equipos tecnológicos y exista la predisposición de su planta administrativa y, sobre todo, a la

inexistencia de una investigación que aborde los factores vinculados a competencias digitales, factores personales y percepciones de los docentes, es por ellos que urge brindar capacitaciones de información y manejo de seguridad para que profundicen el conjunto de competencias e identifiquen la formación del docente para asumir las condiciones óptimas, las responsabilidades propias del desarrollo de funciones y tareas de su profesión, por lo que “un sistema desprotegido ante ataques es vulnerable, estas debilidades pueden presentarse en cualquiera de los sistemas y su consecuencia son los impactos como efectos nocivos de un evento.”(Peñafiel Lucuy Kevin Andrés, 2021, pp147)

III. Desarrollo

Gestión pedagógica en el aula

Desde la posición de (María A. López Paredes, 2017, pp, 202) la gestión pedagógica tiene como objetivo el encargo social de la educación en el desarrollo integral de la personalidad, esta gestión pedagógica dentro del sistema educacional debe reconocerse como un proceso que facilita la orientación y coordinación de las acciones que despliegan los docentes en los diferentes niveles para administrar el proceso docente educativo en la consecución eficiente de los objetivos que se quieren lograr. “Una gestión adecuada pasa por distintos momentos: diagnóstico, planeación, ejecución, seguimiento y evaluación en concordancia.”(Quispe-Pareja, 2020, pp 8), estos momentos están en constante interacción que ayudan en el proceso de enseñanza, “contribuyendo al desarrollo de la sociedad, propiciando la generación de experiencias teóricas y prácticas que sirvan para el adecuado comportamiento de las personas como integrantes de una comunidad.”(Orihuela Lázaro, 2020,pp, 26)

Competencias digitales para docentes

“Las competencias entendidas desde el panorama educativo, según lo manifestado son asumidas a manera de instrumentos de gran utilidad que permite la movilización de actitudes, conocimientos y procesos”.(Lévano et al., 2019, pp,572) por lo que los docentes adquieren conocimientos para poder transferir a los estudiantes.

“El docente se prepara para adquirir conocimientos, poner en práctica las competencias digitales en beneficio de los estudiantes y atender a la diversidad de aprendizajes en el aula de clases” (Macías Figueroa et al., 2021 pp 291) porque se debe atender a los estudiantes donde ellos desarrollen sus habilidades en la forma integral, para lograr una educación de calidad.

Vulnerabilidad

Las vulnerabilidades en seguridad informática se refieren a la debilidad que poseen los sistemas informáticos los cuales pueden ser utilizados por un agente externo como un hacker o cracker para causar daño, ocasionando malestar en las bases de datos y en la información de carácter privado de la organización.(Sánchez-Gamboa, 2018,pp,27) sin embargo, las políticas o controles de seguridad de la información por sí solos no garantizarán la protección total de la información, los sistemas de información, los servicios o las redes, los controles implementados mitigan los riesgos, pero existe la probabilidad que persistan vulnerabilidades residuales que reducen la efectividad y facilitan la ocurrencia de incidentes de seguridad de la información. (Rodrigo Arturo Proaño Escalante1, 2018,pp,91)

Para lo cual se detallaran las vulnerabilidades informáticas que existen según (Quiroz Zambrano & Macías Valencia, 2017,pp,684) y las diferenciamos en tres tipos de vulnerabilidades según cómo afectan a nuestro sistema:

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al

que afecta y para las cuales ya existe una solución, que se publica en forma de parche. Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa. Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo.

Seguridad informática

“La seguridad informática, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información”.(Figuroa-Suárez et al., 2018, pp, 147) es decir es la encargada de implementar medidas de seguridad para proteger los sistemas informáticos.

Así como los sistemas de información son más amplios y abarcan a los sistemas informáticos, la seguridad de la información es más amplia que la seguridad informática. La seguridad informática se concentra en la protección de los recursos informáticos.

