DOI: https://doi.org/10.46502/issn.1856-7576/2023.17.04.4
Cómo citar:
Edel Navarro, R., & Pérez Castillo, N. (2023). Competencias digitales en administrativos de un instituto politécnico Uso de TICCAD para la seguridad informática institucional. Revista Eduweb, 17(4), 30-42. https://doi.org/10.46502/issn.1856-7576/2023.17.04.4

Competencias digitales en administrativos de un instituto politécnico Uso de TICCAD para la seguridad informática institucional

Digital skills in administrators of a polytechnic institute Use of TICCAD for institutional computer security

Rubén Edel Navarro
https://orcid.org/0000-0002-7066-4369
Sistema Nacional de Investigadoras e Investigadores del Consejo Nacional de Humanidades, Ciencia y Tecnología (SNII-CONAHCYT). Miembro, México.
Nieves Pérez Castillo
https://orcid.org/0000-0003-0786-1762
Maestra Técnico Profesional (Ministerio de Educación) de República Dominicana, República Dominicana.

Recibido: 12/04/23
Aceptado: 25/07/23

Resumen

Las conductas dirigidas a garantizar la seguridad informática forman parte del perfil de competencias profesionales indispensables en los empleados administrativos de las instituciones de educación superior (IES). La investigación planteó como objetivo identificar las competencias digitales de empleados administrativos para el uso seguro de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en un Instituto Politécnico de Santiago, República Dominicana. Se realizó un estudio cualitativo con abordaje hermenéutico-dialéctico. Participaron 13 empleados administrativos seleccionados con muestreo teórico, a quienes se les aplicó un cuestionario con preguntas abiertas. La reducción de datos identificó las categorías emergentes: a) seguridad informática y buen uso de las tecnologías, b) penetración-hackeo de información, c) dificultades para usar tecnología y d) alfabetización digital. Los participantes poseen conocimientos básicos sobre seguridad informática y se identificó vulnerabilidad en el sistema de seguridad institucional que afecta los procesos administrativos y estimula prácticas administrativas inadecuadas. Existe un nivel moderado en competencias digitales y bajo conocimiento sobre herramientas para la ejecución de tareas administrativas, en contraste, un alto uso de redes sociales en horario laboral. Se concluye la necesidad de capacitar-entrenar en competencias digitales para instaurar comportamientos informáticos seguros y, por tanto, mayor efectividad en los procesos administrativos institucionales.

Palabras clave: competencia digital, educación, seguridad informática.

Abstract

The behaviours aimed at guaranteeing computer security are part of the profile of essential professional competencies in administrative employees of higher education institutions (HEIs). In accordance with the above, the objective of this research was to identify the digital skills of administrative employees for the

safe use of digital information, communication, knowledge and learning technologies (TICCAD) in the Polytechnic Institute of Santiago, Dominican Republic. To achieve the above, a qualitative study was carried out, through a hermeneutic-dialectical approach. The participants were 13 administrative employees selected through a theoretical sampling, to whom a questionnaire with open questions was applied, elaborated from deductive categories, and validated by experts. The information analysis process was carried out by a categorization system, with which it was possible to identify the emerging categories of, a) computer security and good use of technologies, b) penetration or hacking of information, c) difficulties with the use of technology and d) digital literacy. The results postulate that the participants have basic knowledge of computer security, however, vulnerabilities are identified in the institutional security system that affect administrative processes and stimulate inadequate administrative practices. A moderate level is determined in the digital skills of the employees, with a low level of knowledge about tools for the execution of administrative tasks, in contrast to the high use of social networks during working hours. It concludes with the need to train-train in digital skills to establish safe computer behaviors and, therefore, greater effectiveness in institutional administrative processes.

Keywords: computer security, digital competence, education.

1. Introducción

Las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) son herramientas imprescindibles en los distintos procesos que se llevan a cabo en las instituciones educativas en sus diferentes niveles. Sin embargo, si bien estas cumplen con una importante función en los procesos de aprendizaje a través de la relación docente-estudiante, también son fundamentales para el desarrollo de las diversas actividades administrativas que se llevan a cabo en las instituciones de educación superior (IES). Según indica Tapia (2020) las tecnologías en los centros de enseñanza cumplen con la función de mejorar la productividad y eficiencia requeridas para la gestión administrativa, simplificando las tareas y ampliando la capacidad de comunicación y cooperación entre los miembros del equipo de docentes y administrativos. La gestión administrativa comprende diversos procesos relacionados con la función académica, tales como matrículas, procesamiento de calificaciones, actas de grado, solo por citar algunas, las que deben caracterizarse por su confidencialidad y la precisión en el manejo de información y datos, además de garantizar la seguridad en virtud de la probable intervención de agentes externos que vulneren los sistemas y alteren el correcto y ético funcionamiento de los procesos académico-administrativos institucionales. Para Anchelia-Gonzales et al., (2021) la gestión administrativa en las instituciones educativas comprende aquellas tareas que son ejecutadas para cumplir los objetivos de dicha institución, entre los cuales se menciona la planificación del curso escolar, delimitación de funciones, procesos financieros, administración de la planta física y, en especial, el manejo de la data académica de cada estudiante. De lo anterior se puede afirmar que los procesos administrativos en las instituciones educativas se articulan en una amplia dinámica institucional que incluye "desde la relación del centro con su medio, asignación de tareas y la organización para la enseñanza, hasta el manejo del personal y las demandas administrativas del plantel" (Anchelia-Gonzales et al., 2021, p.5).

