UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA)

VICERRECTORÍA DE INVESTIGACIÓN Y POSGRADO

DOCTORADO CONSORCIADO EN CIENCIAS DE LA EDUCACIÓN

TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA: ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA DOMINICANA

NIEVES DEL CARMEN PÉREZ

Santiago De Los Caballeros, 2023

UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA)

TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA: ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA DOMINICANA

Tesis presentada como requisito para optar al título de Doctor en Ciencias de la Educación, considerado en nombre de la Universidad Abierta Para Adultos (UAPA), por el siguiente Jurado, en la ciudad de Santiago de Los Caballeros en el mes de octubre de 2023.

Por: NIEVES DEL CARMEN PÉREZ

Director de la tesis: DR. RUBEN EDEL NAVARRO

Santiago De Los Caballeros, 2023

TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA:
ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA DOMINICANA

Por: NIEVES DEL CARMEN PÉREZ

Tesis presentada como requisito para optar al título de Doctor en Ciencias de la Educación, considerado en nombre de la Universidad Abierta Para Adultos (UAPA), por el siguiente Jurado, en la ciudad de Santiago de Los Caballeros en el mes de octubre de 2023.

Dra. María Elena Chan Núñez
Jurado

Dr. Ruíz Méndez Germán
Jurado

Dra. Beatriz Veracoechea
Jurado

Dra. Jovanny Rodríguez
Jurado

Dr. Luis Bayonet
Jurado

Santiago De Los Caballeros, 2023

DEDICATORIA

Ante todo, a Dios por ser el centro de mi vida, por guiarme por el camino correcto y permitirme enseñar con calidad, por darme la salud, las fuerzas necesarias para culminar este importante proyecto de mi carrera profesional.

A mi familia por su apoyo incondicional, sobre todo a mi esposo Lic. José Tavárez por estar siempre cuando más lo necesitaba. A mi hija, Lic. Shanellys Tavárez. A mis hijos José Enmanuel Tavárez y Alwin José Tavárez, por el tiempo que les quité de compartir juntos en familia, esto es un logro de todos. Destacar a mis padres, hermanos, gracias por impulsarme hacia el camino del éxito, promoviendo la educación y la investigación.

AGRADECIMIENTOS

En primer lugar, al padre celestial, por caminar conmigo en todos los proyectos de mi vida.

A la Dra. Magdalena Cruz, Vicerrectora de Investigación y Posgrado en la Universidad Abierta Para Adultos, UAPA y el Doctorado Consorciado, UCATECI, UCNE, UTECO por la oportunidad, sobre todo al Dr. Jesús Canelón, Coordinador de la 1ra. Cohorte del Doctorado en Ciencias de la Educación, de la Universidad Abierta para Adultos, UAPA por su excelente trabajo, quien se convirtió en un amigo para todo el equipo.

A INAFOCAM por su invaluable apoyo económico

De modo muy especial, al Director de Tesis Dr. Rubén Edel Navarro, por su tiempo dedicado a supervisar, revisar, guiar la investigación durante todo el proceso. Además, por creer en mí, inspirando confianza, sobre todo flexibilidad a la hora de las entregas, demostrando su liderazgo y profesionalidad.

A la administración del Instituto politécnico Martina Mercedes Zouain por permitirme realizar esta importante investigación, docentes y estudiantes del área técnica de informática.

A los expertos que validaron los instrumentos de evaluación y sus recomendaciones de mejora:

Dra. Ruth M. Mujica-Sequera, Ed.D.

Dra. María Elena Chan Núñez.

Héctor David Lantigua Reynoso M.A.

Concepción Ortiz M.A.

Dra. María Gisela Escobar

Dr. Jesús Alberto Roberti

A los profesores de la primera cohorte del doctorado consorciado, agradecida de sus enseñanzas y motivaciones, al mismo tiempo a los compañeros doctorantes, especialmente a Renata Jiménez, Elías Yanet Díaz, a José Luis Días, M.A, por impulsarme hacia el éxito y finalmente a mi familia, mi esposo e hijos por su comprensión y apoyo incondicional.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA)

TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA: ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA DOMINICANA

Autor: Nieves del Carmen Pérez

RESUMEN

La presente investigación se llevó cabo con la finalidad de estudiar las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en estudiantes, docentes y administrativos del Instituto Politécnico Martina Mercedes Zouain, República Dominicana. El estudio fue de tipo cualitativo, a través del método hermenéutico dialéctico en los actores educativos del Instituto Politécnico Martina Mercedes Zouain, ubicado en Santiago, por medio de la observación participante y cuestionarios a 91 estudiantes y entrevistas abiertas aplicadas a 19 docentes y 13 integrantes del personal administrativo. La técnica de análisis de información fue el sistema de categorización por medio de la identificación de códigos, categorías axiales y categorías selectivas. En el proceso de análisis se dio respuesta a los objetivos planteados encontrándose que existe, en todos los participantes, conocimientos básicos en cuanto a seguridad informática. No obstante, se detectan vulnerabilidades en el sistema de seguridad institucional que afecta los procesos académicos y administrativos. Los estudiantes tienen buenas competencias digitales, aun cuando las emplean más para la interacción social que con fines académicos, mientras que los docentes tienen competencias medias y deben capacitarse más en las plataformas educativas. Los administrativos están alfabetizados digitalmente para el manejo de documentos. Sin embargo, requieren mayores destrezas en herramientas virtuales para los procesos institucionales. En cuanto a la ciudadanía digital, se identificó que en los participantes existe conciencia sobre los elementos éticos y la responsabilidad en la interacción digital, pese a ello, es necesario reforzar el rol de docentes y padres.

Palabras clave: Competencia digital; seguridad informática; educación; ciudadanía digital.

UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA)

INFORMATION TECHNOLOGIES AND DIGITAL COMPETENCE IN SECONDARY EDUCATION: CASE STUDY AT THE MARTINA MERCEDES ZOUAIN POLYTECHNICAL INSTITUTE, DOMINICAN REPUBLIC

Autor: Nieves del Carmen Pérez

ABSTRACT

This research aimed to study the contribution of digital skills in the safe use of information technology, communication, knowledge, and digital learning (ITCKDL), in students, teachers and administrative personnel of the Martina Mercedes Zouain Polytechnic Institute, Dominican Republic. The qualitative study was carried out through the dialectical hermeneutic method in the educational actors of the Martina Mercedes Zouain Polytechnic Institute, located in Santiago, through participative observations and questionnaires to 91 students and open interviews applied to 19 teachers and 13 members of the administrative staff. The information analysis technique was the categorization system through the identification of codes, axial categories and selective categories. In the analysis process, a response was given to the proposed objectives, finding that there is basic knowledge in terms of computer security in all participants, but vulnerabilities are detected in the institutional security system that affects academic and administrative processes. Students have good digital skills, even so, they use them more for social interaction than for academic purposes, but teachers have average skills and should be trained more in educational platforms. Administrative staff are digitally literate for document management, however, they require greater skills in virtual tools for institutional processes. Regarding digital citizenship, it was identified that the participants are aware of the ethical elements and responsibility in digital interaction, even though. it is necessary to reinforce the role of teachers and parents.

Keywords: Digital competence; informatics security; education; digital citizenship.

INTRODUCCIÓN

La sociedad mundial en pleno siglo XXI ha experimentado un dinamismo significativo que le hace más cambiante, moderna, exigente y competitiva, lo cual acusa la redimensión de las organizaciones e instituciones con roles trascendentes en los sectores de servicio, verbigracia, como el educativo. En ese orden de ideas los institutos educativos de República Dominicana están llamadas a adaptar sus resultados a las exigencias de la tecnologías y didácticas educativas

En este sentido, la integración de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales es (TICCAD) en los procesos de enseñanza-aprendizaje constituyen una realidad, a la cual docentes, alumnos y personal administrativo deben integrarse, ya que cada vez con mayor fuerza se exigen competencias que permitan un adecuado desempeño en las herramientas didácticas virtuales. Definitivamente estos mediadores tecnológicos han transformado los procesos de enseñanza-aprendizaje ya que generan un enfoque interactivo distinto al convencional al incorporar estrategias orientadas a dinamizar las actividades que potencian habilidades cognitivas, sociales e incluso emocionales.

Cabe destacar que para Cabero et al (2018), actualmente en la virtualización de las clases en línea se percibe en el docente, falta de compromiso y motivación en cuanto al desarrollo de proyectos colaborativos que ayuden al estudiante a desarrollar competencias como el desarrollo de liderazgo, empatía, responsabilidad, y es especialmente preocupante el manejo responsable de las plataformas virtuales y por otra parte, según Mujica-Sequera (2020), los docentes de hoy se relacionan con estudiantes que son nativos digitales, los cuales poseen capacidades altamente eficaces en el uso de las tecnologías, así que es necesario que en el proceso pedagógico consideren la constante inmersión de los jóvenes en el mundo tecnológico y las dificultades que esto conlleva

Sobre la base de estas premisas este trabajo propone el estudio de las competencias digitales en el uso seguro de las TICCAD en estudiantes, docentes y administrativos del Instituto Politécnico Martina Mercedes Zouain, República Dominicana. Se parte de la necesidad de mejorar la calidad educativa desde la perspectiva de la tecnología cibernética en el aula, de tal modo que se pueda optimizar sus resultados, con lo cual, el usuario adquiera herramientas y

destrezas digitales, posibles de ser usadas en un marco axiológico, cónsono las esperanzas de calidad educativa demandadas por el país.

Por lo tanto, con la intención de este trabajo se ha emprendido una investigación cualitativa que permite recoger información en estudiantes, docentes y empleados administrativos del Instituto Politécnico Martina Mercedes Zouain para entender como las competencias que poseen estos actores institucionales se vinculan con la posibilidad de emplear las tecnologías de forma segura para sus actividades académicas.

En tal sentido, el estudio queda a disposición de las autoridades directivas, académicas y administrativas para su evaluación y consideración en función de los objetivos que se aspiran a desarrollar en el Instituto Politécnico Martina Mercedes Zouain. En la intención de que los hallazgos se constituyan en un ejemplo en el ámbito tecnológico educativo, respaldado por un riguroso estudio investigativo.

Desde esta perspectiva, el trabajo se dispone según la siguiente estructura:

Capítulo I, se muestra el marco epistémico y los elementos que orientan el estudio, como es la precisión del problema y objetivos.

Capítulo II con el marco teórico referencial que da forma a la investigación a partir de distintos conceptos fundamentales, iniciando con los antecedentes del estudio.

Capítulo III se sigue con el marco metodológico, que se define de corte humanístico cualitativo a través del método Hermenéutico Dialéctico, y se explica el proceso de recolección de información.

Capítulo IV se presentan los resultados la investigación.

Capítulo V muestra una propuesta de un marco actualizado de las políticas institucionales de seguridad informática del Instituto Politécnico Martina Mercedes Zouain, se abordan cinco sesiones: Sesión I: Reflexiones sobre opiniones de los participantes involucrados en la investigación: Tecnologías de la información y competencia digital en educación secundaria: Estudio de Caso en el Instituto Politécnico Martina Mercedes Zouain, República Dominicana. En la Sesión II: Consciencia a autoridades, Sesión III: Medidas de Seguridad Digital, Sesión IV: Capacitación a los usuarios, sesión V: Biblioteca digital. Seguido de las Conclusiones, Recomendaciones y Líneas de Investigaciones Futuras.

CAPÍTULO I.
PLANTEAMIENTO DEL PROBLEMA Y OBJETIVOS

La investigación pretende abordar la problemática sobre el uso seguro de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales en el ámbito educativo, y cómo estas deben relacionarse a la construcción de entornos seguros mediante la administración de medidas y capacitación de las mismas, por parte de las instituciones educativas que, minimicen los riesgos y las vulnerabilidades inherentes a la comunicación mediada por internet, considerando que se trata de una situación actual y vigente, que debe atenderse de modo urgente.

En efecto, la revisión de la literatura para la elaboración del estado del arte de esta investigación muestra que los riesgos de seguridad en las instituciones educativas suelen ser bastante alto, gracias a la utilización de las plataformas educativas virtuales que son compartidas. Por ello, se ha planteado que más allá de la inversión en sistemas de seguridad informática, resulta fundamental la preparación y formación en competencias que faciliten las acciones responsables por parte de los distintos actores implicados.

Si bien se trata de una problemática vigente, es necesario profundizar en un marco epistémico e investigativo que permita profundizar en estas temáticas. Dicho lo anterior, en el presente capítulo se establecen los elementos que orientan la investigación, así como los fundamentos conceptuales para dar sentido a la información teórica y los resultados que se identifican en el desarrollo metodológico.

1.1. Problema de Investigación

El Instituto Politécnico Martina Mercedes Zouain corresponde al Distrito Educativo 06 de la regional 08 de la ciudad de Santiago de los Caballeros, República Dominicana. Esta es una institución pública que ofrece educación general y técnica profesional que incluye los cursos desde tercero (3ro) a sexto (6to), con el objetivo de capacitar a los estudiantes para su inserción laboral a través de pasantías en empresas potenciales empleadoras.

Las áreas curriculares que ofrece en el componente técnico incluye informática, turismo, contabilidad, mercadeo y enfermería. En cuanto a su ubicación, la institución se encuentra en

una zona rural y se localiza en el kilómetro 8 de Gurabo, carretera turística Luperón, entrada Santa Rita de la comunidad la Chichigua, Santiago y la mayoría de los estudiantes proceden de familias de bajos recursos económicos, por lo que presentan limitaciones o dificultades para tomar cursos extracurriculares que fortalezcan sus destrezas y habilidades en el área de las tecnologías de punta.

Pese a que las TICCAD se han ido incorporando progresivamente al currículum de la institución, especialmente después del período de pandemia debido a las necesidades de la educación a distancia, exponen una problemática determinante de relevante observación y estudio, como punto álgido de estudio, desde el punto de vista del uso y de la aplicación adecuada, por parte de los usuarios docentes, cuerpo administrativo y estudiantes.

Cabe destacar que en la actualidad la Institución cuenta con distintas opciones de plataformas con fines educativos, como es el Moodle de la institución, Google Classroom y el Blog institucional. Además, se afianza con la disposición de un laboratorio de informática con computadoras para la realización de actividades y se implementan tareas remotas sincrónicas o asincrónicas que los estudiantes cumplen desde sus hogares con conexión a internet.

Por tal motivo puede afirmarse que en los distintos programas es fundamental la vinculación de los estudiantes y docentes con las tecnologías, mediante los hallazgos del presente estudio, a fin de crear una cultura y consciencia sobre el espectro de las tecnologías educativas y sus implicaciones de seguridad cibernética y su radio de acción axiológica y así minimizar la problemática percibida.

La autora de la presente investigación, ha observado que no existen programas definidos sobre capacitación dirigidos a docentes y empleados administrativos, orientados a promover las competencias digitales y, asimismo, en consecuencia, los estudiantes no son orientados adecuadamente, en esta urgente y emergente necesidad.

Desde esta perspectiva se enfoca con más precisión que la preparación de los docentes en este sentido es autónoma y no se transmite a los estudiantes estrategias claras para garantizar la seguridad informática en sus actividades académicas. En general, se ha observado que existen situaciones que pueden implicar la vulneración de la seguridad en distintos aspectos, por ejemplo, debido al uso de computadoras compartidas, inestabilidades en el acceso a internet y especialmente, a que no existe una cultura asociada a la ciudadanía digital que demuestre una conciencia clara en el uso de estas herramientas para fines educativos.

Cabe destacar que según el informe presentado por Molina (2016) al analizar la infraestructura tecnológica en los planteles públicos del país, para ese momento, la Institución en estudio contaba con insuficientes espacios tecnológicos para atender a la población estudiantil, kit multimedia y equipos de computación insuficientes; asimismo, conectividad deficiente y energía eléctrica irregular.

Según exponen Marcelo et al (2019) si bien se realizan esfuerzos en República Dominicana a través del programa República Digital Educación para introducir innovaciones en el uso de la tecnología en el sistema educativo nacional, la realidad es que además de la brecha digital y las insuficiencias en infraestructura, existe un bajo o muy bajo nivel de competencia digital en los docentes, razón por la cual la integración de las tecnologías digitales en los centros educativos no es un proceso fácil. Estos autores también destacan que uno de los problemas importantes que deben ser atendidos es la seguridad y el mantenimiento de la infraestructura tecnológica.

Según la identificación de la situación que ha sido expuesta, se plantea que las deficiencias en cuanto al acceso a los recursos tecnológicos y capacitación en docentes y empleados administrativos puede tener un impacto en la seguridad informática de la institución, ya que se falla en transmitir competencias a los estudiantes para lograr un adecuado uso de las TICCAD.