Antiguamente, la información se manejaba sólo en papel por lo que la seguridad era física, pero en la actualidad, además, se maneja de manera electrónica lo que implica que la seguridad se lleve a cabo con un soporte informático.(Sisti, 2019,pp, 19)

Así pues, el principio de seguridad impone al responsable de tratamiento obligaciones de medios, lo que exige la adopción de medidas de seguridad distintas de acuerdo con el tipo de

datos que trate. Pero, para la adopción de dichas medidas es preciso, en el caso ecuatoriano, crear una autoridad de protección de datos personales con capacidades regulatorias que pueda emitir normativa vinculante en aspectos de protección de datos personales (Novoa, 2020, pp, 84)

IV. Metodología

El método de investigación que se aplicó en este trabajo fue el cualitativo y cuantitativo; cualitativo porque se hace una descripción de la información de la entrevista sacando los indicadores que demuestran la importancia de la investigación; lo cuantitativo se sustenta en el planteamiento de la encuesta a los docentes y el análisis estadístico que se hicieron de las mismas, el tipo de investigación que se desarrolló fue de campo y se utilizó el método científico por medio del análisis y síntesis de la información obtenida para responder a los objetivos planteados.

La investigación se realizó en el cantón Montecristi, provincia de Manabí que cuenta con 13 instituciones educativas y una población de 173 docentes debido a que en este distrito solo se establecen 173 docente se acogió la muestra total por el monto básico del número de docentes a quienes se aplicó la encuesta, y 2 expertos en el tema para la entrevista.

V. Resultados y discusión

Encuesta dirigida a docentes

Tabla # 1

Desarrollo activamente mis habilidades de docencia digital

Alternativas	F	%
Rara vez tengo tiempo para mis habilidades de docencia digital.	5	2,9%
Mejoro mis habilidades a través de la reflexión y la experimentación	60	34,7%

Uso una variedad de recursos para desarrollar mis habilidades de docencia digital.	90	52 %
Ayudo a otros compañeros a usar las tecnologías digitales para innovar y mejorar la práctica educativa	18	10,4%

Fuente: Elaboración propia

En los resultados obtenidos en la tabla 1 los docentes exponen que, para el desarrollo de las habilidades de docencia digital, el 52% usan una variedad de recursos por otro lado el 34,7% señalan que mejoran sus habilidades a través de la reflexión y la experimentación. Los datos evidencian que existe interés en los docentes para usar recursos tecnológicos para a utilización de las herramientas digitales que aportan al proceso de enseñanza aprendizaje.

Datos que son corroborados por,(Perón, 2020) “ El trabajo en equipo multiplica las posibilidades para generar conocimientos nuevos y motivar el aprendizaje”

Tabla # 2

¿Conoce usted los riesgos que puede sufrir su computador cuando abre un virus o le hackean su máquina?

Alternativas	F	%
Sí, los conozco completamente	62	36,4%
Si ha escuchado los términos	103	59%
No, los conozco	8	4,6%

Fuente: Elaboración propia

En cuanto a los resultados obtenidos en la tabla 2 exponen el criterio de los docentes respecto a los riesgos que puede sufrir su computador cuando abre un virus o le hackean su máquina, el 36,4% mencionan que, si conocen completamente, por otro lado, el 59% expresaron que si han

escuchado los términos sobre los riesgos de un virus. Estos datos expresan que existe un déficit de conocimiento por parte de los docentes frente a escenarios de seguridad informática. Es por esto que se debe saber más allá de lo básico sobre como instalar medidas de protección (antivirus, antispam, malware, contraseñas seguras, etc.) para preservar vuestros contenidos. Como bien afirma (Ospina Díaz & Sanabria Rangel, 2020) “La ciberseguridad (o seguridad informática) se origina para tomar medidas para la protección de infraestructura, software y hardware, contrarrestando las posibles amenazas mediante internet, y para desarrollar estrategias de contraataque.