2. Referentes teóricos o revisión de literatura

Las tareas de gestión y administrativas son ejecutadas con mayor eficiencia cuando existen competencias digitales en los empleados que llevan a cabo los procesos mediados por las tecnologías; en tal sentido, Martínez-Alvarez (2020) postula que una adecuada gestión administrativa se relaciona positivamente con la integración de las TICCAD y las habilidades del personal en el manejo de estas. Desde la perspectiva de Ticona (2022), si bien el desempeño laboral de los empleados administrativos universitarios mejora gracias a la incorporación de las tecnologías, también se evidencia que la convivencia digital y la tecnología son moderadamente importantes para los empleados, lo cual indica que no existe aún una completa

valoración de la relevancia de las habilidades digitales en su quehacer diario. Las competencias digitales constituyen capacidades en el empleo de los medios informáticos para la recuperación, procesamiento y evaluación de la información para cumplir con los objetivos requeridos, las cuales se adquieren en un proceso de formación y capacitación dirigido a promover un adecuado grado de análisis, razonamiento, alfabetización y comunicación fluida en las diferentes áreas de aplicación de las tecnologías (Reche et al., 2019); dichas competencias implican indudablemente el conocimiento e implementación de las medidas de seguridad informática que permitan controlar las distintas vulnerabilidades que pueden afectar los datos de la institución.

Es importante enfatizar que, si bien los distintos actores en las IES requieren adoptar un modelo informático seguro y competente, en el área administrativa estas medidas son imprescindibles en virtud de que se vinculan, no solo con el control académico, sino con aspectos financieros y organizacionales. La seguridad informática consiste en los procesos de protección que se realizan en un sistema informático, lo que implica una diversidad de acciones, entre las que se destacan el respaldo de datos, disponibilidad de la información, confidencialidad del usuario e integridad, brindando garantía de que los datos no sean manipulados por terceros (Gaitán, 2020).

Para el caso de los procesos administrativos, los datos informáticos pueden ser objeto de distintas amenazas, cuyo fin es la apropiación de información o su manipulación, lo cual afecta el óptimo desenvolvimiento de la gestión institucional. Para lograr la vulneración de la información existen distintas modalidades entre las más frecuentes se encuentran el robo de identidad y la obtención de contraseñas e intercepción de mensajes, entre otras, conocido como penetración o *hackeo* de información (Chiliquinga, 2020). A lo anterior habrá que acotar que, según destaca Narváez (2019) la mayoría de las amenazas a la seguridad informática en las organizaciones se deben a omisiones y descuidos atribuibles al factor humano, como compartir equipos y contraseñas, dispositivos de almacenamiento o no cerrar sesiones de forma segura.

Al respecto, Baca (2016) destaca la importancia de que los datos se manejen de forma efectiva, con disponibilidad y apego a los estándares de seguridad, como el control de acceso, autenticación o verificación de identidad de usuarios y/o sitios de *internet*, antes de realizar cualquier transacción y envío de información. Las IES no solo deben contar con que todos sus actores sean competentes digitalmente y apliquen las medidas de seguridad informática, sino poseer mecanismos tecnológicos que garanticen un entorno seguro.

De acuerdo con Gaitán (2020) las actividades tecnológicas en las instituciones educativas suelen realizarse a través de dispositivos en red que vinculan distintos sistemas electrónicos como computadoras, *routers*, *red lan*, *wan*, *man*, repetidores, servidores, lo que permite a través de *internet* tener acceso a las redes instaladas en los diferentes departamentos de la organización. Es recomendable que se implementen programas y *softwares* institucionales que garanticen la protección y seguridad a los usuarios en línea, aun y cuando esto también se asocie a una mayor inversión por parte de la institución (Chiliquinga, 2020).

Es precisamente el factor económico el que permite que las diversas IES no posean los *softwares* y equipos necesarios para garantizar la seguridad digital, dejando estas medidas de seguridad en manos de los usuarios, razón por la cual puede afirmarse que tanto estudiantes, docentes como empleados administrativos deben ser competentes digitalmente para asegurar las vulnerabilidades a las cuales están expuestos los datos. Marín et al., (2021) señalan que es fundamental que las competencias digitales a desarrollar en los actores educativos incluyan componente clave, tales como información y alfabetización informacional, comunicación y colaboración, creación de contenidos digitales, seguridad y resolución de problemas. Por otra parte, Zambrano y Valencia (2017) señalan que el empleo seguro de las TICCAD implica competencias que garanticen proteger los recursos de los riesgos o ataques informáticos, además del cuidado de los datos confidenciales de la institución, lo cual conlleva a un comportamiento académico

y ético cuyas dimensiones cognitiva, procedimental y actitudinal contemplan las medidas de seguridad informática para el manejo apropiado y socialmente aceptable de las TICCAD.