Por tal motivo, en la presente investigación se propone estudiar en las competencias digitales existentes que permiten desarrollar prácticas seguras en el manejo informático en los docentes, estudiantes y personal administrativo educativos del Instituto Politécnico Martina Mercedes Zouain, considerando la necesidad de evidenciar un conjunto de habilidades que permitan que las interacciones virtuales con fines académicos se produzcan de forma confiable. Por tanto, se ha definido la siguiente pregunta-problema de investigación:

¿Cómo las competencias digitales influyen en el uso seguro de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en los distintos actores educativos del Instituto Politécnico Martina Mercedes Zouain, República Dominicana?

Preguntas de investigación

De forma más precisa, se generan las siguientes interrogantes que también han sido consideradas para este trabajo.

¿Qué medidas de seguridad emplea la Institución en la capacitación de los docentes y personal administrativo para el manejo de la tecnología educativa, en tal magnitud que se influya positivamente en los estudiantes?

¿Cuál es el nivel de competencia digital de los estudiantes, docentes y empleados administrativos?

¿Qué destrezas tienen los actores de la institución educativa para emplear de forma segura las TICCAD?

¿Cómo contribuir en la puesta en marcha de un cuerpo de medidas de seguridad en el contexto digital en la institución educativa?

1.2. Objetivos

General

- Estudiar las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en estudiantes, docentes y personal administrativos del Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

Específicos

- Identificar las competencias digitales que poseen estudiantes, docentes y técnicos para el desarrollo de sus actividades específicas en la institución.
- Analizar los riesgos y vulnerabilidades que se presentan en el manejo de los sistemas tecnológicos en la institución.
- Caracterizar las medidas de seguridad informática normadas por la Institución y las empleadas por los diferentes actores institucionales para el logro de la ciudadanía digital.
- Coadyuvar en la propuesta de un marco actualizado de las políticas institucionales de seguridad informática del Instituto Politécnico Martina Mercedes Zouain.

1.3. Justificación

En virtud de la realidad de avanzada tecnológica en la que se desarrollan las generaciones actuales es de suponer que las exigencias en el campo laboral y social demandará mayores destrezas. Desde esta perspectiva el presente estudio es relevante por cuanto con la

puesta en práctica de los objetivos propuestos se estaría aportando soluciones a estas habilidades y destrezas tecnológicas requeridas

Desde el ángulo de la educación, esta investigación retoma importancia porque da al docente una oportunidad de repensar su formación educativa en diversos niveles de impacto. Por ejemplo, contribuiría a: (a) replantear la determinación del nivel alcanzado en cuanto a apropiación tecnológica; (b) reflexionar sobre el modo tradicional versus las demandas y exigencias de los cambios educativos, en función de las nuevas tecnologías y así, de alguna manera a enfrentar sus debilidades mediante el apoyo concreto de la investigación; y, (c) incrementar el proceso del aprendizaje significativo, al desplegar dominios de tecnología educativa como un recurso didáctico amigable.

Más específicamente, en el ámbito de la educación secundaria, el presente estudio se justifica porque con los hallazgos propios de la investigación se entregaría al docente, las herramientas tecnológicas precisas para contrarrestar la vulnerabilidad que acarrea la tecnología y, en consecuencia, las aplicaciones que de algún modo toman por sorpresa a los usuarios, a través de los diversos dispositivos. Cabe destacar que la ciberseguridad será el norte de los nuevos sistemas informáticos para docentes, personal administrativo y estudiantes que se están formando en el aula, cada vez más de modo imperativo y ello entra en el rango de la preocupación del estudio llevado a cabo.

En consideración a lo arriba expuesto, esta investigación tendría un impacto significativo en la formación consciente de los docentes, personal administrativo y los estudiantes, dado el intento formulado mediante los objetivos en la mejor comprensión de las respectivas competencias digitales, logrando así, la obtención, apropiación y mejoría de las habilidades tecnológicas requeridas en el aula y, en consecuencia, en el plano educativo cibernético.

El presente trabajo de investigación es relevante desde la perspectiva del uso seguro del internet, por cuanto, intenta promover la consciencia de su administración controlada en la escuela, hogares, a toda comunidad educativa, propiciando a la vez, valores humanos como la ciber ética, responsabilidad, honestidad. Por demás, Identificando los riesgos y desafíos de las tecnologías, especialmente durante la navegación en internet y las estrategias para combatirlos.

Este estudio es importante porque promueve la innovación tecnológica, las actualizaciones constantes alineado con las demandas de la sociedad. Además, este estudio puede influir en la formulación de nuevas políticas educativas en el Centro Educativo, a nivel distrital, regional o Nacional que podrían ser útiles para apoyar la formación docente en competencia digital y fortalecer el uso responsable y efectivo de las tecnologías en las escuelas de la Republica Dominicana y otros países del mundo.

Desde la axiología y la conducta humana, el estudio redimensiona su importancia ya que se presentan estrategias sobre el comportamiento de las conductas inadecuadas de los individuos, la falta de ética, el bulling, ciberbulling, sexting, extorsión, hackeo, entre otros. Con lo cual se estaría haciendo eco a aspectos legales que emergen a la par de las exigencias tecnológicas, para el buen desempeño moral y social de los usuarios y más aún en un contexto educativo.

Finalmente, este estudio reviste relevancia porque contribuiría a enaltecer la línea de investigación Innovación, Ciencia y Tecnología de la Educación en el contexto de la Investigación Educativa y así, resaltar la importancia de los estudios doctorales de la Universidad Abierta para Adultos (UAPA), y el Doctorado Consorciado, UCATECI, UCNE, UTECO.

1.4. Supuesto preliminar

A la luz del problema se plantea el supuesto preliminar de que las medidas de capacitación en las destrezas digitales de los docentes, estudiantes y administrativos de la institución en estudio, presentan deficiencias en el dominio seguro de las TICCAD y, por tanto, hay fallas en las destrezas didácticas para el manejo seguro de la tecnología, lo cual redunda en limitadas competencias digitales en los estudiantes de la institución. Dicho lo cual, resulta fundamental promover en todos los actores, la ciudadanía digital.

1.5 Límites de la investigación

Esta investigación se desarrolló en el contexto docentes, personal administrativo y estudiantes de Secundaria del Instituto Politécnico Martina Mercedes Zouain Distrito 08-06 Santiago, con lo cual cabe destacar que ello es una limitante en el estudio, puesto que la intención era ampliar la investigación a un gran número de instituciones educativas similares en el país, a fin de consolidar un marco de referencia detallado y preciso sobre medidas para la competencia en el uso de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales. La limitante ocasionada por el confinamiento del COVID-19 llevó a realizar la investigación en dicho entorno. Además de la situación crítica de salud presentada en el momento.

En cuanto a otra limitante de la investigación se debe mencionar, principalmente, la escasa información documental existente sobre competencia digital y seguridad informática en instituciones educativas en Latinoamérica y específicamente en República Dominicana, lo cual evidencia que es un tema poco investigado en la región y en el país, pese a su gran importancia. De hecho, la mayor parte de la información recuperada procede de tesis de licenciatura realizadas en Ecuador, Colombia y México, las cuales debieron ser descartadas debido a que no alcanzan los niveles requeridos en una investigación doctoral.

La pandemia COVID-19 y las dificultades en la aplicación de los instrumentos de evaluación por las medidas de confinamiento, limitó la posibilidad de recopilar el 100% de las respuestas de los informantes claves, por lo que durante la aplicación de los instrumentos en tiempos de pandemia las aula con los alumnos y docentes contagiados lo retiraban por un lapso de tiempo hasta regresar con una prueba negativa, sabiendo también que los cursos asistían solo la mitad por sesiones para mantener la distancia, algunos le tocaba asistir a clase martes y jueves y otros lunes, miércoles y viernes, esto era una orden directa del Ministerio de Educación. Pues todo el cronograma planificado había que restructurarlo con frecuencia.

1.6. Definición de términos

En esta sección se organizan los términos fundamentales a partir del concepto de Competencias Digitales desde la axiología y la comprensión de la conducta humana, lo cual permite profundizar sobre los ejes temáticos que se plantearon al definir los objetivos,

Educación superior

La educación superior constituye una etapa en el sistema educativo que se focaliza a generar conocimientos avanzados teóricos y técnicos a la población que ha cumplido los subsistemas formales anteriores de la educación formal. El currículo, los materiales, la didáctica y métodos están constituidos por cuerpos de ideas avanzadas y técnicas que en la mayoría de los casos están vinculadas con el avance y desarrollo de los países.

El personal académico que integra estas instituciones es de formación avanzada y especializada que cuenta en la mayoría de los casos con la capacitación necesaria para transmitirla a sus estudiantes, no obstante, dada la naturaleza cambiante de los distintos determinantes que sustentan la educación superior, los docentes están llamados a tomar consciencia de una permanente actualización, en beneficio de los estudiantes y, en definitiva, de la sociedad en que se desenvuelven a fin de apuntalar el desarrollo social alcanzado.

Asimismo, en este sistema de educación superior se ubican los institutos tecnológicos o politécnicos, los cuales ofrecen programas cortos y específicos de formación en áreas, con un menor énfasis en la formación teórica y mayor interés en fomentar capacidades específicas en áreas prioritarias para el mercado laboral y el desarrollo de los países (Clark, 1991).

Competencias digitales

Se refiere al dominio cognitivo, procedimental y actitudinal de las tecnologías de la información comunicación, conocimiento y aprendizaje digitales es para su empleo seguro, crítico y creativo en los procesos educativos, de ocio y de comunicación. Por tal motivo, conlleva a un uso amplio, en el cual se consideran actividades tales como recuperar, evaluar, almacenar, producir, presentar, intercambiar informaciones e interactuar en redes de colaboración mediadas por Internet (Gallego-Arrufat, 2019).

Uso seguro de la tecnología de la información la comunicación, conocimiento y aprendizaje digitales (TICCAD)

Es conveniente darle el uso apropiado a la tecnología, cuidar los equipos de los virus, para mantener los datos y contraseñas seguras. Zambrano y Valencia (2017) señalan que el empleo seguro de las TICCAD implica proteger los recursos de los riesgos o ataques informáticos, además del cuidado de los datos confidenciales de la institución. Por tanto, conlleva el 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, (Silva y Miranda, 2020).

Dicho comportamiento juega un papel importante en los procesos de formación docente, en la cual se consideran diferentes perfiles profesionales y el modelo pedagógico específico, siendo fundamental la supervisión escolar y familiar para su adecuado desarrollo (Bonilla y Ferra, 2021).

Seguridad informática

Es vital el cuidado de los aparatos electrónicos y las redes que se utilizan en las instituciones educativas, Baca (2016), define la seguridad informática como los mecanismos para proteger los datos que se encuentran almacenados en los equipos, redes, sistemas computarizados, contra las amenazas de virus informáticos, evitando los riesgos a los cuales están expuestos.

Implica que los datos se manejen de forma efectiva, eficiente, confiable, integra, con privacidad, con disponibilidad y apego a los estándares como el control de acceso, autenticación o verificación de identidad de usuarios o sitios de internet, antes de realizar cualquier transacción y envío de información a otra entidad. Lo anterior permite que los datos lleguen sólo a los lugares autorizados, impidiendo un desvío de información o *hackeo*. La seguridad informática debe ir acompañada de un plan de prevención de ataques y recuperación por pérdida o robo de archivos.

Seguridad informática en educación

Si bien los principios de la seguridad informática en educación guardan ciertas similitudes con la seguridad que se ejerce en cualquier organización, existen diferencias sustanciales debido a que el acceso a los canales de comunicación e interacción están dirigidos fundamentalmente a la recuperación de información y al acervo del conocimiento.

En tal sentido, el uso de las TICCAD, en educación, no sólo permite vulnerabilidades en cuanto a la identidad y protección de datos, sino que se presenta otras debilidades relacionadas con el uso de la información, como el caso del plagio, el robo de propiedad intelectual, la actualización de contenidos o el acceso a información confiable (Salazar et al 2021).

Por tal motivo, las competencias no solo deben ir dirigidas a la ciberseguridad sino al adecuado tratamiento de la información académica, y ello sólo es posible en una interacción entre los estudiantes, académicos y la institución.

Ciudadanía digital

En efecto, los ciudadanos manejan la tecnología de diferentes formas, unos con uso responsables y otros de forma inmoderada, esto hace la diferencia entre personas críticas, investigadoras con valores éticos, morales, personas con falta de ética que crean conflictos frecuentemente y situaciones no favorables para la comunidad.

Catalina-García et al (2018) consideran que la ciudadanía digital consiste en la capacidad de ejercer los derechos participativos en los entornos virtuales, a través de la posibilidad de vincular el conocimiento ciudadano con las habilidades y requerimientos en el entorno online**.** Por su parte, para Amador-Ortiz y Velarde-Peña (2019) este criterio abarca temas relacionados con los valores humanos, la conducta, la ética, aspectos culturales, sociales, además de los tecnológicos, en el cual se incluye el uso seguro de las tecnologías, trabajos colaborativos, liderazgo y responsabilidad en el quehacer.

Ciudadanía digital como axiología de la conducta humana

Las destrezas para el funcionamiento de las tecnologías comprenden desde la apropiación tecnológica en cuanto a los conocimientos adquiridos, y la conceptualización, resolución de problemas, dominio de herramientas tecnológicas y la investigación científica, Amador-Ortiz y Velarde-Peña (2019). Estas destrezas deberían ser desarrolladas desde los primeros niveles educativos con el apoyo de docentes capacitados en las características, alcances y límites de esta tecnología

Más allá de las destrezas en el manejo instrumental, la interacción a través de las herramientas tecnológicas se vincula con la axiología humana, en tanto instrumentos que transmiten conocimientos, más aún, valores y principios éticos, sobre los cuales descansa la ciudadanía digital y que, indefectiblemente hay que atender en todo contexto educativo, razón por lo cual el ámbito axiológico se considera un eje medular del presente trabajo de investigación, en la intencionalidad de contribuir y prevalecer en el Centro educativo estudiado, una cultura digital inmersa en el bienestar social, moral y ético, de su comunidad escolar.

Como énfasis en este aspecto, Ulloa (2018), define la axiología como ciencia únicamente empírica, donde los valores humanos hacen o no presencia en el individuo, por consiguiente, la axiología demanda sabiduría, libertad de expresión, capacidad de escucha, observación con capacidad de discernir y toma de decisiones. Estos procesos de alto valor en las habilidades y juicio moral deberían estar comprometidas en el desarrollo de competencias digitales basadas en un sistema de responsabilidad y ciudadanía.

Por tal motivo, las competencias del docente deben ir también encaminadas al empleo de la tecnología como un recurso y no como un fin, es decir, la transmisión de conocimientos y principios al estudiante a través de los contenidos en línea deben ir encaminados a generar habilidades para para cuestionar, investigar y transformar la realidad a través del uso responsable y consciente de la información (Prado, 2021).

CAPÍTULO II.

MARCO TEÓRICO-CONCEPTUAL

2.1. Estado del arte

En los actuales momentos cuando la tecnología educativa está en vertiginoso avance se hace indispensable determinar que l educación cobra relevancia fundamental, especialmente cuando se trata del uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD), en manos de estudiantes, guiados por docentes y a la vez, atendidos por personal administrativo en las instituciones educativas quienes, indefectiblemente requieren actualización permanente en las competencias de esta área. Desde esta perspectiva, surgen algunos estudios específicos en los últimos cinco años, los cuales han sido revisados y que tienen estrecha vinculación con la investigación planteada, tanto en el ámbito internacional como nacional.

Cabe destacar que en esta búsqueda de antecedentes se tuvo como prioridad identificar estudios realizados en el país que indicaran una relación entre seguridad informática y competencias digitales en educación. Lamentablemente, en el proceso de indagación no logró recuperarse información procedente de artículos científicos o tesis doctorales, lo cual permite suponer que esta temática no ha sido considerada a nivel nacional y nos invita a seguir profundizando en esta línea de trabajo.

Por tal motivo, se ha optado por enfocar la revisión desde los aportes internacionales producidos en América Latina y en España, los cuales coinciden en señalar, como se verá más adelante que, los estudiantes en las instituciones educativas utilizan el internet inmoderado y atendiendo a sus intereses de interacción social, lo cual reduce las opciones de una relación segura. Destaca así que, con esta investigación se contribuye a dar luz en este tema, a nivel nacional, a la vez, de dar aliciente a futuras investigaciones doctorales que enriquezcan el estudio en curso.