Tabla # 3

¿Conoce Ud. los protocolos de seguridad informática para crear claves de seguridad para el ingreso a las plataformas virtuales?

Alternativas	F	%
Sí, los conozco	113	56,6 %
No, los conozco	60	43,4%

Fuente: Elaboración propia

Los resultados de la tabla 3 indican que un 56,6% de docentes conocen los protocolos de seguridad informática para crear claves de seguridad para el ingreso a las plataformas virtuales. Esta información revela que existe un mediano conocimiento sobre la temática lo que es importante saber que la seguridad es primordial para que la información no sea interceptada por nadie, puesto que, al caer en manos de un ente ajeno, puede ocasionar problemas por lo cual siempre se debe dar prioridad a la seguridad. Al respecto (Sistemas et al., 2020) considera que la falta de seguridad en los accesos o también la falta de seguridad en la forma de comunicarse y

traspasar información en vías de internet puede resultar peligroso a tal punto de que los hackers puedan tomar dicha información y seas víctimas de ellos.

Tabla # 4

Entiende usted el significado del término de las políticas de seguridad en relación al uso del computador.

Alternativas	F	%
Sí las entiendo	75	43,4 %
No las entiendo	98	56,6%

Fuente: Elaboración propia

Los resultados obtenidos en la tabla 4 muestran que el 56,6% de los docentes no lo entiende el término de las políticas de seguridad en relación al uso del computador, y por otro lado el 43,4% si lo entienden. Se deduce que los docentes tienen limitaciones sobre políticas de seguridad informática que se debe saber para una declaración de intenciones que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.

Como lo afirma (Bustamante García et al., 2021,pp,71) es importante implantar políticas, normas y procedimientos a fin de prevenir y disminuir los riesgos de pérdida de datos de la organización, ofreciendo información oportuna, clara y veraz.

Para profundizar el estudio fáctico se realizó una entrevista a expertos, se les cuestionó acerca de qué conocimientos tienen sobre competencia digital en la gestión pedagógica indicando que

saben crear contenidos digitales, organizar y analizar la información de acuerdo al objeto que se quiera lograr, además comparten recursos a través de herramientas en línea.

Como señala (Pozos Pérez & Tejada Fernández, 2018) La competencia digital no solo proporciona la capacidad de aprovechar la riqueza de las nuevas posibilidades asociadas con las tecnologías digitales y los retos que plantean, sino que resulta cada vez más necesaria para poder participar de forma sistemática en la nueva sociedad y economía del conocimiento del siglo XXI.

Con relación a la pregunta ¿Tiene usted conocimiento de las diferentes vulnerabilidades que se presentan en las competencias digitales docente con relación a la seguridad informática? Los expertos señalaron que si conocen sobre las vulnerabilidades que existen y estas se pueden dar por el uso inapropiado de los datos de los ciudadanos, la hipervigilancia digital o por la presencia masiva de sistemas operativos o programas informáticos determinados.

Tal como sugiere Álvarez Flores “La incorporación de las tecnologías en todos los ámbitos ha hecho necesario que los usuarios adquieran competencias para su tratamiento, puesto que de forma paralela a los beneficios que aportan los avances tecnológicos se presentan prácticas de riesgo, peligro, moralidad, identidad” (Alvarez-Flores, 2021)

Acerca de la pregunta ¿Utiliza Ud. protocolos de seguridad informática en las competencias digitales de la gestión pedagógica docente? Los expertos señalaron que, si los conocen, y son utilizados en el entorno educativo para poder manejar el internet de la mejor manera y no sufrir ataques que perjudiquen el sistema informático. Este punto de vista se apoya en (Acosta Z. Jennifer Alexandra; Baño N. Freddy Patricio., 2018) que nos indica no es fácil definir el protocolo, sabemos que el protocolo está al servicio del ser humano, no al revés. Lo que significa que, conforme cambia la sociedad humana, y a su ritmo, ha de adaptarse, cambiando, el

protocolo. Protocolo es aquella disciplina que, con realismo, técnica (pues tiene de las tres cosas), determina las estructuras o formas bajo las cuales se desarrolla una actividad humana pluripersonal e importante; con el objeto de su eficaz realización y, en último lugar de mejorar la convivencia.