El empleo seguro de las TICCAD debe ser suficientemente afianzado en los procesos de formación del personal docente y administrativo de las instituciones educativas, tomando en cuenta que en estos equipos se integran diferentes perfiles profesionales juntamente con el modelo pedagógico específico, razón por la cual es fundamental la supervisión escolar para su adecuado desarrollo (Bonilla y Ferra, 2021). De tal manera que uno de los aspectos que se destacan en las instituciones educativas es la necesidad de integrar los valores de la responsabilidad personal y la responsabilidad institucional relacionados con la seguridad informática (Pérez, 2018); para ello se requiere establecer tanto medidas como modelos de mediación que permitan identificar como cada actor educativo percibe o incorpora los valores inherentes a la seguridad de los datos personales y compartidos. Las mediaciones tecnológicas deben estar contenidas en las normas y valores institucionales, pero adicionalmente, la conducta de cada individuo debería ser monitoreada a través de una planeación educativa institucional que permita un buen desempeño en materia de ciber-seguridad. Lo anterior armonizando que, en materia de seguridad institucional, las competencias digitales individuales y los objetivos institucionales deberían estar articulados. Cabe destacar lo postulado por Baca (2016), acerca de la efectividad de la prevención del riesgo informático en la institución dependerá del costo de inversión, de los aparatos electrónicos y del personal calificado para manejar adecuadamente el sistema tecnológico en la institución. Lo anteriormente expuesto destaca la interrelación relevante entre los distintos actores educativos y las instituciones, sin descuidar las políticas educativas que permitan alcanzar las necesarias competencias digitales para desarrollar entornos informáticos seguros. Las TICCAD en una institución de educación superior no solo se aplican en los procesos de enseñanza-aprendizaje, sino que conforman un sistema operativo que permite que la institución funcione con eficiencia, por tal motivo, las políticas educativas integran a todo el personal en el proceso de adopción de las competencias digitales. En la República Dominicana el programa de transformación digital en las instituciones educativas comienza con la implementación del proyecto República digital en el 2017, proporcionándole a todo el personal docente, directivos y estudiantes computadoras o tabletas; de igual forma la integración de profesionales expertos en tecnología asignados a los centros educativos desempeñándose como tutores y facilitadores para capacitar al personal impulsando la apropiación de las TICCAD. El programa de transformación digital fue impulsado por el Ministerio de Educación (MINERD), Programa de las Naciones Unidas para el Desarrollo (PNUD), Acción Empresarial por la Educación (EDUCA) y Asociación Dominicana de Rectores Universidades (ADRU). Dentro de las capacitaciones a nivel nacional se destacan la formación en competencias tecnológicas para la práctica docente y las metodologías necesarias para la educación a distancia. Este programa se implementa además por causa de la pandemia COVID-19 obligando a toda la nación a trabajar el año escolar 2020-2021 totalmente virtual (García et al., 2019). En este contexto, el interés de la investigación se enfocó en identificar las competencias digitales de un grupo de empleados administrativos en un Instituto Politécnico en la República Dominicana y, como las citadas competencias, garantizaban la seguridad informática de la institución. En tal sentido, se planteó como objetivo principal del estudio valorar las competencias digitales de empleados administrativos para el uso seguro de las TICCAD en el Instituto Politécnico.

3. Metodología

El desarrollo de la investigación se abordó bajo paradigma sociocrítico, considerando las diferencias epistemológicas entre las ciencias sociales y naturales que permiten suponer que la realidad social es construida y no está determinada por relaciones causales, como es el caso de las ciencias naturales (Ibáñez, 2009). En el tenor anterior, se relaciona también con los enfoques que sustentan el objeto de estudio, es decir, las perspectivas constructivista y conectivista que contemplan que los aprendizajes están mediados por las interacciones sociales y tecnológicas (Hernández-Sampieri et al, 2016). El estudio se fundamenta también en el método hermenéutico-dialéctico, el cual se caracteriza por la posibilidad de establecer interpretaciones de la información y de este modo lograr la comprensión de los significados

(Martínez-Miguelez, 1996). Desde la perspectiva teórico-conceptual descrita, la investigación se propuso una interpretación de las competencias digitales para el uso seguro de la TICCAD con fines educativos en los empleados administrativos de la institución en estudio.

Contexto de estudio

La investigación se realizó en un Instituto Politécnico ubicado en Santiago, República Dominicana, institución pública que tiene como objetivo la formación de técnicos profesionales capacitados para integrarse al proceso productivo de la nación en las áreas de *informática*, *turismo*, *contabilidad*, *mercadeo* y *enfermería*. Los estudiantes de las áreas técnicas oscilan en las edades de 14 años para 4º grado, 15 años para 5º grado y 16 años para 6º grado.

La institución educativa atiende generalmente a estudiantes que pertenecen a familias de bajos recursos socioeconómicos; los jóvenes al ser contratados en sus respectivos centros de pasantías pueden cubrir sus propios gastos para iniciar su carrera universitaria o ser microempresarios, lo cual les permite apoyar a sus familias. Cabe destacar que el instituto está ubicado en un área rural en el cual prevalece una población juvenil, menor de 30 años.