2.1.1. Investigaciones sobre uso de las TICCAD en estudiantes

En el nivel internacional, Fernández-Prados y Lozano-Díaz (2020) se propusieron como objetivo una descripción del ciberactivismo en estudiantes universitarios españoles y relacionarlo con comportamientos en internet, tales como las horas dedicadas y las actividades que realizan en sus tiempos de ocio. La investigación fue de enfoque cuantitativo, con una muestra de 608 estudiantes universitarios de educación a quienes se aplicó una Escala de ciberactivismo validada.

Los resultados señalan que los estudiantes en su mayoría acceden a internet a través del móvil y su uso diario es intensivo. El mayor uso de internet está destinado a las redes sociales, seguido del uso para realización de trabajos académicos; en menor medida lo emplean para investigar o informarse sobre un aspecto específico.

Por otro lado, los autores encontraron que las conductas relacionadas con el ciberactivismo, tales como firmar alguna petición, sumarse a una actividad colectiva o contactar con algún partido político, fueron poco frecuentes. Estos resultados permiten afirmar que entre los jóvenes predomina más el uso de internet por razones lúdicas o de entretenimiento que la ciudadanía digital mediada por el ciberactivismo.

Los jóvenes se han convertido en adictos a las Tic, de manera que no pueden convivir con su familia, comer, sin acceso a ella, sobre todo los celulares, de hecho, el uso excesivo del teléfono les crea distracción en la escuela y no se concentran en sus clases, y es una situación que algunos docentes no pueden controlar.

Por otra parte, Del Barrio-Fernández (2018) realizó su tesis doctoral sobre la importancia y vigencia de las Tecnologías de la Información y la Comunicación en la vida personal y académica de los adolescentes en la Universidad de Extremadura (España). Los objetivos de la investigación se orientan a conocer a fondo la situación actual y real de los jóvenes, en cuanto a las soluciones tecnológicas que emplean en sus experiencias educativas.

Además, determinar los riesgos, existentes en el abuso de las tecnologías que permitan establecer medidas de prevención, efectivas. El trabajo se llevó a cabo empleando un diseño muestral a través de encuestas. Los resultados permitieron confirmar la hipótesis del uso frecuente de las tecnologías y la ausencia de estrategias de acción frente al abuso de los recursos digitales.

Los aportes de este antecedente para efectos de la investigación planteada están sustanciados con la información de ausencia de estrategias de acción frente al uso de los recursos digitales, los cual anima a profundizar en l investigación, a fin de enriquecer aportes sobre l luz que amerita esta temática.

Asimismo, Rodríguez (2015), llevó a cabo una investigación sobre Uso de las TIC para favorecer el proceso de aprendizaje de estudiantes con discapacidad Intelectual, en la Institución Educativa Nicolás Gómez Dávila en Bogotá, Colombia. Estudio de caso. Con el propósito de determinar la manera en que se promueve el uso de las Tic en el proceso de enseñanza aprendizaje de distintos estudiantes, con discapacidad intelectual (DI) quienes cursan tercero de básica primaria y están incluidos en el aula.

La investigación se realizó bajo el enfoque de la investigación cualitativa, donde se aplicaron instrumentos como la entrevista y la observación a educandos y educadores, con el objetivo de determinar en qué manera se puede favorecer y optimizar el uso de las TIC. Además, se entrevistaron a los padres de familia para corroborar la información.

Los resultados se agruparon por categorías y subcategorías que surgieron durante la investigación y de ellos se evidenció que en el ámbito educativo es donde cobra mayor fuerza el uso de las TIC y que favorecen el proceso de aprendizaje de los educandos con DI y, les permiten lograr la adquisición y fortalecimiento de nuevos aprendizajes de manera significativa. Las TIC juegan un papel fundamental, dando la posibilidad de expresarse, comunicarse con otros, superando barreras, metas, desafíos y sobretodo, respetando la diversidad cultural con una educación más incluyente y al alcance de los seres humanos.

La relación del estudio precedente, pese a ser un trabajo para tesis de maestría, se relaciona con el trabajo de investigación presente, por su búsqueda de información vinculada con las TIC, los estudiantes y los docentes, en un momento de alta vigencia y con cuyos resultados abre potencialmente puertas a la investigación sobre TICCAD, en República Dominicana.

2.1.2 Investigaciones sobre capacitación docente en TICCAD

En este contexto, en el que por un lado los estudiantes nativos digitales hacen un uso excesivo de las tecnologías, los docentes tienen grandes retos y desafíos en cuanto a la formación y mediación tecnológica, hacia los estudiantes para que estos puedan dominar la tecnología,

integrarlas en sus diferentes asignaturas, además, de utilizar plataformas e implementar el trabajo en equipo.

Al respecto, Villaman (2018), realizó un estudio cuyo objetivo fue determinar el desenvolvimiento de los docentes en la práctica educativa colaborativa del área de Lengua Española a nivel superior, a fin de identificar los puntos de reforzamiento necesarios para adecuarlo a las clases en la modalidad semipresencial mediada por las TIC.

El estudio fue realizado a través de una metodología mixta. Los resultados evidencian la necesidad del trabajo en equipo y colaborativo para integrar las Tic en el área de Lengua Española, lo cual se vincula con el desarrollo de las competencias digitales necesarias en los alumnos. El autor destaca que la gran mayoría de los estudiantes actualmente son nativos digitales, sin embargo, es fundamental el reforzamiento adecuado para lograr destrezas que permitan el buen uso de las herramientas con propósitos de su desarrollo académico.

A efectos de la presente investigación resalta el hecho que, el docente debe considerar utilizar la tecnología como medio que le permita desarrollar su práctica pedagógica con calidad y de forma interactiva y más aún, replantear el uso de la tecnología educativa, pensando en sus estudiantes permanentemente.

En ese sentido, los autores Habowski y Conte (2020), realizaron un estudio analítico cuyo objetivo estuvo dirigido a comprender las problemáticas y desafíos de las tecnologías de la información y la comunicación (TIC) en la educación. Esta investigación se basó en un enfoque hermenéutico, que considera la interpretación y construcción del conocimiento para la comprensión de las acciones educativas.

La información bibliográfica recopilada a través de la literatura consultada en el estudio permitió analizar críticamente las convergencias de las tecnologías con la educación y especificar los límites en cuanto al uso indiscriminado y no consciente, así como acciones que deben preverse. Para ello es fundamental establecer las interacciones dialécticas u colaborativas entre el maestro, alumno y la tecnología, en la cual se propicien habilidades y estrategias autocríticas que permitan comprender la tecnología como mediador para el desarrollo de competencias cognitivas y académicas.

En un artículo de investigación de Sierra et col. (2016), publicado en la Universidad del Zulia, Venezuela, señalan que la innovación, tecnología de la información y la comunicación, TIC, es uno de los proceso más cambiantes y dinámicos en el mundo globalizado, para el

mejoramiento de la calidad educativa. En este sentido, el propósito de dicho artículo fue analizar el uso de las herramientas tecnológicas TIC, en los docentes de las instituciones educativas de la ciudad de Riohacha, con base en un estudio de tipo descriptivo con diseño no experimental y de campo. Se utilizó la técnica de la encuesta personal trabajo de campo y observaciones dentro de las instalaciones educativas.

Los autores concluyeron que se requiere del desarrollo profesional del docente, en un entorno tecnológico que facilite la creación de nuevos ambientes educativos, mediante el uso de estrategias pedagógicas en las aulas de clase de las instituciones educativas. A efectos del presente estudio, este artículo reviste importancia en cuanto a que el uso referido, debe estar supeditado a regulaciones, a normativas que regulen su disponibilidad en manos del discente, dicho lo cual, da paso a atender las inquietudes acá propuestas.

2.1.3. Investigaciones sobre competencias digitales

Expuesto los antecedentes anteriores es preciso considerar investigaciones orientadas a las competencias digitales en docentes y estudiantes, ya que indiscutiblemente, ambos actores del proceso enseñanza-aprendizaje, deben tener apropiación tecnológica como competencia básica.

Al respecto, Aguirre et al (2018), realizaron una investigación de tipo exploratorio acerca de las competencias digitales de estudiantes de bachillerato, en el cual participaron 44 instituciones de media superior en de los estados de Oaxaca, Veracruz y Zacatecas de México, realizado en 12 colegios Veracruzanos. Los estudiantes desarrollan competencias digitales sobre el manejo de los programas y los componentes del computador, con conocimiento en algunos de los recursos para comunicarse entre sí y en pares.

Además, se encontraron debilidades en el uso de plataformas con fines educativos. Como conclusiones resaltan que, los estudiantes tienen habilidades digitales cumpliendo con el modelo educativo en el país, y que deben tener buen manejo, y conocimiento informático, adueñarse de las tecnologías ya que éstas ayudan a ampliar y desarrollar mayores competencias; que los estudiantes reconozcan la importancia del trabajo en línea, grupal a través de plataformas educativas, para la producción de contenidos y conocimientos. En efecto, los docentes deben adquirir competencias innovadoras que mejoren continuamente su proceso de enseñanza-aprendizaje.

Por su parte, Revelo et al (2018), realizaron un estudio sobre la integración de la competencia digital docente, con el propósito de especificar el nivel de apropiación de las tecnologías en docentes de matemática en el nivel universitario en México, identificando el nivel de innovación que emplean los profesores a través de la web para integrar en su labor didáctica.

En la investigación se empleó un nivel descriptivo de enfoque cuantitativo. Los resultados evidencian que los docentes universitarios en el área de matemáticas poseen niveles básico y medio en habilidades como el dominio, el uso y la innovación. Asimismo, tienen niveles bajo-medio en destrezas tales como en la creación de contenidos digitales, seguridad informática, solución de problemas, comunicación y colaboración, alfabetización informacional digital, aun y cuando estos integran las TIC en sus actividades docentes regulares.

Para los docentes, la adquisición de competencias digitales es una decisión personal más que administrativa. Algunos no se capacitan por diferentes razones como la edad, tiempo, tecnofobia, en definitiva, educar es un proceso de investigación continuo. Este hallazgo es de suma importancia a efectos de la presente investigación, pues destaca el potencial y la responsabilidad que asume el docente, pese a las limitantes gerenciales de una institución educativa, en cuanto a capacitación digital. De allí que aquí el mismo, encuentre alicientes para su respectiva formación.

Por su lado, Gallego Arrufat et al (2019) desarrollaron una investigación que evalúa la competencia digital de docentes en formación en España y Portugal. La muestra estuvo conformada por 317 estudiantes que respondieron a un cuestionario dirigido a conocer el nivel y perfil predominante de competencias durante el proceso de formación, bajo 3 constructos: conocimientos, usos e interacciones y patrones actitudinales.

El análisis de resultados arrojó que el 47% de los participantes poseen riesgo digital medio, el cual se presenta gracias a prácticas que implican vulnerabilidades tales como compartir contenidos digitales de forma no responsable, uso de contraseñas no seguras, y desconocimiento de conceptos fundamentales para las actividades virtuales. Asimismo, se demostró que los futuros docentes tienen una actitud adecuada hacia la seguridad, pero fallan en los conocimientos, destrezas y prácticas para el uso seguro y responsable de Internet. Se recomienda que la formación de docentes esté dirigida a una ciudadanía más formada y competente digitalmente, tomando en cuenta la educación desde las primeras etapas educativas en seguridad, privacidad e identidad virtual.

Por su parte, las competencias digitales de los alumnos dependen en gran parte de las competencias del docente, se considera una gran cantidad de docentes con tecnofobia o miedo a las Tic, donde muchas veces les piden ayuda a sus estudiantes para poder integrar la informática en el aula, aunque debe suponerse que el docente debe ir preparado al aula para dar su clase, sobre todo con empoderamiento y apropiación tecnológica. Acá encontramos un aporte relevante para la investigación, como lo es el hecho de la tecnofobia por parte del docente y la realidad que, en la mayoría de los casos, el estudiante supera al docente en el uso de las tecnologías de la información y eso es un riesgo si ambos desconocen la regulación de un uso adecuado.

Además, Colás-Bravo et al (2019) realizaron un estudio en la cual se plantea el desarrollo de un modelo para la competencia digital docente con base en el enfoque sociocultural, considerando cuatro categorías: Dominio, Preferencia, Reintegración y Apropiación. Para ello, aplicaron un cuestionario 1881 estudiantes cursantes de distintos niveles de educación obligatoria en Andalucía, España, la cual buscaba evaluar el nivel de competencia digital de los docentes en las clases con sus estudiantes.

Los resultados promedios muestran un nivel medio de los docentes en el desarrollo de la competencia digital, lo cual permite afirmar que existen necesidades no cubiertas en la implementación de las TIC en la formación de docentes, lo cual se relaciona con un uso limitado de las estrategias, para lograr competencias digitales en los estudiantes, las cuales deben promoverse a fin de lograr las habilidades necesarias para un uso responsable y adecuado de dichas herramientas, tanto en los procesos académicos como en la vida personal.

2.1.4. Investigaciones sobre el rol de las instituciones y personal administrativo

Es de suponer que, las administraciones de las instituciones educativas pueden invertir en redes con servidores confiables que permitan la protección de sus datos, capacitando al personal administrativo. Además, de concientizar a los docentes y estudiantes sobre el uso seguro de las Tic sobre todo en internet, por esta razón, en esta investigación se observan estudios en este ámbito.

De tal modo, Chiliquinga (2020) en su tesis doctoral, analiza la seguridad digital en la implementación de las TIC durante el confinamiento por la pandemia COVID- 19, para el desarrollo de las clases virtuales. El uso de estos recursos digitales educativos también ha dado

la oportunidad a los delincuentes informáticos (hacker) de obtener informaciones personales a través de las bases de datos de los usuarios.

Señala la investigadora que, a partir de la identificación de los procesos empleados por estos delincuentes, se pueden abordar las debilidades, mediante la implementación de programas y softwares institucionales para la protección y seguridad a los usuarios en línea. No obstante, esto también requiere un cambio en cuanto a la inversión para administración de los servicios digitales, equipos y energía, en resumen, mayores gastos institucionales. Destaca además que el valor fundamental debe ir dirigido a lograr en los usuarios un mayor conocimiento en el uso de la tecnología en cuanto a las medidas de seguridad informática.

Por este motivo es pertinente que, los centros educativos dispongan de una red segura que permita la protección de los equipos y los datos administrados en ella, y definitivamente este aporte se constituye en baluarte a efectos de la presente investigación, ya que se alerta sobre un punto débil, representado en el cuerpo de personal administrativo de una institución educativa, en cuanto a consciencia de seguridad digital.

Asimismo, Narváez (2019), llevó a cabo un estudio dirigido a analizar las vulnerabilidades existentes en la red de la empresa *Hidromag* en Ecuador que pueden incidir en la infraestructura de los sistemas informáticos de la organización, con miras a diseñar patrones de medidas de prevención para los riesgos identificados.

Se llevó a cabo una investigación de campo y bibliográfica bajo el método analítico-sintético, hipotético-deductivo. Los resultados encontrados indican que es posible obtener información no autorizada a través de los servicios internos y externos manejados por el último usuario, los cuales amenazan la seguridad de los datos. La mayoría de las amenazas evidenciadas para la obtención de datos, robo de identidad, intercepción de mensajes, pérdida de información se deben al factor humano por descuido, documentos compartidos o memorias internas o robo.

Si bien es cierto que la investigación precedente no se llevó a cabo en un contexto educativo, no deja de representar un aporte valioso a efectos del presente estudio, pues se evidencia el común denominador del personal administrativo de ambas organizaciones, en cuanto a debilidades de seguridad digital y sus consecuencias. Cabe destacar así, que, desde esta revisión, hay un aporte en la óptica del alerta y posibles soluciones, encaminadas a la capacitación del personal administrativo escolar.

2.1.5. Investigaciones sobre ciudadanía digital

Desde la perspectiva axiológica abordada en esta investigación es fundamental la noción de ciudadanía digital, la cual constituye la meta a lograr a través de las competencias digitales y la seguridad informática. Por ello se plantean hallazgos en este aspecto.

En este sentido, González-Andrío et al (2020) presentaron un estudio cuyo objetivo fue comprender los efectos de la utilización, difusión y elaboración de las redes sociales sobre la ciudadanía digital. Se llevó a cabo un estudio descriptivo de enfoque mixto a través de un cuestionario en línea. La muestra estuvo constituida por 127 estudiantes españoles.