VI. Conclusiones

Los resultados de la investigación muestran un limitado conocimientos por parte de los docentes frente a escenarios de seguridad informática, los profesores manifiestan conocer brevemente los riesgos que implican los ataques informáticos, sin embargo, no saben actuar adecuadamente antes estas situaciones, lo que pone en evidencia la vulnerabilidad a la que se enfrentan al hacer uso de medios tecnológicos constantemente en el auge de la educación digital en la que nos encontramos.

El estudio evidencia que los docentes conocen sobre los protocolos de seguridad informática al crear claves seguras para ingresar a las plataformas virtuales lo que es importante saber que la seguridad es primordial para que la información no sea interceptada por nadie, en vista de que, al caer en manos de un ente ajeno, puede ocasionar problemas por lo cual siempre se debe dar prioridad a la seguridad.

Por lo tanto, trabajar con tecnología es correr el riesgo de ser vulnerables es porque se debe desarrollar competencias y tomar precauciones básicas de seguridad para no enfrentar amenazas graves en los sistemas informáticos.

VII. Referencias

Acosta Z. Jennifer Alexandra; Baño N. Freddy Patricio. (2018). *Universidad regional autónoma de los Andes uniandes facultad de sistemas mercantiles "protocolo de seguridad*

informática para usuarios en.

<https://dspace.uniandes.edu.ec/bitstream/123456789/8725/1/PIUASIS016-2018.pdf>

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, 12(2), 69–79.

<https://doi.org/10.29019/ENFOQUEUTE.743>

David Estrada-Esponda, R., Luis Unás-Gómez, J., & Oleskyenio, |. (2021). *Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá* *Information Security Practices in Times of Pandemic. Case Universidad del Valle, Tuluá campus* *Práticas de segurança da informação em tempos de pandemia*. 13(3), 98–110. <https://doi.org/10.22335/rlct.v13i3.1446>

De la Hoz Franco, E., Martínez-Palmera, O., Combata-Niño, H., & Hernández-Palma, H. (2018). N° 1-2019 Recibido Abr. *Información Científica*, 30(1), 255–262.

<https://doi.org/10.4067/S0718-07642019000100255>

De la Rosa Rodríguez, P. I. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. *RIDE Revista Iberoamericana Para La Investigación y El Desarrollo Educativo*, 12(23). <https://doi.org/10.23913/ride.v12i23.980>

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, 2(12), 145. <https://doi.org/10.23857/pc.v2i12.420>

Julio Delgado, A., & Sánchez, E. F. (2020). *Certainty of the teacher of the Polytechnician “ Julio Antonio Delgado Introducción*. 1–13.