Participantes

Actualmente la institución educativa cuenta con 40 docentes en distintas áreas. La población estudiantil la constituyen 620 estudiantes de los diferentes niveles educativos y 13 empleados administrativos. De acuerdo con los objetivos del estudio, la selección de los *informantes clave* se enfocó en el personal administrativo. El personal administrativo proviene de diferentes comunidades, su experiencia institucional se identifica en el rango de 6 meses a 23 años de servicio. Sus conocimientos académicos son diversificados con títulos de Licenciatura, Maestría y Bachilleres y sus salarios se establecen con base en sus niveles de titulación. Para la investigación se consideró como *informantes clave* a toda la nómina de empleados administrativos, es decir, a 13 empleados, quienes fueron seleccionados bajo un criterio de muestreo teórico, análogo al muestreo no probabilístico de carácter intencional, lo cual indica que no se establecieron procedimientos de muestreo (Hernández-Sampieri et al., 2016). Cabe destacar que todos los participantes contaron con un consentimiento informado.

Categorías deductivas

Para los fines de la investigación y de acuerdo con los objetivos de esta, se estableció un sistema de categorías deductivas para la reducción de datos, siguiendo lo propuesto por Cisterna-Cabrera (2005) lo que permitió definir los temas a abordar a partir de la información teórica recopilada en forma preliminar. Las categorías se describen en la siguiente tabla.

Tabla 1
Categorías deductivas.

OBJETIVO	CATEGORÍAS	SUBCATEGORÍAS
Identificar las competencias digitales de empleados administrativos para el uso seguro de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en un Instituto Politécnico.	**COMPETENCIA DIGITAL** Dominio cognitivo, procedimental y actitudinal de las TICCAD que garantizan su empleo seguro, crítico y creativo de los procesos educativos (Edel, 2020)	**Dimensión cognitiva** Apropiación de las TICCAD relacionada con las destrezas, saberes, conocimientos y habilidades de pensamiento (Edel & Ruiz, 2022) **Dimensión procedimental** Apropiación de las TICCAD acerca de su empleo, uso, usabilidad, utilización, aplicación e implementación (Edel & Ruiz, 2022) **Dimensión actitudinal** Apropiación de las TICCAD en virtud de los actos, conductas, disposición, comportamiento y aceptación (Edel & Ruiz, 2022)
	USO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIÓN, CONOCIMIENTO Y APRENDIZAJE DIGITALES (TICCAD) Comportamiento académico y ético cuyos componentes cognitivo, procedimental y actitudinal contemplan las medidas de seguridad informática para el manejo apropiado y socialmente aceptable (Silva, & Miranda, 2020)	**Comportamiento académico ante las TICCAD** Conductas y destrezas escolares para el apoyo-colaboración y dirección-influencia que fortalecen los conocimientos (Balderas et al, 2021) **Comportamiento ético ante las TICCAD** Conductas y destrezas para proteger la privacidad en línea y la libertad de expresión (Balderas et al., 2021) **Medidas de seguridad informática** Percepción del docente o estudiante en cuanto al nivel de las medidas de seguridad informática que emplea para realizar sus trabajos habituales (Balderas et al, 2021) **Manejo apropiado y socialmente aceptable de las TICCAD** Percepción en cuanto al nivel de manejo y destrezas de las TICCAD (Balderas et al, 2021)

Instrumentos de recolección de datos

Se emplearon cuestionarios con preguntas abiertas elaborados a partir de las categorías deductivas, conformados por 10 preguntas abiertas, las cuales se validaron por juicio de expertos y fueron sometidas a una prueba piloto a fin de verificar la comprensión de su contenido.

Análisis de información

El proceso para en análisis de la información se realizó mecánicamente por medio de un procedimiento de análisis de categorías emergentes derivadas de los cuestionarios (Monje, 2011). Para lo anterior se realizaron las codificaciones abierta, axial y selectiva que permitieron la definición de las categorías emergentes que se exponen en el siguiente apartado. De manera posterior se llevó a cabo la triangulación

entre instrumentos, referentes teórico-conceptuales y evidencia empírica de los investigadores, perfilándose los resultados del presente estudio.

4. Resultados y discusión

En la próxima tabla se describen las categorías emergentes y las subcategorías identificadas, en la recolección de información y datos, a través de la aplicación de los cuestionarios a los 13 empleados administrativos de la institución.

Tabla 2.
Categorías emergentes personal administrativo

CATEGORÍAS	SUBCATEGORÍAS
SEGURIDAD INFORMÁTICA Y BUEN USO DE LAS TECNOLOGÍAS	▪ Verificación de fuente. ▪ Trabajo manual para evitar penetración de información institucional. ▪ Violación de privacidad. ▪ Distracción.
PENETRACIÓN O HACKEO DE INFORMACIÓN	▪ Intercepción de correo electrónico. ▪ Pérdida de usuario y contraseña. ▪ Riesgo de pérdida de información. ▪ Contraseñas con vulnerabilidad. ▪ Manipulación de dispositivos electrónicos.
DIFICULTADES PARA EL USO DE TECNOLOGÍA	▪ Brecha digital. ▪ Docentes con tecnofobia. ▪ Dificultad para el manejo de Moodle. ▪ Conexión inestable *internet*, electricidad, telefonía.
ALFABETIZACIÓN DIGITAL	▪ Navega en *internet*. ▪ Realiza descargas de aplicaciones y documentos. ▪ Manejo de documentos en línea. ▪ Manipula su cuenta en línea con contraseña segura.