Los resultados mostraron que los jóvenes destacan que, los problemas éticos en las redes sociales son los cuestionamientos más relevantes, destacando el engaño, la crueldad, el ciberacoso, la desacreditación de personas a través de las redes, la intolerancia, los prejuicios y los discursos que generan odio o rencor.

Desde estos resultados, los autores discuten sobre el concepto de ciudadanía digital y las responsabilidades inherentes a las relaciones en la web, ya que evidencian que estas afectan tanto positiva como negativamente el concepto de participación e interacción ciudadana.

Al momento de llevar a cabo la planificación educativa se deben tomar en cuenta actividades que sean interactivas, motivadoras, innovadoras, que mantengan al grupo trabajando con armonía, entusiasmo, y que promuevan los valores y principios de la responsabilidad digital. Definitivamente este aporte en el plano axiológico enriquece el estudio llevado a cabo, pues garantiza una visión certera y guiada en posibles respuestas que coadyuven en la entrega de un cuerpo de medidas de seguridad, las cuales contemplen la ética y los valores contemplados en el currículo escolar.

Al respecto, Marín et al (2021) llevaron a cabo una investigación de revisión sistemática de literatura en torno a los procesos de ciudadanía digital con la finalidad de detectar las tendencias científicas predominantes. Se realizó un estudio descriptivo de carácter retrospectivo en las bases de datos Scopus y Web of Science, y se seleccionaron 87 artículos.

Las competencias digitales que se destacan en las tendencias estudiadas son: 1) Información y alfabetización informacional; 2) Comunicación y colaboración; 3) Creación de contenidos digitales; 4) Seguridad y 5) Resolución de problemas).

Los investigadores concluyen que la utilización de TIC como mediadores didácticos en la enseñanza y aprendizaje no sólo tienen un impacto positivo en el desarrollo académico, sino también, en el aprendizaje de habilidades para la vida y la formación de ciudadanos digitales. Asimismo, detectaron que las competencias más importantes se identifican en las capacidades en las áreas de Información, alfabetización informacional y comunicación. También encontraron que las competencias digitales se relacionan con la edad y el nivel educativo, siendo fundamental en procesos tales como la motivación, participación ciudadana y trabajo colaborativo.

Los antecedentes expuestos sobre las investigaciones sobre: (a) uso de las TICCAD en estudiantes; (b) capacitación docente en TICCAD, (c) competencias digitales; (d) el rol de las instituciones y personal administrativo; y, (e) ciudadanía digital se constituyen en valiosos aportes que apuntalan el espíritu de la presente investigación llevada a cabo. Por una parte, dan luz sobre determinantes que realzan y validan la problemática planteada y por otra, contribuyen a concebir posibles respuestas al presente estudio doctoral.

Además, en la síntesis de la información recogida en este estado del arte, se enfatiza la necesidad de un mayor abordaje de los trabajos sobre seguridad y competencias digitales en las instituciones educativas que permitan comprender los distintos factores que limitan el acceso seguro a los recursos tecnológicos educativos, y que de dichos hallazgos, se deriven líneas de investigación enfocados en el énfasis y compromiso de los docentes, personal administrativo y estudiantes, en cuanto el uso seguro, consciente , apropiado y eficaz de las tecnologías educativas.

2.2. Bases Teóricas

A continuación, se exponen las bases teóricas que fundamentan la investigación, refiriendo en primer lugar los procesos tecnológicos inherentes a la competencia digital que posteriormente son vinculados a la educación virtual. Seguidamente se consideran los postulados de la seguridad informática y la ciber ética, que permiten comprender el concepto de ciudadanía digital, así como las habilidades y competencias requeridas para lograr este principio axiológico.

Finalmente, se cierra con las teorías de enfoque constructivista que son parte de la investigación y que son tomadas en cuenta debido a los procesos interactivos que existen en la

relación a través de los medios tecnológicos. Cabe destacar que, en el desarrollo de este marco teórico se consideran los aportes de distintos autores, los cuales son complementados por la interpretación de la autora a fin de lograr un marco explicativo requerido según el método hermenéutico-dialéctico que apoya la presente investigación.

2.2.1. Competencias digitales y habilidades en el uso de las TICCAD

La competencia digital se refiere a las habilidades en el empleo de los medios digitales para la recuperación y evaluación de la información y su procesamiento; dichas competencias dependen del desempeño de habilidades informáticas que se han adquirido en el proceso de formación.

En este sentido, Reche et al (2019) plantean que el aprendizaje de las competencias informacionales (CI) en los estudiantes y docentes es esencial para lograr la meta propuesta en el modelo educación por competencias y las destrezas para las fases de la evaluación de calidad, búsqueda de información y el tratamiento de comunicación de nuevos conocimientos. De una forma más precisa, los autores entienden por competencia, al grado de la capacidad, el análisis, el razonamiento, la alfabetización y la comunicación fluida en las diferentes áreas del saber.

Evidentemente, las competencias digitales son fundamentales para el logro de un aprendizaje activo y cooperativo, en el entorno de las TICCAD, que permita a los estudiantes vincularse con las plataformas educativas digitales y adquirir nuevas habilidades gracias a la capacidad de seleccionar y transformar rápidamente dicha información según la calidad y cantidad de la misma, (Hernández et al 2016).

Paralelamente, la interacción con estos entornos no puede ser ilimitada, sino que debe estar respaldada por un sistema seguro que garantice que la información y los datos son de estricto uso personal y educativo.

Dicho lo anterior, en la siguiente sección se describen distintos componentes de las competencias digitales, de acuerdo con lo que se integra en la revisión de diferentes autores. Estas competencias se han considerado en el desarrollo del apartado metodológico de la presente investigación (Tabla 1).

Dominio cognitivo, procedimental y actitudinal de las TICCAD

Según Edel (2020), las competencias digitales poseen una dimensión cognitiva relacionada con las destrezas, saberes, conocimientos y habilidades de pensamiento. Una dimensión procedimental, que se refiere al nivel de apropiación de las TICCAD acerca de su empleo, uso, usabilidad, utilización, aplicación e implementación, y una dimensión actitudinal que consiste en la apropiación de las TICCAD en virtud de los actos, conductas, disposición, comportamiento y aceptación.

Los dominios que refieren a las competencias digitales indudablemente están relacionados con procesos específicos que refieren a una intencionalidad o conciencia en el uso de la tecnología. La intencionalidad en el uso de la tecnología va a depender de la disposición emocional del individuo, sumándole el factor tiempo, edad y actividad o función que desempeñe profesionalmente.

En el caso de la aplicación para uso educativo, la intencionalidad del docente o investigador se evidencia en la búsqueda permanente de actualización acorde con el avance de la tecnología hasta lograr la apropiación tecnológica y las estrategias necesarias para cumplir sus objetivos en la docencia o en la función que desempeñe en la organización o institución.

Al respecto, Según Meza y Moya (2020), la intencionalidad tecnológica implica una acción consciente en el uso pedagógico y didáctico de las herramientas, en la cual se genera la capacidad de vincular procesos aparentemente aislados en un contenido que permite el cumplimiento de los objetivos planteados. Esto permite que, en el proceso didáctico en un contexto ausubeliano, los estudiantes sean capaces de construir significados a partir del conjunto de actividades, permitiendo no solo la incorporación de conocimientos, sino que cada experiencia tiene un sentido.

Capacitación continua

La formación en competencias digitales por parte de los profesores es esencial para enfrentar los retos del sistema educativo en la actualidad, Reche et al (2019). La prioridad de esta formación es reforzar las actualizaciones en competencia digital. Por tal motivo, las

políticas educativas a nivel mundial establecen mecanismos para promover la actualización docente en las tecnologías y su aplicación en la didáctica de sus cursos.

En la República Dominicana, el programa de transformación digital comienza con la implementación del proyecto República digital en el 2017, proporcionándole a todo el personal docente, directivos y estudiantes computadoras o tabletas. Asimismo, la integración de profesionales expertos en tecnología asignados a los centros educativos desempeñándose como tutores y facilitadores para capacitar al personal de los centros educativos, distritos, regionales, técnicos nacionales, impulsando la apropiación TIC.

El mismo 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 (Marcelo et al 2019). Los procesos de capacitación continua de los docentes también implican un mayor desarrollo y destreza en el uso de las TICCAD para su empleo seguro.

Innovación e investigación educativa

La innovación y la investigación educativa son competencias fundamentales en la educación mediada por las TICCAD. La innovación es el proceso de transformación de los principios tradicionales en el proceso de enseñanza aprendizaje que es susceptible de generar nuevos conocimientos, a través de diversas estrategias creativas, entre los cuales destacan los MOOC (Massive Online Open Course), como plataformas que permiten diversidad de recursos y favorecen la actividad colaborativa.

Por otro lado, se mencionan los proyectos de innovación educativa que abarcan la diversidad de metodologías y estrategias del docente en los cuales la actualización tecnológica está presente, tal es el caso de la clase invertida, la innovación revolucionaria, la innovación incremental o la mejora continua. Asimismo, otros modelos de innovación educativa suponen la incorporación de elementos tecnológicos multimediales basados en las artes para promover el desarrollo del pensamiento complejo en áreas de conocimiento específicas, Sánchez (2019).

Es fundamental que la innovación educativa también se relacione con el desarrollo de habilidades de pensamiento crítico y uso creativo de las TICCAD, ya que no puede existir innovación sin una completa consideración de las utilidades y fortalezas de las tecnologías para aportar al avance del conocimiento.

En tal sentido, se considera que las competencias digitales son procesos que comprenden diversas dimensiones necesarias en el desempeño del docente, en el cual, la interacción discente-docente e institución educativa constituyen piezas claves que promueven la innovación.

Ahora bien, la innovación es posible gracias al fomento de la investigación. Uno de los aportes positivos que se atribuye a internet con fines educativos es la posibilidad de investigar información de forma amplia a través de infinidad de medios accesible.

Desde esta perspectiva, Castillo-Fonseca (2019) interpreta que la investigación va de la mano con la ciencia, y es el proceso crítico, sistemático que abarca desde el razonamiento, el procedimiento, la metodología y la tecnología que permiten obtener datos concretos o informaciones, en la búsqueda de mejoras de los conocimientos. Al mismo tiempo, el autor señala que, la investigación ayuda a otros investigadores a realizar sus publicaciones fortaleciendo su área de desempeño y disciplina.

Al considerar la importancia de la investigación en el desarrollo de las competencias académicas, Martin et al (2017) especifican que un investigador es un profesional con conocimientos, preparación en las prácticas educativas y metodológicas, las estrategias, los valores éticos y morales; dedicado, además, a la investigación científica, competencia que ha sido estimulada y fomentada en las propuestas educativas más recientes.

Por tal motivo, los sectores públicos y privados del sistema educativo promueven la formación de los investigadores de las instituciones proporcionando recursos e incorporando jóvenes a la investigación, a través de un uso responsable y seguro de los recursos digitales, asignando espacios como laboratorios, bibliotecas que fomenten la investigación científica. Es así como, según indica Gallego-Arrufat et al (2019), la investigación constituye uno de los pilares considerados en las competencias digitales de los estudiantes, y por tal motivo, en la presente investigación se plantea como un elemento fundamental y de suma relevancia.

Alfabetización digital y habilidades informáticas

Uno de los temas más considerados en los procesos de incorporación de las tecnologías en la educación se refiere a la alfabetización digital. Al respecto, Sánchez-Duarte (2019), expresa que los docentes y estudiantes necesitan una formación constante en los principios de los recursos digitales, conocido también como alfabetización digital.

Este autor observa que, si bien se conoce que la mayoría de los estudiantes son nativos digitales, la alfabetización digital debe ser para todos los involucrados en la acción formativa y en los diferentes sectores de la ciudadanía digital, incluso para los jóvenes que desde su infancia han estado vinculados activamente a las tecnologías.

Este proceso de alfabetización ha sido comparado con el aprendizaje de una segunda lengua que requiere la relación con la nueva gramática y vocabulario a través de didácticas específicas. Asimismo, los nativos digitales necesitan nuevas metodologías para lograr tener competencias digitales que permitan interacciones más avanzadas con las posibilidades académicas del mundo virtual e interactuar de forma segura y responsable conforme a los nuevos tiempos. Por tal motivo, la alfabetización digital no implica únicamente saber emplear los comandos de las herramientas tecnológicas sino adquirir el uso crítico y responsable para un buen uso de las TICCAD con fines académicos.

Relacionado con lo anterior, se considera que una vez adquirida la alfabetización digital el logro de competencias digitales debe ir orientado hacia la adquisición de habilidades informacionales y habilidades informáticas, dos destrezas que suelen ser confundidas y que a continuación se aclaran.

Las habilidades informacionales son destrezas trascendentales propias de un investigador a nivel global que se asocian al acceso a la información y el conocimiento a través de herramientas tanto tecnológicas como educativas, tomando la investigación como destreza principal que conlleva a mejorar las funciones formativas con mayor eficacia, (Rodríguez et al 2018).

No debe olvidarse que las TICCAD integran un sistema global de comunicación e información, por tanto, las habilidades informacionales se relacionan a los recursos con los que cuenta el usuario (en este caso, docente y estudiante) para acceder al conocimiento a través de dicho sistema. Por su parte, las habilidades informáticas son destrezas que especifican el grado

de apropiación tecnológica que posee el individuo y se asocian con la eficacia en el resultado de un proceso (Mora et al 2019).

Es decir, son las capacidades individuales para acceder a dichos sistemas informacionales, haciendo uso de las propias competencias para efectuar una relación efectiva con el dispositivo tecnológico. En el sistema educativo, estas habilidades se relacionan con las capacidades que el docente tiene para diseñar las distintas actividades establecidas en el entorno virtual.

Con lo expuesto, puede interpretarse que, las competencias digitales requeridas faciliten el proceso de enseñanza-aprendizaje, por cuanto, integran tanto las habilidades informacionales como las habilidades informáticas con las que cuentan docentes y estudiantes.

Empleo de las TICCAD en la educación virtual

Tal y como se ha venido exponiendo en el desarrollo de este trabajo, la integración de las tecnologías como herramienta pedagógica es el complemento para fomentar el proceso de enseñanza aprendizaje, tanto en las clases presenciales como en la modalidad a distancia y semipresencial, ya que promueven un conjunto de habilidades que generan una mayor autonomía en el estudiante, propician el trabajo colaborativo e interactivo, todo ello gracias a la flexibilización de las prácticas pedagógicas y a la integración de contenido multimedia que permite el acceso a distintos recursos textuales y no textuales (Díaz et al 2018). Por tal motivo, el empleo de las TICCAD debe estar asociadas al desarrollo de las competencias digitales tanto de los docentes y alumnos que permitan su optimización.

En la educación virtual se utilizan estrategias y modelos colaborativos que mejoran el proceso de enseñanza aprendizaje por medio de la construcción colectiva de conocimientos que permite la realización de proyectos mediados por herramientas tecnológicas y softwares interactivos, Miguel-Vallés (2017).

Esto promueve la discusión entre el maestro y el alumno, atendiendo a las diferentes áreas requeridas, las cuales pueden llevarse a cabo con una comunicación sincrónica y asincrónica, uso de chats, videos o MOOC. El autor señala, al respecto, algunos elementos importantes para el trabajo colaborativo como responsabilidad por parte de cada miembro,

trabajo en equipo, solidaridad, respeto mutuo, trabajo cooperativo, interdependencia, liderazgo, capacidad para la resolver conflictos y negociación o consenso de ideas.

Por otro lado, el docente puede reforzar los aprendizajes no sólo a través de las estrategias evaluativas, sino también, con la coevaluación y otras actividades que pongan en evidencia las competencias socioculturales e interculturales.

Una de las grandes ventajas de la educación mediada por la tecnología es el apoyo de contenidos multimedia e hipertextuales que promueven la innovación y la interacción, ya que están compuestos por informaciones sonoras, fotográfica, audiovisual, textual, siendo almacenados como archivos digitales. Bajo esta óptica, Acosta (2020) explica que el diseño de contenidos multimedia son vías de comunicación relevantes que permiten que la exposición de los materiales didácticos pueda ser realizada por distintos medios que propician el aprendizaje.

Es así como el contenido textual no se limita a información en documentos *Word* o pdf, sino que también puede ser presentado a través del uso de etiquetas, bloques, encabezados o tablas que permitan la navegación eficiente y motivadora. Asimismo, se cuenta con formatos AVI, MIDI, MP3, MP4, Flash, donde se toman los requerimientos como subtítulos, transcripción, audio suave, video y el audio descripción que son recursos fundamentales para complementar la información en formatos diversos y accesibles.