- Laje, F. J. (2020). La Competencia Digital Docente. Estudio bibliométrico de la producción científica sobre la Competencia Digital del profesorado. *Informes Científicos Técnicos - UNPA*, 12(3), 66–84. <https://doi.org/10.22305/ict-unpa.v12.n3.741>
- Lévano-Francia, L., Sanchez, S., Guillén-Aparicio, P., Tello-Cabello, S., & Herrera-Paico, N. (2019). Competencias digitales y educación Digital Competences and Education. *Z*, 7(2), 569–588. <https://doi.org/10.20511/pyr2019.v7n2.329>
- Levano, L., Sanchez, S., Guillen, P., Tello, S., Herrera, N., & Collantes, Z. (2019). Digital Competences and Education. *Propositos y Representaciones*, 7(2), 569–588. <https://bit.ly/3jDkaQ0>
- Macías Figueroa, F. M., Mendoza Vergara, G. M., Mieles Pico, G. L., & San Andrés Soledispa, E. J. (2021). Competencias digitales del docente para atender a la diversidad de aprendizajes en la pandemia COVID – 19. *Polo Del Conocimiento*, 6(54), 288–306. <https://doi.org/10.23857/pc.v6i1.2142>
- María A. López Paredes. (2017). María A. López Paredes. *Cien*, 3, 201–215.
- Novoa, E. (2020). *El derecho a la protección de datos de personales en la prestación de servicios de cloud computing . Una perspectiva ecuatoriana Introducción*. 22, 64–89.
- Orihuela Lázaro, E. M. (2020). Escuela de Posgrado BIOMETRÍA. *Psikologi Perkembangan*, October 2013, 1–126. <http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/3000/SilvaAcosta.pdf?sequence=1&isAllowed=y%0Ahttps://repositorio.comillas.edu/xmlui/handle/11531/1046>
- Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la

ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2), 199–217.

Peñañiel Lucuy Kevin Andrés. (2021). *Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos*. http://www.scielo.org.bo/pdf/rfer/v21n21/v21n21_a09.pdf

Perón, J. M. R. (2020). Teamwork as a transversal competence of the teaching staff in higher medical teaching. *Revista Cubana de Medicina Militar*, 49(4), 1–14.

Pozos Pérez, K. V., & Tejada Fernández, J. (2018). Competencias Digitales en Docentes de Educación Superior: Niveles de Dominio y Necesidades Formativas. *Revista Digital de Investigación En Docencia Universitaria*, 12(2), 59–87. <https://doi.org/10.19083/ridu.2018.712>

Quiroz Zambrano, S., & Macías Valencia, D. (2017). Computer security: considerations. *Dominio de Las Ciencias*, 3(3), 676–688.

Quispe-Pareja, M. (2020). La gestión pedagógica en la mejora del desempeño docente. *Investigación Valdizana*, 14(1), 7–14. <https://doi.org/10.33554/RIV.14.1.601>

Rodrigo Arturo Proaño Escalante¹, A. F. G. M. (2018). *Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana (Strategy for responding to computer incidents of insecurity set in Ecuadorian law)*. 1, 90–101. <http://ingenieria.ute.edu.ec/enfoqueute/>

Sanchez-Gamboa, H. (2018). Identificación de vulnerabilidades y riesgos en los activos de ti de energitel. *Universidad Nacional Abierta y a Distancia UNAD*, 37–45.

<https://repository.unad.edu.co/handle/10596/28221>

Sistemas, A. De, Milagro, E. De, & Sistemas, A. De. (2020). *Ciencias de la computación*

Artículo de investigación. 6, 835–846.

Sisti, M. (2019). *Seguridad informática: La protección de la información en una empresa*

Vitivícola de Mendoza 2019. 1–86.

CERTIFICACIÓN DE APROBACIÓN

En mi calidad de tutora del maestrante: Marjorie Silvana Delgado Santana, que cursa estudios en el programa de Maestría en Educación Mención Educación y Creatividad, impartido en la Universidad San Gregorio de Portoviejo.

CERTIFICO:

Que he analizado el informe del trabajo científico en la modalidad: **Artículo científico** con el título: **Seguridad informática: Competencia digital docente en la gestión pedagógica de aula**, presentado por el maestrante Marjorie Silvana Delgado Santana, con cédula de ciudadanía No. **131192702-2**, como requisito previo para optar por el Grado Académico de Magíster en Educación Mención Educación y Creatividad. El trabajo científico ha sido postulado en la revista: **Rehuso revista de Ciencias Humanísticas y Sociales** con fecha **16 de mayo del 2022**. Considero, reúne los requisitos y méritos suficientes necesarios de carácter académico y científico, por lo que lo apruebo.



Tutor: Sonia Monserrate Párraga Muñoz

Portoviejo, 16 de mayo del 2022.