Seguridad informática y buen uso de las tecnologías

Todos los miembros del personal administrativo entrevistados afirman que el uso de la tecnología en la institución está asociado con el conocimiento de medidas de seguridad que garantizan la privacidad y confidencialidad de los datos personales e institucionales.

Considerando que los *informantes clave* son profesionales encargados de los procedimientos administrativos en la institución educativa, lo que implica actividades académicas, financieras y de infraestructura, entre otras, uno aspecto que destaca en los resultados es que diversas actividades no se realizan *online*, para evitar la posible penetración de los datos institucionales, particularmente porque la institución está afiliada a *internet* a través de un servidor manejado por una empresa privada con alta vulnerabilidad de datos e información. Debido a que los empleados conocen que existen vulnerabilidades, la mayoría de los participantes señala que prefieren garantizar el acceso seguro a través de sitios confiables cuando es necesario consultar información, los que identifican con un *candado* o páginas oficiales de fácil discriminación. Sin embargo, indican que el riesgo de emplear *internet* no es únicamente la posibilidad de que se vulnere la seguridad si no se conocen las medidas pertinentes, sino que esta herramienta es usada de forma excesiva por algunos compañeros durante su tiempo laboral para conectarse a las redes sociales, fomentando la distracción del trabajo. En este sentido, en algunas respuestas se logró identificar que el excesivo tiempo dedicado a las redes sociales no solo redunda en poca eficiencia laboral, sino que es también un problema de seguridad informática que puede afectar el buen uso de la tecnología en el

tratamiento de la información de la institución, ya que, al emplearse las computadoras institucionales para estos fines, las contraseñas pueden quedar expuestas.

Penetración o hackeo de información

La mayoría de los empleados administrativos conoce los riesgos de penetración de la información cuando no se toman medidas seguras; sin embargo, en las respuestas a los cuestionarios realizados se pudo conocer que dos entrevistados desconocen cómo puede llevarse a cabo el *hackeo* de información personal o institucional, lo cual se considera una conducta de riesgo informático que denota un nivel bajo de competencia digital. Tal y como se indicó en la categoría anterior, la mayoría de los participantes concuerda en que existen vulnerabilidades en el uso de los dispositivos tecnológicos de la institución que pueden permitir la penetración de la información que se maneja internamente, razón por la cual se evita el uso de la red para determinados procesos. Debe tomarse en cuenta que para cualquier institución educativa la seguridad de la información académica es prioritaria, y al no existir un *software* seguro, optan por llevar a cabo las actividades de forma tradicional, tal y como ocurre en el área de coordinación. Sin embargo, para algunos participantes esta medida no evita la penetración de la información, ya que es necesario en primer lugar un conocimiento claro de que se está potencialmente expuesto a través de la conexión del celular o la computadora, y en segundo lugar, que la inexistencia de un sistema institucional de seguridad informática permite que estas vulnerabilidades se mantengan.

En este sentido, un aspecto señalado por los entrevistados es la penetración de los correos electrónicos que permite ingresar a información personal. Estas situaciones se generan especialmente por olvidos involuntarios de usuario y contraseña, o cuando estos datos quedan expuestos en las computadoras que se manejan en las áreas administrativas. Asimismo, indican que existen contraseñas con vulnerabilidad, que pueden ser fácilmente ingresadas por terceras personas. Por tanto, en esta categoría la mayoría de los participantes indican que el sistema informático institucional es susceptible a hackeo o penetración de la información, ya sea por descuidos personales o por falta de *software* de seguridad.

Dificultades para el uso de tecnologías

En este grupo se identificó una categoría asociada a las dificultades para usar tecnologías. De forma objetiva, los empleados administrativos señalan que al no estar directamente vinculados con el proceso académico han podido observar distintas problemáticas en cuanto al uso de las TICCAD. Como elemento resaltante, seis de los trece empleados, destacan que el nivel de conocimiento y apropiación de las tecnologías no es suficiente para la labor administrativa que realizan, por lo cual es necesario recibir mayor capacitación en esta área. Esto también se asocia al uso de sistemas manuales en lugar de los procesos automatizados, lo que conlleva a que los procedimientos sean más lentos. Cabe destacar que en la categoría *seguridad informática* se destacaba que estos procedimientos se realizan para evitar penetraciones de agentes externos, pero en los resultados se evidenció que las bajas competencias digitales en algunos de los participantes es también un factor que se asocia a esta problemática, por lo cual puede afirmarse que el recurso manual no es solo una medida de seguridad sino un comportamiento producido por bajos niveles de competencias digitales en algunos empleados. Desde el punto de vista institucional, los participantes también destacan que la conexión inestable a *internet* y a la energía eléctrica, así como la poca señal en la telefonía celular, inciden negativamente tanto en los procesos académicos como en la ejecución de los procesos administrativos, así que de manera general la adaptación tecnológica no es completamente efectiva en la institución. Esta situación estructural, aunado a las escasas competencias digitales en un grupo de los empleados administrativos se relacionan con vulnerabilidades a la seguridad y poca eficiencia en los procedimientos.