Estos recursos además pueden ser enlazados con otros recursos de acceso abierto como la plataforma YouTube, permitiendo llegar a todo público y del mismo modo, acceder rápidamente a un contenido específico que ya ha sido difundido. Cuando los contenidos digitales son almacenados en plataformas como Moodle, es posible guardar de forma segura y permanente los archivos digitalizados, lo cual es un buen indicador para la investigación presente.

Interacción, colaboración y divulgación en plataformas virtuales

Indudablemente, las plataformas virtuales promueven y se sustentan en la interactividad y la colaboración, ya sea de forma síncrona o asíncrona. En cuanto a ello, Mejías-Madrid (2019) señala que gracias a las herramientas digitales de las cuales se dispone, es posible desarrollar estrategias colaborativas que promueven competencias digitales de los estudiantes; sin embargo, dichos procesos interactivos dependen de la capacitación y dominio que muestran los docentes para poder proporcionar los recursos adecuados para el desempeño de los alumnos, así como de

la plataforma de la cual dispone cada centro educativo. Además, en la interacción de plataformas virtuales se trabaja de forma creativa y significativa.

Los docentes de hoy interactúan con estudiantes que son nativos digitales, los cuales poseen capacidades altamente eficaces en el uso de las tecnologías; por tal motivo, es necesario que el uso de los recursos digitales se fundamente de manera primordial en la interacción docente-alumno basadas en los entornos multimedia e hipertextuales. Al respecto, Mujica-Sequera (2020), expresa que la mayoría de los estudiantes de hoy día aprenden con más facilidad, a través de las plataformas virtuales debido a las facilidades comunicativas docente-estudiante y estudiante-estudiante que ofrecen dichos ambientes.

Es por todos conocido que la información que circula a través de internet es de acceso público y llegan a innumerables personas. Los contenidos digitales no académicos se divulgan a través de páginas web que son accesibles a través de Google o Youtube. Sin embargo, es necesario también mencionar el contenido académico y científico que circula a través de bases de datos, bibliotecas, repositorios en línea, revistas, los cuales tienen como misión compartir recursos e informaciones que favorezcan las necesidades docentes y del investigador. Además, compartir proyectos y experiencias científicas para la comunidad académica. La consulta de estos recursos digitales científicos debe ser también promovido en los estudiantes como parte de sus competencias digitales (Martín y Lago, 2021).

Sin embargo, el acceso libre a información electrónica ya sea científica o no, permite también la práctica del ciberplagio, que consiste es la apropiación de contenidos digitales de otra persona sin previa autorización, sin las debidas normas de citación y sin respetar el derecho de autor. En este aspecto, según Gallent y Tello, (2017), esta práctica no sólo atenta contra de la moral de la investigación científica, sino que también permite que las estrategias de investigación no sean suficientemente responsables, especialmente en los estudiantes. Por ello, uno de los requerimientos de la ciudadanía digital debe ser inducir a la concientización de la autoría y la prevención del plagio de las informaciones encontradas.

2.2.2 Uso seguro de las TICCAD en educación

Tal y como ocurre en cualquier organización, las instituciones educativas requieren el establecimiento de medidas de seguridad informática para proteger la información existente, la cual no sólo refiere a datos personales de los distintos actores, sino que también, al acceso a

información como notas académicas o información bancaria de usuarios y de la propia institución. Cuando los estudiantes o docentes acceden a una red institucional es posible que mucha información quede expuesta, permitiendo así el acceso de terceras personas.

Con lo arriba expuesto, se aborda la caracterización de las competencias digitales como una categoría fundamental a abordar en la presente investigación. El siguiente apartado se enfoca en la seguridad informática en educación, un tema que según se ha logrado evidenciar ha sido poco abordado en la literatura. No obstante, el aspecto de la seguridad es tan importante, que se presenta como una preocupación latente especialmente en las instituciones de educación superior, tal y como señalan Morales et al (2019), quienes además indican que las instituciones educativas públicas son más vulnerables que las privadas, ya que carecen de sistemas específicos de protección.

Por lo cual, en el desarrollo de este apartado se presentan distintas consideraciones en el tema de la seguridad informática en educación, los cuales han permitido la exposición del marco metodológico de la presente investigación (Tabla 1).

Riesgos en el manejo de la información en instituciones educativas

La seguridad informática se refiere a los procesos de protección que se llevan a cabo en un sistema en red, los cuales implican una diversidad de acciones como respaldos de datos, disponibilidad de información, confidencialidad de usuario, e integridad, garantizando que las informaciones no sean manipuladas por terceros (Gaitan, 2020). Para que exista seguridad informática existen diversos mecanismos, algunos referidos a las medidas de seguridad de los dispositivos tecnológicos, y otros referidos a las prácticas de los usuarios.

En cuanto a los dispositivos existentes en las instituciones educativas, es necesario establecer una política en la cual se inviertan recursos que garanticen la seguridad informática para la ejecución de los programas, como el caso de la criptografía para encubrir datos confidenciales, protegerlos de otros usuarios mal intencionados, y aun con acceso al documento otra persona que no sea el receptor no pueda ver o descifrar el mensaje (Sánchez, 2019).

Además, otros aspectos relacionados con la seguridad se deben al factor humano, tal y como indica Narvaez (2019), ya que la mayoría de las amenazas evidenciadas para la obtención

de datos, robo de identidad, intercepción de mensajes, pérdida de información se deben al factor humano por descuido, documentos compartidos, memorias internas olvidadas o robo.

Como ya se ha venido relatando, internet es una gran fuente de información de todo tipo a la cual pueden acceder personas de cualquier edad, nivel educativo o interés. Como fuente de información, internet no está exenta de riesgos y amenazas, no sólo a la seguridad, sino que también, a la integridad de los individuos. Es así como Pons (2018), señala que es fundamental identificar los tipos de ataques cibernéticos que existen y sus fines, a fin de establecer las medidas de protección pertinentes en internet.

Algunos de estos ataques o vulnerabilidades tienen intensiones simples, como el *hacking* que, por diversión, aunque también existe el hackeo con la finalidad de cometer estafas, actos terroristas o apropiarse de información sensible o confidencial. A esta conducta se le agrega el *pishing*, que se dedica a robar identidades a través de mensajes por ventanas emergentes o anuncios en internet y mensajes a correos a los usuarios, generalmente con fines de estafas.

Otra conducta que vulnera la seguridad en la red es el g*rooming* orientado al acoso sexual de jóvenes especialmente menores de edad y las redes de pornografía infantil. De allí, la importancia de implementar aplicaciones y herramientas que ayuden a detectar los hackers informáticos con el descifrado de los usuarios mal intencionados.

Por otro lado, las grandes compañías que poseen informaciones proporcionadas por los propios usuarios, como videos, fotos o datos personales a través de plataformas virtuales o redes sociales, archivan estos datos que pueden ser publicados o utilizados posteriormente con otras empresas para fines lucrativos, lo cual permite afirmar que no hay privacidad en internet y es a criterio del propio usuario acudir a los mecanismos que pueda seguir para garantizar su seguridad y confidencialidad (Martínez-Béjar, 2020). No cabe duda que en las instituciones educativas los estudiantes están continuamente accediendo a redes sociales, lo cual permite la exposición de su información personal, sin mencionar que el acceso a redes abiertas puede vulnerar la información institucional.

Medidas de seguridad informática

El aprendizaje de los estudiantes depende en gran parte de las estrategias implementadas por el docente y en este caso, las destrezas en seguridad informática resultan fundamentales. Si

bien queda claro que en la mayoría de los casos los estudiantes son nativos digitales, en la educación virtual el docente debe mostrarse competente, innovador, investigador haciendo uso de las tecnologías como medio para integrar en su planificación diaria y desarrollando actividades con un diseño instruccional claro y coherente que esté acompañado de un adecuado protocolo de seguridad.

Por tal razón, el docente no sólo debe poseer destrezas en cuanto a las tecnologías, diseño instruccional y constantes actualizaciones que le permitan una apropiación que facilite el uso de estas, sino también, como señala Fernández (2017), conocer diferentes herramientas o aplicaciones que permitan un entorno seguro, atendiendo a las diversidades de los alumnos y favorezcan la transferencia y construcción de conocimientos con flexibilidad y trabajo colaborativo

Por su parte, los estudiantes demandan empoderamiento del estudio con apropiación tecnológica, capacidad de resolución de problemas con autonomía, capacidad de trabajo en equipo, liderazgo, iniciativa propia y creatividad (Fernández, 2017). No obstante, debe considerarse que los estudiantes suelen poseer destrezas en el manejo de la tecnología que muchas veces superan las habilidades del docente.

Por ello también tienen otros requisitos como acceso inmediato e ilimitado a la información y accesibilidad a distintos formatos (textuales y multimedia). Adicionalmente, los recursos didácticos virtuales ofrecen al estudiante la posibilidad de acceder en un mismo entorno a las tareas y actividades, así como a los espacios de sus entregas, permitiendo una gestión más adecuada del tiempo y los recursos.

Según indican Viteri et al (2021), el empleo de dispositivos tecnológicos portátiles como computadoras y celulares les permite a los estudiantes acceder a una amplitud de información que no solo tiene que ver con los contenidos suministrados por el docente, sino la posibilidad de vincular otras materias y adicionalmente de investigar en la web sobre los temas requeridos. Esto ha permitido que en la actualidad los jóvenes dispongan de una mayor cantidad de recursos que siendo bien aprovechados bajo los principios de la seguridad informática, la competencia y la ciudadanía digital, les abre las puertas para el conocimiento.

Indudablemente, las actividades realizadas en las instituciones educativas tanto públicas como privadas, se llevan a cabo generalmente a través de sistemas de redes informáticas donde están relacionado una serie de dispositivos electrónicos como computadoras, *routers*, red Lan,

Wan, *Man*, repetidores, servidores, donde a través del internet se pueden tener acceso a las redes instaladas en los diferentes departamentos, según indica Gaitán (2020).

Así, una de las vulnerabilidades más importantes que pueden afectar la seguridad son los dispositivos en red, configuración que puede encontrarse con mucha frecuencia en instituciones educativas. Por ello, es necesario que la protección o ciberseguridad logre garantizar la disponibilidad, confidencialidad, integridad, discreción de las informaciones, equipos, y de los programas interconectados a través del internet.

Además, Salazar et al (2021) proponen reglas y técnicas de ciberseguridad que pueden considerarse en la institución, tales como la autentificación de contraseñas, bases de datos, servidores, uso de firewalls y VPN que impiden filtración a la red; asimismo el endurecimiento de sistemas operativos y encriptación de datos para probar la confidencialidad de informaciones de manera de garantizar que los datos que se manejan en las instituciones permiten un acceso seguro.

Indudablemente, los ataques informáticos intencionados que se realizan con cualquier finalidad causan la violación de la privacidad y acceso a la información confidencial. En este sentido, Baca (2016) explica que la efectividad de la prevención del riesgo va a depender del costo de inversión, de los aparatos electrónicos y del personal calificado para manejar adecuadamente el sistema en la institución.

De igual forma, para la instalación de los sistemas de seguridad informática institucional se debe tomar en cuenta que el plan sea adecuado a la necesidad para poder proteger los datos. Ahora bien, este es un aspecto importante a tomar en cuenta que, la mayoría de las instituciones educativas cuentan con presupuestos limitados para el equipamiento electrónico, razón por lo cual, un gran porcentaje de la prevención de riesgo, debe estar enfocado en la capacitación del recurso humano, en estrategias que reduzcan las vulnerabilidades y en la seguridad de la información.

Ciudadanía digital y comportamiento académico responsable

Para Balderas (2021), el comportamiento académico en la seguridad informática se refiere a la evidencia de conductas y manejo de destrezas para el apoyo, la colaboración y la dirección, a través de los medios digitales que fortalecen tanto los conocimientos como el

manejo responsable por parte de los estudiantes de los distintos sistemas y contenidos a los cuales se accede. El comportamiento académico responsable en la seguridad informática va de la mano con la ciberética y la ciudadanía digital, y son parte de la axiología humana, como un proceso orientado a la búsqueda de responsabilidad y elección de las diferentes informaciones accesibles a través de las tecnologías (Prado, 2021).

Por tal motivo, es importante tratar las implicaciones humanas en las vulnerabilidades que existen a través de la web y que presentan con mucha frecuencia en la práctica docente debido al desconocimiento o mal manejo de las medidas de seguridad de las cuales dispone la institución o al uso de los dispositivos tecnológicos personales de los estudiantes.

De igual forma, Pons (2018), manifiesta que la ciudadanía digital procura la seguridad informática, puesto que contempla la protección individual y colectiva ante cualquier ataque informático en sus diferentes modalidades. Sobre la base de esta idea, dicha responsabilidad implica una diversidad de acciones que limitan al entorno institucional, además del uso de las TICCAD en el hogar, tomando en cuenta que las tecnologías están llamadas a satisfacer necesidades personales, educativas o laborales. En tal sentido, en este proceso están implicados educadores y padres en el cumplimiento de las normativas de seguridad que son requeridas y sancionadas legalmente, 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".

Así que la seguridad informática en el entorno académico requiere de un proceso de capacitación y socialización que permita a los docentes tener las habilidades críticas para comprender la importante función en el resguardo de la información personal y de la institución, así como del acceso de los estudiantes a los distintos contenidos que se le proporcionan (Cano, 2015). Esto permite suponer que la información académica segura debe tener un uso pedagógico o didáctico claro y fomentar el empleo proactivo y responsable de las herramientas proporcionadas.

Ética en la seguridad informática

El comportamiento ético se refiere a las conductas y destrezas autónomas y conscientes empleadas por el estudiante y el docente para proteger la privacidad en línea y la libertad de expresión (Balderas et al 2021) Desde la axiología y la conducta humana es necesario considerar y tomar en cuenta las implicaciones en el individuo de la libertad y la responsabilidad que son inherentes a los riesgos del uso inadecuado de las tecnologías.

Por tanto, en este ámbito se considera que la seguridad informática en una institución educativa no es un tema únicamente técnico, sino que también tiene implicaciones éticas. Al mismo tiempo, Pérez (2018), expone que es necesario integrar los valores de la responsabilidad personal y la responsabilidad institucional, para ello se requiere establecer medidas o modelos de mediación que permitan identificar como cada individuo percibe o incorpora los valores inherentes a la seguridad de los datos personales y compartidos.

Estas mediaciones deben estar contenidas en las normas y los valores institucionales, pero adicionalmente, la conducta de cada individuo debería ser monitoreada, a través de un planeamiento educativo institucional que permita un buen desempeño en materia de ciber seguridad.

Además de estos principios normativos, es necesario señalar los valores humanos que provienen de los hogares y que repercuten en las relaciones de los niños y niñas en las escuelas, tanto en la relación social, como en el plano académico, donde también está involucrado el buen uso de la tecnología (Arévalo, 2021).

De acuerdo con lo planteado por la autora, se puede agregar que, en la familia se deben tomar en cuenta ciertas características que definen la forma de ser y actuar de los miembros que la conforman entre los que podemos citar la comunicación, la convivencia del sistema familiar, y la convivencia social, siendo estos factores imprescindibles cuando se considera desarrollar conciencia y responsabilidad en la seguridad informática. Es así como el comportamiento ético en el uso de las tecnologías se vincula con el concepto de Ciudadanía Digital.

Por otra parte, en el mundo globalizado, la ciberética es aún un tema pendiente, tal y como queda demostrado en un estudio realizado por Dans et al (2019) quienes señalan que las redes sociales es el sistema digital más usado por los jóvenes, accesible en un 89% a través de teléfonos inteligentes. En EEUU el 54% de los jóvenes aseguran acceder a ellas con tiempo

excesivo y el 72,5% del personal educativo incluyendo las familias de los estudiantes, consideran como efectivo el uso de las redes sociales.

Esto se asocia con una inadecuada supervisión por parte de las instituciones y las familias sobre el comportamiento de los jóvenes en el mundo digital, tomando en cuenta las medidas de restricción necesaria sobre el tipo de aplicaciones utilizadas y el tiempo de uso, lo cual permite la existencia de conductas inseguras como el ciberbullying, la suplantación de identidad y el robo de información, entre otras.

Cabe destacar que, como iniciativa en la República Dominicana, el ministro de Educación Dr. Roberto Furcal, ha integrado al currículo dominicano, en enero 2022, las Cátedras Ciudadanas que cumplen con un eje del plan estratégico, lanzando un nuevo modelo con la finalidad de transformar críticamente el sistema de valores cívicos, en el cual indudablemente está involucrado el buen uso de las tecnologías e internet. Este es un paso encaminado hacia el logro de estudiantes responsables digitalmente.

Apropiación responsable y aceptable de las TICCAD

Según se ha mencionado en los apartados anteriores, el uso seguro de las TICCAD requiere un proceso de autonomía y actualización consciente de las ventajas y las vulnerabilidades existentes en el uso de éstas. Es por ello que para Balderas et al (2021) el manejo apropiado y socialmente aceptable, implica la percepción de los actores educativos en cuanto al nivel de manejo y destrezas en las tecnologías.

Tal y como se ha venido exponiendo, las tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) forman parte del quehacer diario en el individuo que exigen aprender y reaprender habilidades que no sólo se refieren al manejo tecnológico, la innovación o la investigación científica, sino al intercambio de saberes, la responsabilidad y la ética orientada a propiciar ciudadanos responsables, críticos, con eficiencia y eficacia, autonomía, participación, capaces de resolver problemas tecnológicos, de seguridad informática desde la ética y la moral. Por tal motivo, en la presente exposición se consideran los aspectos que permiten relacionar las formas de apropiación de las tecnologías con las destrezas y competencias necesarias para una aplicación crítica de los recursos informáticos.

Se ha expuesto, cómo la seguridad informática puede ser violentada por agentes externos o por prácticas poco seguras de los propios usuarios. Sin mencionar las prácticas intencionales

de robo de información o de uso de imágenes que vulneran la dignidad de adultos y niños. Queda en evidencia que, las informaciones subidas por las personas a las redes sociales en internet con frecuencia son transportadas con fines de comercialización (Martínez-Béjar, 2020).

Según lo expresado, no basta con implementar sistemas sofisticados de seguridad informática, sino que es necesario concientizar a los actores educativos sobre las causas y consecuencias que provoca el mal uso de las tecnologías. Por tanto, es necesario generar las competencias tecnológicas para determinar la forma o el medio por el cual los datos personales pueden ser vulnerados provocando daños irreparables.

Es este aspecto, Gaitan (2020) destaca que, para garantizar destrezas aceptables en las TICCAD, se requiere contar con medidas de seguridad de manera que las actividades puedan ejecutarse con control y riesgos mínimos. En tal sentido, del lado de docentes y estudiantes se requieren de destrezas específicas de acuerdo al rol que les toca desempeñar en el proceso de enseñanza-aprendizaje. En esta línea, uno de los aspectos más importantes que se debe fortalecer en la relación docente-alumno mediada por las TICCAD son los diseños instruccionales.

En tal sentido, se define el diseño instruccional e-Learning como un proceso sistemático y contínuo mediado por internet y sus tecnologías asociadas, el cual parte de la detección e identificación de necesidades de aprendizaje y/o productividad organizacional a fin de planificar, diseñar, desarrollar e implementar las estrategias requeridas para que el estudiante adquiera competencias en un contenido o materia en particular (Álvarez, 2018).

El diseño instruccional debe considerar las técnicas y las herramientas que permitirán el logro del aprendizaje y cuál es el mejor espacio para implementarlos, además debe garantizar que los estudiantes accedan a los recursos digitales y a los contenidos de forma segura. De tal manera, según propone Mejías-Madrid (2019), un buen diseño instruccional permite que las competencias digitales de formación sean evidentes y además, pueden ser monitorizados en la práctica docente gracias a los diferentes recursos tecnológicos utilizados en el aula a través de la generación y la profundización y los conocimientos básicos de las TICCAD, permitiendo cumplir con los procesos de seguridad requeridos, tales como el acceso seguro a los recursos, uso adecuado de los sistemas de gestión de la información y confidencialidad de los datos personales.

2.3 Constructivismo y conectivismo como teorías que median en la interacción de las TICCAD

En este punto se considera la interacción a través de las TICCAD en los procesos estudiados en esta investigación (seguridad informática, competencias y ciudadanía digital) teniendo en cuenta que en la relación pedagógica se construye un espacio de mediación o individuo-individuo e individuo-tecnología que promueven aprendizajes y conductas adecuadas. Por ello, el constructivismo y el conectivismo no deben ser omitidos en este trabajo.

Al tratarse de un proceso educativo, las TICCAD son herramientas que actúan en la búsqueda de un fin, y también medios de formación y la construcción de conocimientos. En este caso, tal y como se considera desde la axiología humana, este espacio de interrelación debe ser aprovechado por el docente para el logro conjunto de competencias digitales. Dicho lo anterior, en primer lugar, se presenta el constructivismo, teoría psicológica que está integrada por importantes exponentes del siglo XX que ven la educación como un proceso relacional para el logro de las adquisiciones cognitivas.

Posteriormente, se considera la teoría del conectivismo, una teoría más reciente que a partir de algunos postulados constructivistas considera las mediaciones tecnológicas no solo como herramientas sino como lenguajes que permiten el desarrollo del aprendizaje. Finalmente se establecen relaciones entre ambas para los fines del estudio.

2.3.1 Espacios de formación de competencias digitales: Constructivismo

El constructivismo es una teoría psicológica que ha tenido importante auge a partir de la segunda mitad del siglo XX ya que permitió comprender los procesos cognoscitivos como una actividad en construcción y desarrollo a partir de las relaciones sociales. Esta teoría se nutre fundamentalmente de los aportes de la Psicología Sociohistórica de Lev Vygotsky y el Aprendizaje Significativo, de David Ausubel y ha tenido una aplicación muy importante en el ámbito de la educación porque enfatiza en el rol del docente como promotor de los aprendizajes y en el papel activo del estudiante.

Desde la perspectiva histórico social de Vygotsky, la relación colaborativa cumple un rol fundamental en el aprendizaje; en tal sentido, el profesor es un guía, que debe fomentar las oportunidades para el aprendizaje propiciando las herramientas necesarias al estudiante,

inicialmente con ayuda y luego permitiendo que éste genere sus propias adquisiciones de forma autónoma, señalando que la cultura proporciona los conceptos necesarios a través del lenguaje. según exponen Salas et al (2020),

Al respecto, Vygotsky (1978), desde su modelo sociocultural destaca las actividades de aprendizaje con sentido social, atribuyendo gran importancia al entorno socio comunicativo del sujeto, para su desarrollo intelectual y personal. Sostiene que la cognición se da en la zona de desarrollo próximo. Es decir, la distancia entre el nivel real de desarrollo y el nivel posible, mediante la resolución de problemas, siendo el aprendizaje repentino algunas veces visto en sentido de visión integradora. (p.101).

En esta teoría sobresale el concepto de andamiaje educativo, el cual establece el uso de herramientas para brindar apoyo, ampliar el alcance del sujeto, permitir la realización de tareas que de otro modo serían imposibles y usarlos selectivamente cuando se necesiten.

Por otra parte, Ausubel (1990), con la teoría del aprendizaje significativo, observa un sentido muy particular, la cual es incorporar la información nueva o conocimientos a un sistema organizado de conocimientos previos, en el que existen elementos que tienen algunas relaciones con los nuevos.

Para Ausubel, el estudiante que carece de tales esquemas desarrollados, no puede relacionar significativamente el nuevo conocimiento con sus débiles esquemas de comprensión, por lo que, ante la exigencia escolar de aprendizaje de los contenidos disciplinares, no puede sino incorporarlos de manera arbitraria, memorística, superficial o parcial. Este tipo de conocimiento es difícilmente aplicable a la práctica y, por mí mismo, fácilmente olvidado, (p.90).

Lo citado indica que las secuencias de aprendizaje deben ordenarse partiendo de los conceptos más generales y avanzados de forma progresiva hacia los conceptos más específicos, con el fin de lograr una diferenciación del conocimiento del estudiante, sí como una reconciliación integradora posterior.

En esta misma línea teórica se enfatiza que, los autores antes mencionados apuntalan el concepto de aprendizaje significativo de Ausubel, quien refiere que todo aprendizaje se construye a través de cuerpos organizados de material que permite que el estudiante pueda generar reestructuraciones a partir de las nuevas informaciones, siendo un ente activo en su

propio conocimiento. Cuando la información conocida se relaciona con la nueva información, se considera que se ha producido un aprendizaje significativo.

A tal efecto, los aportes de la teoría constructivista son relevantes para la presente investigación, ya que permite, a través del aprendizaje, representar las relaciones significativas entre conceptos propios de la tecnología educativa. En atención a que actualmente se consideran el fundamento para la red semántica de aprender a construir sobre el propio entorno, en este caso, el mundo digital en cuestión. Lo que al trasladarlo a la investigación sería de amplia profundidad, puesto que les serviría a los docentes, estudiantes y cuerpo administrativo de la institución, en sus procesos educativos, en la implicación de las TICCAD.

Las aplicaciones del enfoque constructivista a los procesos de enseñanza y aprendizaje se establecen a través del rol del docente como facilitador y la mediación de herramientas y estrategias que potencian dichas interacciones. De esta manera, el aporte fundamental del constructivismo al aprendizaje virtual y el uso de TICCAD, implica considerar que los estudiantes son quienes construyen su conocimiento en relación con las oportunidades que se le ofrecen a través de la educación con plataformas digitales (García-Varcárcel y Gómez-Pablos, 2015).

Esto hace que los materiales proporcionados y las competencias de los docentes sean fundamentales para el logro de los aprendizajes y la construcción de conocimientos en los estudiantes. Por tal motivo, puede afirmarse que las competencias digitales pueden ser elaboradas a través de adecuadas interacciones formativas que sean motivadoras y colaborativas, tal y como se explicará más adelante.

2.3.2. Educación mediada por TIC: Conectivismo

Por su parte, el conectivismo se propone como una teoría alternativa al constructivismo aplicada específicamente a la enseñanza en entornos virtuales. Se puede definir como una actividad cognoscitiva, dirigida por un docente y procesada por un estudiante para el desarrollo de habilidades, capacidades, emociones, valores, hábitos y conocimiento mediado por las TIC. No obstante, este proceso, además de la trasmisión de contenidos o la repetición de saberes, el objetivo es que el conocimiento se fundamenta en el fortalecimiento de las competencias, a través de las experiencias virtuales (Hernández et al 2016).

En el conectivismo se considera el papel fundamental del mediador tecnológico y se plantea que el aprendizaje es continuo y determinado por múltiples estímulos, por tanto, no es únicamente un proceso cognoscitivo, sino que puede estar en una base de datos en la cual se almacena información que es vital para el desarrollo del conocimiento, o puede circular a través de los contenidos que se producen en las interacciones en un Moodle o en un Mooc, Según plantea Ovalles (2014).

Desde esta perspectiva, se observa cómo las tecnologías toman un papel fundamental en el proceso de enseñanza-aprendizaje-evaluación, ya que la construcción de entornos virtuales fomenta los ambientes de aprendizaje cooperativos. Esta teoría, además, considera la importancia de la toma de decisiones, ya que frente al cúmulo de información a la cual se puede acceder a través de las TICCAD, el estudiante debe ser capaz de discernir entre información relevante e información secundaria. A partir de la información recibida en las diversas plataformas de aprendizaje, el individuo debe hacer nuevas conexiones que le permiten generar diversos aprendizajes y competencias.

2.3.3. Contribuciones del constructivismo y el conectivismo en la formación de competencias digitales y seguridad informática

Las teorías del constructivismo y del conectivismo, a efectos de la investigación llevada a cabo, pueden integrarse para comprender la aplicación de las TICCAD en el aprendizaje, considerando la complementariedad de ambas teorías. Tal y como se ha podido apreciar en las definiciones anteriores, en ambos enfoques se considera el rol activo del estudiante en el proceso de aprendizaje, permitiendo que sea el estudiante que desarrolle la capacidad de integrar y configurar la información a partir de la disposición de distintos estímulos que se presentan.

Es significativo acotar que, ambos enfoques teóricos también tienen puntos que los diferencian y que deben ser considerados. Básicamente el constructivismo es un enfoque que se basa en las adquisiciones cognitivas y materiales didácticos de cualquier índole, mientras que, en el conectivismo, se analizan los mismos procesos mediados por la tecnología y las posibilidades de información ilimitada que estas proporcionan.

Tomando en cuenta los aportes de ambas teorías, por su parte, Castillo (2008) considera que el sistema de interacción didáctica que desarrolla el docente es vital en la adquisición de habilidades y competencias por parte del estudiante, y éste debe ser capaz de construir los

conceptos a través de un proceso de interacción entre los objetos (la tecnología) y los sujetos, es decir, docente y demás estudiantes que integran el entorno de aprendizaje.

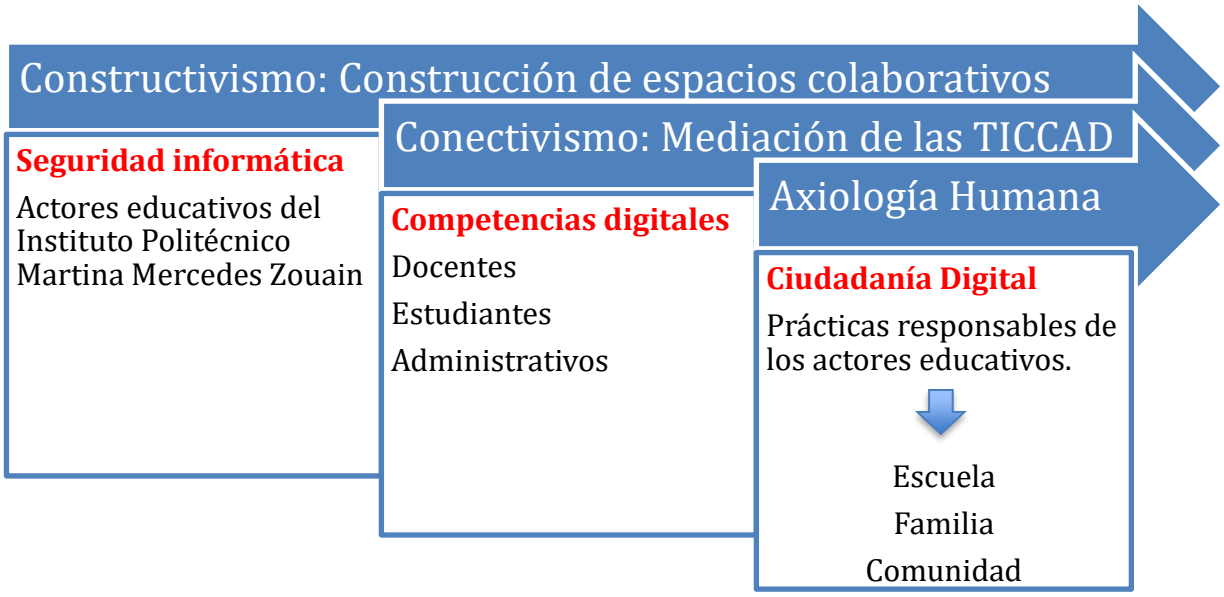
Esto sugiere que los procesos cognoscitivos que median en el aprendizaje también se están adaptando a estas formas tecnológicas. En el caso en estudio, puede señalarse que los recursos tecnológicos presentados por el docente a través de un adecuado diseño instruccional deben ser lo suficientemente claros, innovadores y motivadores para permitir el desarrollo de un conocimiento creativo que establezca conexiones con otras áreas del saber que sean significativos para el estudiante.

Cabe destacar que, como se ha venido insistiendo en los apartados anteriores, estos entornos tecnológicos deben ir acompañados de las competencias necesarias en el manejo seguro de los recursos, de forma que la relación educativa sea confiable, responsable y ética. Por tanto, siguiendo ambos enfoques teóricos, que poseen una base pedagógica importante, cualquier herramienta de mediación debe ser conscientemente empleada por el docente, asumiendo tanto sus ventajas como sus riesgos, los cuales deben ser minimizados al favorecer las competencias necesarias para un uso seguro.

Por este motivo, tomando en consideración el objetivo de esta investigación, el cual es estudiar la contribución de las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en el Instituto Politécnico Martina Mercedes Zouain, República Dominicana, puede afirmarse que las tendencias teóricas consideradas permiten abordar las tecnologías como mediadoras en el aprendizaje y la importante función y acceso al conocimiento que éstas permiten a estudiantes y docentes. En estas condiciones, el aprendizaje actualmente es mucho más rápido ya que la información está accesible inmediatamente a través de los dispositivos electrónicos, a diferencia del aprendizaje tradicional, que tiene otras características en cuanto al tiempo y el espacio.

A fines de cierre de este capítulo y a modo de integración, en la figura 1, se presenta una síntesis esquemática de lo planteado, mostrando la vinculación entre las teorías anteriormente referidas, con el tema de investigación y los conceptos clave: seguridad informática, competencias digitales y ciudadanía digital.