Alfabetización digital

Uno de los principales valores de la alfabetización digital es garantizar la seguridad informática, a través de descargas seguras de aplicaciones y documentos, así como el uso de páginas confiables y los procedimientos que garantizan que estas aplicaciones son útiles y seguras, conductas que varios de los participantes realizan. Otro de los valores importantes que indican la alfabetización digital son las acciones para la navegación en *internet*, no solo en cuanto a seguridad de los datos sino en cuanto a la verificación de las fuentes, aspecto también reportado por los entrevistados. Sin embargo, la alfabetización digital también evidencia las competencias digitales para el manejo de documentos administrativos y la información institucional. En este sentido, los empleados reportan un manejo muy limitado de herramientas de uso administrativo, y en su lugar generalizan distintos tipos de aplicaciones como útiles para su labor, destacando como las más usadas las siguientes: *internet*, redes sociales, pantallas digitales, *WhatsApp* y herramientas de *office* (sin precisar cuáles).

En líneas generales, en esta categoría se destaca nuevamente la necesidad de la capacitación y formación digital para lograr mejores destrezas en el trabajo eficiente, especialmente en cuanto a la importancia de los protocolos para el manejo de documentos en línea, como los formularios, en los cuales puede quedar expuesta información importante. Por ello mencionan la necesidad de tener competencias digitales que les permita la utilización de documentos en red aseguradas por el propietario y los usuarios con permiso de edición.

5. Discusión

Al analizar las categorías emergentes en los participantes del estudio, se logró apreciar que la seguridad informática constituye una prioridad, ya que consideran la necesidad de evitar que la información administrativa sea penetrada por terceros. Los empleados administrativos de la institución en estudio utilizan formas de prevención básicas, como el uso de contraseñas seguras, evitar las redes *wifi*-abiertas y uso de antivirus. Evidentemente, la seguridad informática es uno de los elementos prioritarios en el desarrollo de competencias digitales en toda institución educativa y son habilidades mínimas que permiten lograr una adecuada y efectiva interacción en el ámbito de aprendizaje y laboral (Revelo et al., 2018). La verificación de las fuentes es otra de las estrategias fundamentales para prevenir las vulnerabilidades en la red por acceso a páginas inseguras. Sin embargo, de acuerdo con lo identificado, existen distintas vulnerabilidades en la institución, debido a que se comparten equipos y se accede a una red abierta, lo cual permite que las contraseñas queden expuestas y sea posible el hackeo de la información o el robo de datos confidenciales. El factor humano es uno de los principales problemas para la obtención de datos, robo de identidad, intercepción de mensajes y pérdida de información, según ha identificado Narváez (2019), lo cual evidencia la necesidad de que la institución realice una inversión en *software* y equipo que permita asegurar el acceso a los equipos tecnológicos y de esta manera garantizar la efectividad de los procesos, recomendación realizada por Chiliquinga (2020) para garantizar el uso seguro en las organizaciones.

En este mismo aspecto, cabe destacar que los empleados administrativos están conscientes de la posibilidad de penetración de los datos, y destacan que tanto las características del *internet* de la institución como los equipos compartidos son inadecuados para garantizar la seguridad ya que existen muchas vulnerabilidades detectadas. Por este motivo han preferido llevar a cabo actividades manualmente y reducir los procesos automatizados para evitar penetraciones en la información interna. Esto evidencia los riesgos en seguridad informática existentes en la institución y permite considerar que aun y cuando los actores institucionales tienen claras las medidas de prevención en seguridad informática, existen fallas institucionales para proporcionar un entorno digital más seguro. En su investigación, Pons (2018), manifiesta que la responsabilidad en la ciberseguridad procura la protección individual y colectiva ante cualquier ataque informático en sus diferentes modalidades. Sobre la base de esta idea, esta

responsabilidad implica una diversidad de acciones que no solo se limitan al entorno institucional sino también al ámbito personal y familiar, tomando en cuenta que las tecnologías están llamadas a satisfacer necesidades personales, educativas o laborales que se articulan tecnológicamente. Por tanto, todos los actores de la institución educativa están implicados en el cumplimiento de las normativas de seguridad que son requeridas y sancionadas legalmente en el país, tal y como destaca el Artículo 5 de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología:

El hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

El hecho de que la seguridad informática está sancionada legalmente indica que las competencias digitales no solo se refieren al buen uso de la tecnología, sino a la conducta responsable en las redes y en el acceso a los datos. Por tanto, no solo se trata de sustituir el uso de la tecnología por el recurso manual como una forma de garantizar la seguridad, sino de enfatizar que todo proceso que implique la penetración y mal uso de la información institucional es considerado un delito. A pesar de que los empleados administrativos poseen conocimientos sobre seguridad informática, sus competencias digitales se ubican en niveles moderados a bajos, condición consistente con lo postulado por Ticona (2022), quien ha encontrado que si bien el desempeño laboral de los empleados administrativos en instituciones de educación ha mejorado gracias a la incorporación de las tecnologías, también se evidencia que sus habilidades en el manejo digital no son suficientemente evidentes en los empleados para un óptimo funcionamiento laboral. Según informan los empleados administrativos, existen las competencias instrumentales para el manejo de documentos, sin embargo, las limitaciones en cuanto a la seguridad informática que posee la institución están incidiendo negativamente en un uso más extendido de las tecnologías para la optimización de los procesos administrativos que se llevan a cabo manualmente.