Figura 1: Articulación de las categorías conceptuales y las teorías que fundamentan la investigación, aplicados al problema de investigación.



CAPÍTULO III
DISEÑO METODOLÓGICO

3.1. Método

La presente investigación se abordó a través de un enfoque humanístico-cualitativo, tomando en consideración, 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 (Ibáñez, 2009). En este sentido, puede relacionarse con los enfoques teóricos que sustentan el objeto de investigación, en la cual se plantea el proceso constructivista y conectivista, en los cuales se considera que los aprendizajes están mediados por las interacciones sociales y tecnológicas.

Tomando en cuenta lo anterior, se aplicó el método Hermenéutico Dialéctico, en el cual se pretende establecer interpretaciones de los datos recolectados a fin de lograr la comprensión de los significados que están presentes en los procesos estudiados (Martínez-Miguelez, 1996) Con dicho interés, se pretende interpretar la realidad social, y de forma particular las competencias digitales para el uso seguro de la TICCAD con fines educativos. Por tal motivo, en esta investigación se considera que existen diversas posibilidades de expresión de realidades sociales que son dinámicas y organizadas por conjuntos de hechos interconectados.

A partir de la aplicación del método hermenéutico dialéctico, se propuso una comprensión e interpretación de los hechos, sin desestimar que la subjetividad de los valores en la conducta humana forma parte de la integridad de la persona en su relación con el contexto educativo. Es así como se considera que el hecho social está constituido en una interrelación que genera acciones entre los sujetos. Es decir que, se trata de realizar una contribución de nuevos conocimientos a la educación como ciencia y solucionar problemas vinculados, con la praxis educativa a partir de su interpretación.

De esta forma, en esta investigación se considera la realidad de los actores que forman parte de la institución en estudio, para confrontar la información recogida con los conceptos y teorías existentes. Así se van describiendo las competencias digitales de estudiantes, docentes y personal administrativo en general en cuanto a las competencias digitales en el uso seguro de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales es (TICCAD).

3.2. Escenario

El contexto de estudio es el Instituto Politécnico Martina Mercedes Zouain del Distrito 08-06 Santiago y la comunidad de docentes, estudiantes y personal administrativo.

3.2.1. Características del contexto

A fin de definir el contexto de estudio, se inicia con la misión y visión de la institución, seguido de los datos relevantes de su fundación y finalmente se explica la ubicación geográfica y las características socioculturales de la población atendida.

Misión

> Formar técnicos profesionales de excelencia, creativos, humanistas con pensamiento crítico, de conciencia ciudadana, para promover el desarrollo integral y comunitario, a través de la difusión y aplicación de las competencias requerido en una sociedad cambiante (Proyecto del Instituto Politécnico Martina Mercedes Zouain, 2019, p. 19)

Visión

> Ser una institución reconocida como promotora del desarrollo de la comunidad, en la formación de nuevos técnicos profesionales, con un alto sentido humano y responsabilidad, capaz de integrarse al proceso productivo de la nación con eficacia y eficiencia (Proyecto del Instituto Politécnico Martina Mercedes Zouain, 2019, p. 19)

Este politécnico corresponde al Distrito Educativo 06 de la regional 08 de la ciudad de Santiago de los Caballeros, siendo una institución pública que ofrece educación general y técnico profesional desde los cursos 3ro a 6to. Su objetivo principal es capacitar o preparar jóvenes para ser insertados en las empresas donde realizan sus pasantías para fines de empleos. Estos jóvenes al ser contratados en sus respectivos centros de trabajo, pueden cubrir sus propios gastos para iniciar su carrera universitaria o ser microempresarios para ayudar a sus familias ya que sus niveles económicos son bajos.

Los egresados salen con una carrera técnica en una de las áreas que más le guste, dentro de las cuales se encuentran: informática, turismo, contabilidad, mercadeo, enfermería. El politécnico tiene 22 secciones, 1 laboratorio de informática, 1 laboratorio de enfermería, 1

laboratorio de turismo, 1 salón multiuso, 1 cocina, 1 cancha, 1 biblioteca, 4 oficinas administrativas, 4 inversores, 1 planta eléctrica, 1 cisterna, 1 copiadora, 1 cafetería.

Como parte de su historia y fundación se señala que la construcción inició por parte del estado dominicano el 01 de septiembre de 2001 y el 28 de abril del año 2002 se realiza su inauguración. Iniciando funciones de docencia, el año escolar 2002-2003.

Este politécnico fue fundado en honor a la profesora Martina Mercedes Zouain, quien se destacó como una mujer luchadora y amante de la educación y fue una de las primeras educadoras en la comunidad de la Chichigua. La profesora Zouain comenzó su trayectoria como docente desde su casa, luego donó las tierras para construir una escuela de nivel básico. La institución comienza a trabajar con 50 empleados. Más tarde en el 2008, se construyen 4 aulas más para aumentar cobertura a las familias de la comunidad.

La institución se encuentra en una zona rural y se localiza en el kilómetro 8 de Gurabo, carretera turística Luperón, entrada Santa Rita de la comunidad la Chichigua, Santiago. Se encuentra al comienzo de la cordillera septentrional, al norte Palo Quemado, al sur Gurabo, al este Guazumal, al oeste Jacagua. La comunidad Chichigua tiene una altitud de 200 m.s.n.m, con una población de 3 mil habitantes aproximadamente, la zona es de clima fresco, con frecuentes lluvias, mucha vegetación, arboles grandes, las familias son muy trabajadoras, se dedican a la agricultura, comercialización.

En cuanto a la situación social de la Chichigua se considera que la población juvenil es de 18 a 30 años con un 45 %, niños-adolescentes de 0 a 17 años con un 20%, y adultos de 35 y más con un 35%. En esta comunidad se encuentran 4 escuelas del nivel básico, 1 colegio privado, 1 politécnico.

Gurabo cuenta con 2 policlínicas, un hospital general para asistencia médica y emergencias, 2 destacamentos de policía, 1 oficina Onza que ofrece transporte a bajos costos, 2 cementerios, 1 parroquia y varias capillas para celebrar la palabra de Dios a los creyentes de Cristo. Para transportarse de la comunidad utilizan motores, vehículos privados y ruta de concho público. La comunidad cuenta con los servicios de agua, luz, teléfono, internet.

La gran mayoría de las familias que conforman la comunidad de la Chichigua son de escasos recursos. En cuanto a las actividades religiosas, celebran las patronales de San Bartolomé y Santa Rita. Las personas de la comunidad mayormente se trasladan a trabajar a empresas cercanas como zonas francas, ebanistería, industrias, herrería, mecánica, salón de

belleza, farmacias, copiados, boticas populares, comercios, supermercado, clubes, agencias de viajes. Para su recreación visitan los clubes, practican la pelota, además de baloncesto, voleibol, domino.

Como propósitos estratégicos el politécnico pretende ser un centro con calidad en el aprendizaje con estudiantes competentes. Promover la convivencia entre el personal del centro, las familias, la iglesia, los empresarios, escuela y comunidad. Dentro de los valores de la institución se destacan: promover estudiantes ordenados, cooperadores, puntuales, afectuosos, responsables, trabajadores, participativos, solidarios, honestos, tolerantes, creativos, respetuosos, patriotas.

Sobre las características y lugar de procedencia de los/as estudiantes, estos se desplazan de diferentes zonas como Palo Quemado, La Cumbre, Guazumal, Jacagua, Gurabo y otras comunidades de Santiago. En cuanto a las condiciones de construcción de sus casas, el 60% están construidas de block, el 20% block, madera y zinc, el 20% de madera y zinc.

3.2.2. Organigrama del Centro Educativo

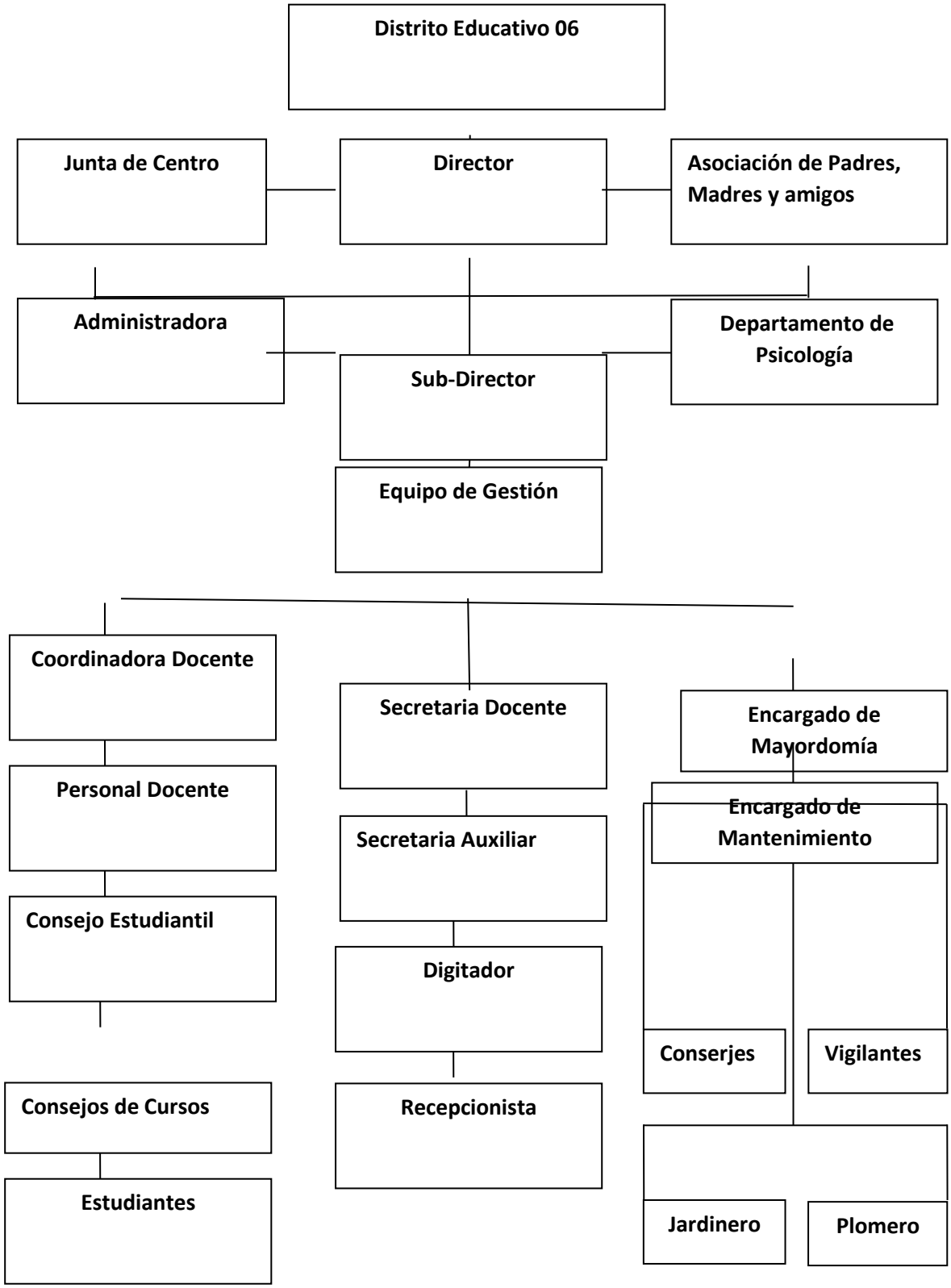
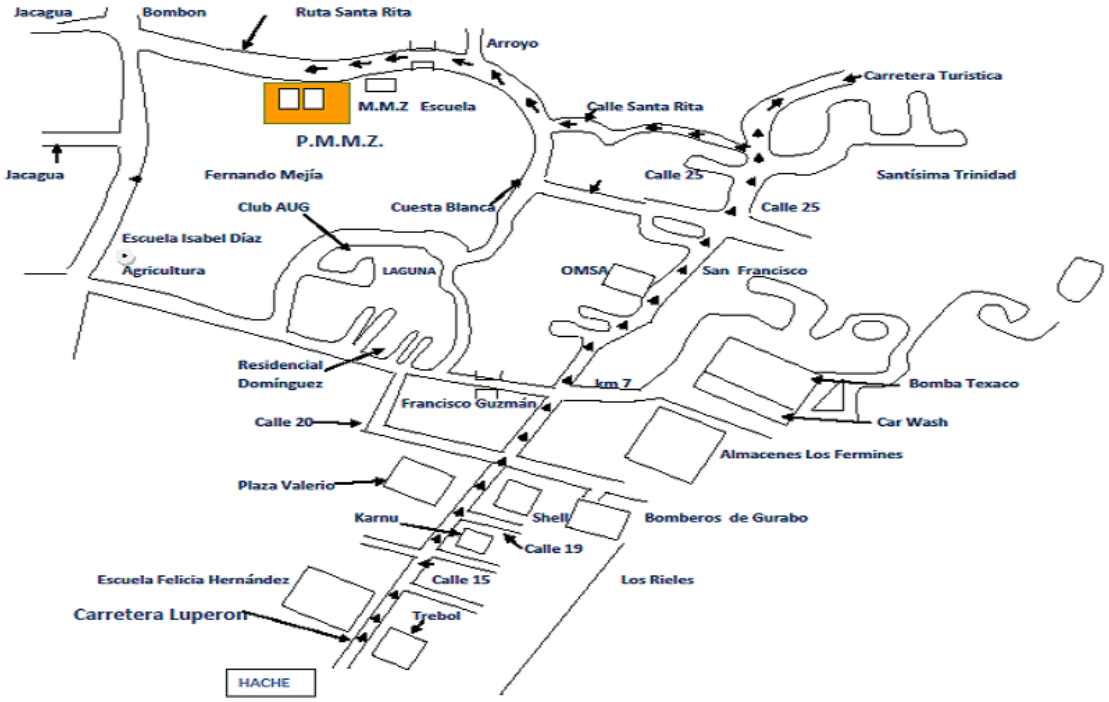


Figura 2

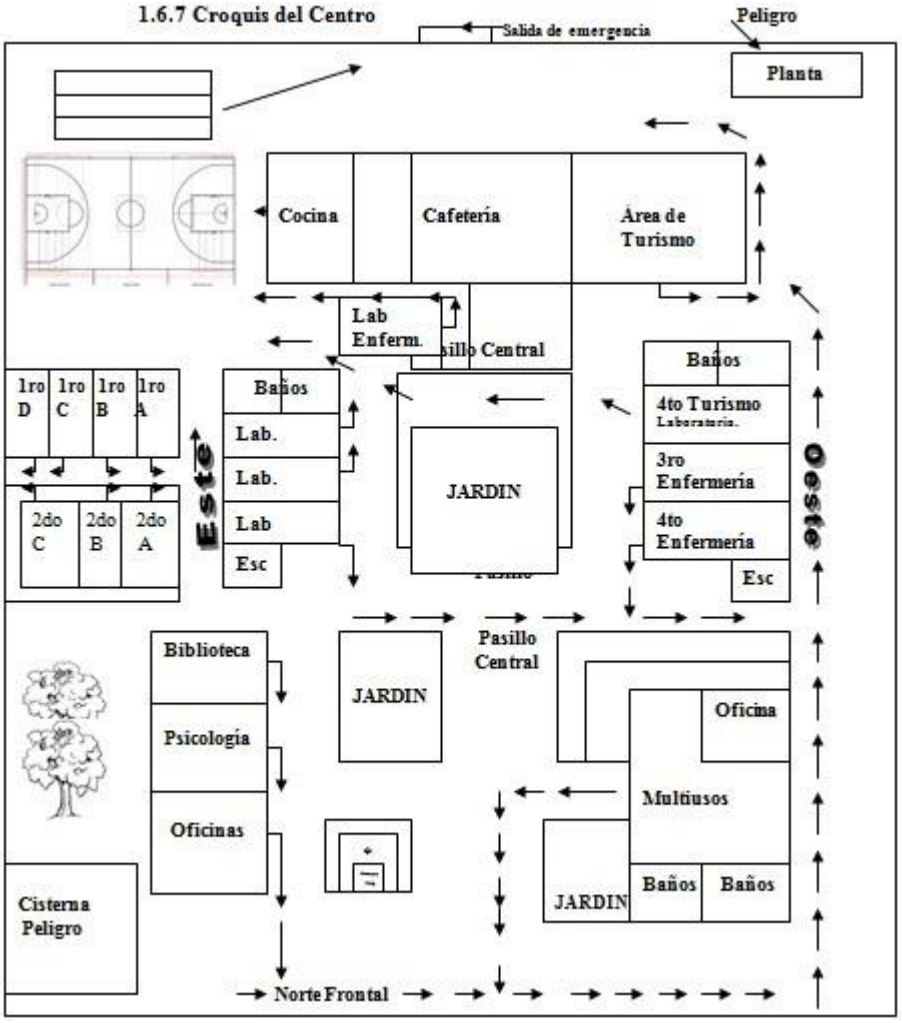
Ubicación del Politécnico Zouain.