Por otro parte, no existen conocimientos, ni destrezas en el manejo de aplicaciones pertinentes para tareas administrativas, de manera genérica se refiere internet, redes sociales, aplicaciones de mensajería y herramientas de *office*, como las alternativas de uso administrativo. Al respecto, puntualizar lo señalado por George (2020) acerca de que la alfabetización digital en personal administrativo se refiere a las competencias básicas para elaborar y procesar de forma eficiente documentos a través de los medios digitales. En este sentido, los empleados administrativos requieren un mayor nivel de competencias que permitan el acceso seguro a documentos, especialmente de *office* y a la utilización de documentos en red, como las herramientas de *google-docs* y *Google-drive* para garantizar la efectividad de su labor. Cabe mencionar que en los resultados también se destaca que el uso de las redes sociales con fines recreativos es una problemática que afecta el desarrollo de las actividades administrativas, ya que hay un uso extendido de estas a través de los celulares y computadoras, lo cual es corroborado al momento de informar que las redes sociales y mensajería *whatsapp* son las herramientas más utilizadas por los empleados. Un resultado similar fue identificado en la investigación realizada por Rosario y Ruiz (2018) al mostrar en un grupo de empleados administrativos de instituciones públicas y privadas en Puerto Rico el uso excesivo de las redes sociales tanto en hogar como en el trabajo, lo cual interfiere en las actividades laborales.

6. Conclusiones

Los empleados administrativos de la institución educativa requieren mayores competencias digitales que permitan la eficiencia en los complejos procesos administrativos que realizan, lo anterior confirma lo postulado por Martínez-Álvarez (2020) al referir que una adecuada gestión administrativa se relaciona positivamente con la integración de las TICCAD en los distintos procesos. Si bien los empleados refieren cumplir con conductas de seguridad informática, dicho comportamiento organizacional no se articula con

procesos digitalmente pertinentes, por lo que no es factible alcanzar la seguridad informática requerida en los lineamientos institucionales.

De acuerdo con lo anterior, la institución requiere de erradicar el empleo indebido de la tecnología, lo cual se asocia principalmente con el uso excesivo de redes sociales, la sustitución de procesos automatizados por procesos manuales y el conocimiento básico de procedimientos en la penetración de datos, los cuales restan efectividad a los procesos administrativos. Hay que destacar en lo anterior, que también las acciones de la institución educativa deberán incidir en los procesos de capacitación del personal administrativo, la incorporación de tecnología y *software* necesarios para lograr la articulación entre la seguridad informática, las competencias digitales de los empleados, y la expectativa para su adecuado funcionamiento.

A manera de epílogo, se postularía abordar la integridad informática institucional a través a) del diseño de un plan de capacitación profesional para personal administrativo con el propósito de fortalecer sus competencias digitales, b) generar un plan de seguridad informática institucional que contemple la implementación de *software* para manejo y protección de datos, c) concientizar acerca del uso moderado de las redes sociales en el entorno laboral y finalmente d) diseñar un programa integral que estimule buenas prácticas para el empleo de las tecnologías de empleados, docentes y estudiantes.

7. Referencias bibliográficas

Anchelia-Gonzales, V., Inga-Arias, M., Olivares-Rodríguez, P., & Escalante-Flores, J. L. (2021). La gestión administrativa y compromiso organizacional en instituciones educativas. *Propósitos Y Representaciones*, 9 (SPE1), e899. Recuperado de: https://doi.org/10.20511/pyr2021.v9nSPE1.899

Baca, G. (2016). *Introducción a la Seguridad Informática*. México: Grupo Editorial Patria.

Balderas, J., Roque, R., López, A., Salazar, R., & Juárez, C. (2021). ¿Cómo cambió la enseñanza-aprendizaje de las asignaturas prácticas en el área de tecnologías de la información con la covid-19? RIDE. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 11(22), e06. Recuperado de: https://doi.org/10.23913/ride.v11i22.826

Bonilla, K., & Ferra, G. (2021). Comunidades virtuales e innovación: propuestas desde la asesoría técnica pedagógica en la escuela telesecundaria. *IE Revista de Investigación Educativa de la REDIECH*, 12, e1102. Recuperado de: https://www.redalyc.org/articulo.oa?id=521665144003

Cisterna-Cabrera, F. (2005) Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa. *Theoria*, 14(1), 61-71. Recuperado de: http://www.ubiobio.cl/theoria/v/v14/a6.pdf

Chiliquinga, W. (2020). *Arquitectura para la gestión de datos en un campus inteligente*. (Tesis Doctoral en Matemáticas). Universidad de Alicante, España. Recuperado de: https://dialnet.unirioja.es/servlet/tesis?codigo=282625

Edel, R. (2020). Entre saberes, competencias y habilidades digitales ¿en dónde estamos las y los docentes? *Conferencia del 6º Encuentro universitario de mejores prácticas en el uso de TIC en la educación: Reinventar la docencia, juntos y a la distancia*. UNAM, México. Recuperado de: https://encuentro.educatic.unam.mx/educatic2020/pdf/presentacion-entre-saberes-edel.pdf

Edel, R., & Ruiz, G. (2022). *Diagnóstico de la Competencia Digital Docente en las Instituciones de Educación Superior*. Editorial ANUIES-SEP. México. Recuperado de: https://acortar.link/PPc987

Gaitán, J. (2020). *Diseño de controles y normas de seguridad para la empresa QWERTY S.A. que garanticen la preservación de la integridad confiabilidad y disponibilidad de los activos informativos de la organización*. (Tesis de Especialización). Universidad Nacional Abierta y a Distancia. Recuperado de: https://repository.unad.edu.co/handle/10596/38802

García, C., Burgos, D., Murillo, P., & Jaspez, J. (2019) Aprender con tecnologías para enseñar con tecnologías en República Dominicana. El programa República Digital Educación. *Revista*

Iberoamericana de Educación, 79(1), 115-134. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6956818

George, C. (2020). Alfabetización y alfabetización digital. *Transdigital*, 1(1). Recuperado de: https://doi.org/10.56162/transdigital15

Hernández-Sampieri, R., Fernández, C., & Batista, P. (2016) *Metodología de la Investigación*. México: Mc Graw-Hill

Ibáñez, T. (2009). *Municiones para disidentes. Realidad-Verdad-Política*. Barcelona: Gedisa.

Ley No. 53-07, del 23 de abril de 2007, contra Crímenes y Delitos de Alta Tecnología. *Congreso Nacional de la República Dominicana*. Recuperado de: https://wipolex.wipo.int/en/text/235325

Marín, D., Cuevas, N., & Gabarda, V. (2021). Competencia digital ciudadana: Análisis de tendencias en el ámbito educativo. RIED. *Revista Iberoamericana de Educación a Distancia*, 24(2), 329-349. Recuperado de: https://doi.org/10.5944/ried.24.2.30006

Martínez-Álvarez, E. (2020). *Integración de las tecnologías de la información y la comunicación y su relación con la gestión académica y gestión administrativa en instituciones educativas colombianas – 2020*. (Tesis Doctorado en Educación). Universidad Norbert Wiener, Perú. Recuperado de: https://repositorio.uwiener.edu.pe/handle/20.500.13053/6237

Martínez-Miguelez, M. (1996). *Comportamiento Humano. Nuevos métodos de investigación*. México: Trillas

Monje, C.A. (2011) *Metodología de la Investigación cuantitativa y cualitativa*. Guía Didáctica. Universidad Surcolombiana: Facultad de Ciencias Sociales y Humanas.

Narváez, A. (2019). *Análisis de Vulnerabilidades para la Red Lan de la Empresa "Hidromag", bajo la metodología Osstmm*. (Trabajo de investigación para obtener la titulación de Ingeniero informático). Universidad Tecnológica Israel, Ecuador. Recuperado de: http://157.100.241.244/handle/47000/2044

Pérez, S. (2018). *Un Modelo de Gestión Empresarial: La responsabilidad Social Corporativa de las empresas del IBEX 35, actitudes y conductas de sus empleados y clientes*. (Tesis Doctoral). Universidad Nacional de Educación a Distancia. Recuperado de: https://dialnet.unirioja.es/servlet/tesis?codigo=254602

Pons, V. (2018). *Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*. (Tesis Doctoral en Ciencias Jurídicas). Universidad de Nacional de Educación a Distancia. Recuperado de: https://dialnet.unirioja.es/servlet/tesis?codigo=204191

Reche, E., Quintero, B., & Lozano, I. (2019) Las competencias informacionales del alumnado de nuevo ingreso de los Grados en Educación Infantil y Primaria. En Sánchez-Rivas, E., Ruiz-Palmero, J., y Sánchez Vega, E. (eds.), *Innovación y tecnología en contextos educativos. Libro de actas correspondiente al Congreso sobre Innovación y Tecnología en Contextos Educativos* (pp. 73-82). Universidad de Málaga. UMA Editorial Recuperado de: https://riuma.uma.es/xmlui/handle/10630/18555

Revelo, J., Revuelta, F., & González-Pérez, A. (2018), Modelo de integración de la competencia digital del docente universitario para su desarrollo profesional en la enseñanza de la matemática. Universidad Tecnológica Equinoccial de Ecuador. *EDMETIC, Revista de Educación Mediática y TIC*, 7(1), 196-224. Recuperado de: https://doi.org/10.21071/edmetic.v7i1.6910

Rosario, I., & Ruiz, E. (2018). La adicción a las redes sociales en una muestra de empleados de varias organizaciones del sureste de Puerto Rico. *Avances En Psicología*, 26(2), 201-210. Recuperado de: https://doi.org/10.33539/avpsicol.2018.v26n2.1191

Silva, J., & Miranda, P. (2020). Presencia de la competencia digital docente en los programas de formación inicial en universidades públicas chilenas. *Revista de estudios y experiencias en educación*, 19(41), 149-165. ISSN 0718-5162. Recuperado de: http://dx.doi.org/10.21703/rexe.20201941silva9

Tapia, C. (2020). Tipologías de uso educativo de las Tecnologías de la Información y Comunicación: una revisión sistemática de la literatura. *Edutec Revista Electrónica De Tecnología Educativa*, (71), 16-34. Recuperado de: https://doi.org/10.21556/edutec.2020.71.1489

Ticona, J. (2022) Uso de las TIC y su relación con el desempeño laboral del personal administrativo de las universidades nacionales. *Revista De Investigaciones*, 9(3), 195 - 204. Recuperado de: https://doi.org/10.26788/riepg.v9i3.2046

Zambrano, S., & Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio De Las Ciencias*, 3(3), 676-688. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824