Fuente: Google sites

Figura 3

Croquis del Centro



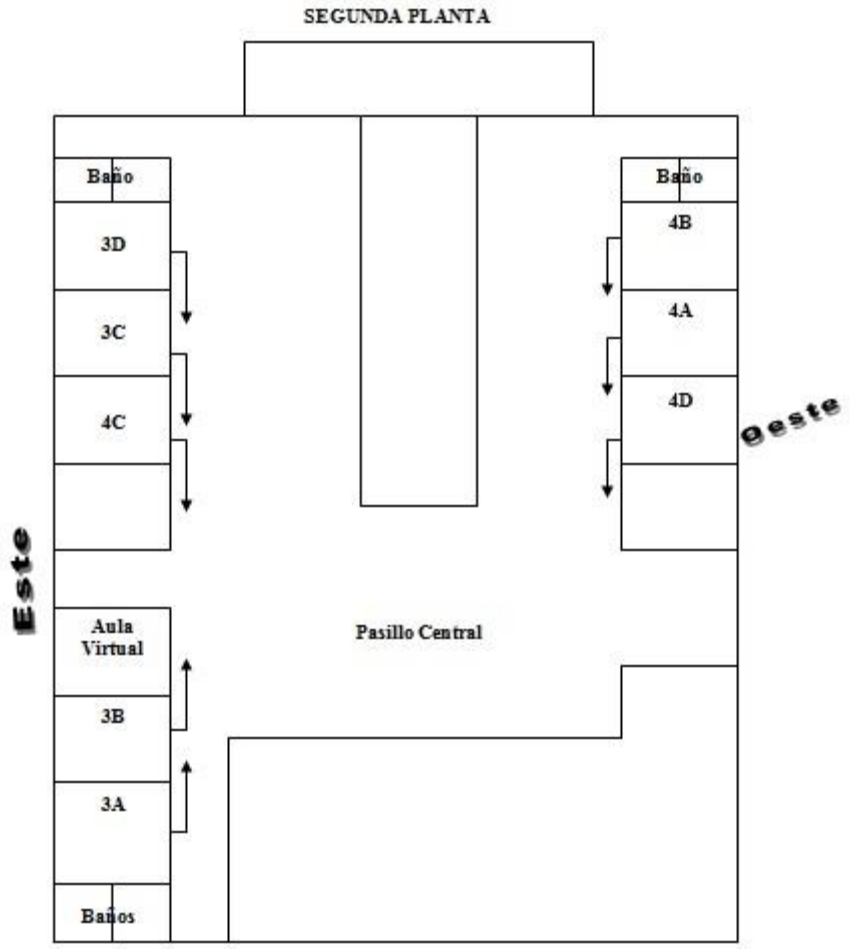

SEGUNDA PLANTA
Baño
3D
3C
4C
Este
Aula Virtual
3B
3A
Baños
Pasillo Central
Baño
4B
4A
4D
Oeste

Figura 4

Imágenes del centro

3.3. Población de los participantes

La población que integra la institución en estudio son Docentes, estudiantes y personal Administrativo del Instituto Politécnico Martina Mercedes Zouain del distrito 08-06, Santiago, Republica dominicana. A continuación, se describen las características de cada grupo.

3.3.1. Docentes

La población total de docentes en la institución es de 40 profesores en las distintas áreas impartidas.

Los docentes se caracterizan por una serie de valores que hacen resaltar su trabajo y distinguirse de las demás instituciones. En su perfil se identifican como organizados, con iniciativa, proyectan buena imagen, respetuosos, mantienen la limpieza en el aula, cuidadosos, cuidan el recreo. Están distribuidos en los cursos atendiendo a la cantidad de estudiantes que requiere el ministerio, aunque los cursos siempre están sobrepoblados. Estos vienen de distintas partes de Santiago, la gran mayoría se transportan en vehículos privados y los demás en transporte público.

Cada uno imparte materias correspondientes a su profesión, estos utilizan la tecnología, aunque muchas veces sus estrategias son repetitivas, algunos con tecnofobia o miedo a la tecnología y métodos tradicionales, se resisten a las capacitaciones. Los docentes tienen desde 1 hasta 28 años en servicio, por lo que sus estrategias didácticas son variadas atendiendo a la diversidad de conocimientos de cada uno. El nivel académico de los docentes está acorde con lo que exige el centro, con títulos de Licenciatura, Diplomados, Especialidades, Ingeniería y Maestrías.

Algunos docentes tienen otra carga de docencia por la noche en universidades que ayudan a mejorar su situación económica, esto hace que el docente se canse más y se estrese al llevar dos jornadas de trabajo, lo cual también se asocia con enfermedades, especialmente de la garganta. En cuanto a lo social, los docentes ven limitada su actividad social, ya que cuando llegan a su casa, deben trabajar su planificación. Además, las salidas que implican gastos, generalmente salen de sus presupuestos económicos.

3.3.2. Estudiantes

La población total de estudiantes que asiste a la institución es de 620, en los distintos niveles educativos.

Las características que comparten los estudiantes de áreas técnicas corresponden a las edades para 4to de 14 años, 5to de 15 años y 6to de 16 años aproximadamente, integrados en su mayoría por dominicanos y seguidos por haitianos, venezolanos y otras nacionalidades. Vienen de familias de escasos recursos, por lo que la institución les proporciona merienda escolar y almuerzo. Inician docencia a las 8:00 AM y salen a las 4:00 PM, con 2 recesos al día.

Estos jóvenes se enferman mucho, especialmente por patologías gástricas, mareos y gripe. Varios de estos jóvenes pasan el día solamente con el alimento que le proporciona el Centro Educativo ya que muchos de sus padres sólo le sustentan, quizás, una cena al llegar a sus hogares. Algunos estudiantes no consumen la alimentación proporcionada porque no le gusta. Cuando el estudiante esta sin comer, esto tiende a tener consecuencias graves como bajar sus calificaciones causa de la anemia por a las faltas de vitaminas y minerales, además presentan un estado de tristeza, sueño, desánimo y desinterés.

Muchos de los estudiantes vienen de comunidades muy lejanas y por ende deben levantarse muy temprano para llegar a tiempo al politécnico, además al estar en un área técnica, los docentes les dejan muchas asignaciones para realizarlas en sus casas. Lo cual se constituye en una situación que afecta a la familia por el poco tiempo de compartir y descansar. El estudiante ocupa mucho tiempo en actividades académicas y pocas de recreación

En cuanto a sus aspiraciones y motivaciones, estos jóvenes tienen mucho deseo de superación, conseguir empleo luego de ser graduados de técnicos en su área, especialmente la de informática que, es la que tiene mayor demanda por el gran avance tecnológico y exigencias de las empresas del dominio de las tecnologías en todas las áreas y departamentos en el mundo laboral. Correspondiente a su desarrollo profesional, su meta es ser técnicos e insertarse en el mercado laboral. Algunos siguen su carrera universitaria, otros se quedan con sólo este título de técnico, insertándose al mercado laboral en donde sea aceptado con su nivel académico o escalar como microempresarios o chiriperos.

3.3.3. Administrativos

La institución cuenta con un total de 13 empleados administrativos.

El personal administrativo al igual que los docentes vienen de diferentes comunidades y se transporta en vehículos privados o públicos. Su tiempo en servicio anda entre los 6 meses a 28 años, con sus títulos de Licenciatura, Maestrías, Secretarias y Bachilleres. Sus conocimientos académicos varían dependiendo de su nivel alcanzado. Unos con más experiencias que otros.

El personal es dinámico, atento, responsable, trabajador, activo en sus funciones. Algunos departamentos no dominan mucho las tecnologías por lo que tardan en realizar sus tareas o funciones asignadas. Como aspiraciones y motivaciones, las secretarias tienen mucho deseo de superación, así como deseos de lograr tener su licenciatura, para estar al nivel de los demás compañeros. En su contexto laboral, el sueldo de las secretarias es mínimo, estas se limitan a trabajar en otro lugar porque el horario de trabajo ocupa los dos turnos del día y en la noche, deben cumplir con las respectivas obligaciones de sus hogares. Los demás cargos administrativos como dirección, subdirección, coordinación y secretaría docente tienen sueldos más atractivos por su titulación docente.

3.4. Caracterización y selección de los participantes del estudio

Tomando en cuenta las características del contexto y la población que integra la población en estudio, arriba detallados. se establecieron tres grupos de participantes. A continuación, se describe su conformación y el procedimiento de selección.

3.4.1. Docentes:

19 docentes. Estos docentes fueron seleccionados a través de un criterio intencional no probabilístico. Según Hernández-Sampieri et al (2014) este tipo de muestreo se aplica a las investigaciones cualitativas y cuantitativas, y obedecen a una forma de selección según el cual el investigador establece criterios a conveniencia para elegir a los participantes en el estudio. Para el caso de esta investigación se seleccionaron a todos los profesores que están en el área de Informática de la institución, a quienes se les solicitó la colaboración, mediante una comunicación enviada a dirección, válida para todos los consentimientos. Ver Apéndice 1, para participar en el estudio y aceptaron participar en grupos focales y responder a las preguntas de las entrevistas.

3.4.2. Personal administrativo:

13 integrantes del personal administrativo. En este caso, los participantes fueron todos los integrantes del personal administrativo, sin selección de un grupo específico.

3.4.3. Estudiantes:

91 estudiantes correspondientes a las siguientes secciones:

4to A=33 estudiantes, de estos 10 femeninas y 23 masculinos

5to A=25 estudiantes, de estos 9 femeninas y 16 masculinos

6to A=33 estudiantes, de estos 6 femeninas y 27 masculinos.

Los cursos que participaron en el estudio fueron seleccionados a través de un muestreo intencional no probabilístico. Para lograr esta participación se contactó con los docentes de informática encargados de cada grupo y se solicitó el consentimiento informado de la institución. Ver apéndice J Una vez realizados estos trámites, se procedió a aplicar los cuestionarios.

3.5. Categorías de estudio

Para la realización del procedimiento metodológico, fue necesario establecer categorías deductivas de estudio, las cuales parten de los objetivos planteados y la recopilación teórica y guiaron la elaboración de las guías de entrevista. Según plantea Gibbs (2007), si bien la investigación cualitativa está guiada fundamentalmente por una lógica inductiva, la existencia de un marco teórico y objetivos a priori son elementos que orientan la recolección de información a partir de una lógica deductiva, la cual permite identificar categorías que serán luego incluidas en los instrumentos.

Tomando en cuenta lo anterior, en el marco teórico de la presente investigación fueron abordados diversos conceptos que fueron integrados y operacionalizados como categorías que orientan la metodología de esta investigación, las cuales son sintetizadas en la Tabla 1:

Tabla 1

Cuadro de categorías deductivas.

CATEGORÍAS	SUBCATEGORÍAS	PROPIEDADES
Competencia digital Es el dominio cognitivo, procedimental y actitudinal de la TCCAD que garantiza 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, 2020)	• Habilidades de pensamiento crítico • Habilidades para el empleo creativo
	Dimensión procedimental; Apropiación de las TICCAD acerca de su empleo, uso, usabilidad, utilización, aplicación e implementación (Edel, 2020)	• Habilidades para el empleo seguro • Estrategias de enseñanza-aprendizaje
	Dimensión actitudinal: Apropiación de las TICCAD en virtud de los actos, conductas, disposición, comportamiento y aceptación (Edel, 2020)	• Habilidades de pensamiento inductivo • Habilidades de pensamiento deductivo
Uso seguro de la tecnología de la información, la 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 y 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)	• Usabilidad pedagógica • Empleo proactivo • Diseño instruccional
	Comportamiento ético ante las TICCAD: Conductas y destrezas para proteger la privacidad en línea y la libertad de expresión (Balderas et al 2021)	• Uso responsable • Empleo socialmente aceptable
	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)	• Actualización permanente de contraseñas • Conductas para protección de datos personales

		• Nivel de conocimiento sobre seguridad informática
	Manejo apropiado y socialmente aceptable de las TICCAD Percepción en cuanto al nivel de manejo y destrezas de las TICCAD (Balderas et al 2021)	• Interacción social adecuada • Habilidades docentes • Habilidades estudiantes

3.6. Técnicas e instrumentos de recolección de datos

La población del objeto de estudio fue abordada a través de diferentes técnicas, tomando en cuenta las características de cada grupo, su disponibilidad y los tipos de relación con las TICCAD. Los instrumentos respectivos fueron elaborados según las categorías deductivas que se presentan en la tabla 1 y estuvieron constituidos por 10 preguntas para todos los grupos. Sólo se establecieron algunas variaciones en las redacciones de las mismas, tomando en cuenta los grupos de edad y función en la institución.

3.6.1. Observación participante en la institución, la cual se registró en un diario de campo en el cual se tomó nota de los aspectos institucionales relacionados con la seguridad informática.

3.6.2. Entrevistas abiertas para profesores (Apéndice A).

El grupo de los profesores fue considerado, a partir de la aplicación de una guía de entrevistas abiertas implementadas de forma individual.

3.6.3. Cuestionario para estudiantes (Apéndice B).

Los estudiantes recibieron cuestionarios auto administrados que fueron presentados en las aulas de clase.

3.6.4. Entrevistas abiertas para el personal administrativo (Apéndice C).

Se elaboró una guía de entrevistas abierta y se llevaron a cabo de forma individual con los participantes de este grupo.

Los instrumentos fueron expuestos a validación por expertos. Para ello se contactó a tres expertos en el área de tecnologías educativas, a quienes se solicitó su colaboración y se entregó

un formato para la evaluación de contenido (Apéndice D), el cual rellenaron y compartieron observaciones pertinentes para mejorar los instrumentos. A partir de las evaluaciones, se aplicaron sus respectivas mejoras. Además de la validación de los expertos, se hizo un piloteo de los instrumentos, para verificar la comprensión de la redacción de las preguntas, con 3 participantes de igual característica de los grupos seleccionados, (3 estudiantes de otro grupo, 3 secretarias, 3 profesores del área técnica), aplicándose dicho piloteo en una semana como antesala del trabajo de campo).

Cabe estacar que el piloteo en su totalidad arrojó resultados positivos, por cuanto, todos los informantes clave, entendieron perfectamente lo que se pretendió investigar. Es decir, con los resultados de los tres grupos sujetos al piloteo, se procedió a la posterior aplicación de los instrumentos, aunque las fechas del cronograma establecido variado por los contagiados de COVID-19 pero dentro del tiempo establecido.

3.7. Fases de la investigación

Se realizaron 4 fases para la investigación, siguiendo las etapas propuestas por Rodríguez-Gómez et al (2006): preparatoria, trabajo de campo, analítica, informativa. A continuación, se describen las etapas y sus respectivos procedimientos.

3.7.1 Primera fase: Preparatoria

A partir de los objetivos y las categorías deductivas se procedió a elaborar los instrumentos y se llevó a cabo una fase de evaluación o consulta con los expertos, seguido de la retroalimentación donde se hicieron ajustes menores a los instrumentos. Dentro de las principales observaciones a los instrumentos se observó: (a) considerar el estándar de competencias en TIC para docentes, creado por la UNESCO; (b) hacer un híbrido de modelos para que se integren subcategorías y propiedades, y, (c) revisar ejemplares de tesis y documentos para afianzar las definiciones de las categorías. Estos cambios se atendieron, se ajustaron y se contemplaron en la versión definitiva de los instrumentos, catalogándolos los expertos como excelentes, con claridad, objetividad, organización, suficiencia, intencionalidad, coherencia y metodología.

Una vez validados los instrumentos, se consideró el piloteo de los instrumentos, con resultados satisfactorios porque los participantes entendieron perfectamente los reactivos, sin demostrar dudas.

3.7.2 Segunda fase: Trabajo de campo

El trabajo de campo se aplicó de manera presencial, durante el periodo octubre-diciembre del 2021. En esta etapa se procedió a realizar las observaciones y aplicar las entrevistas para cada grupo específico. Cabe destacar que para la aplicación de los instrumentos de evaluación se presentó inconvenientes, en cuanto a la continuidad de las clases en la institución educativa por situación de la Covid-19, ya que los estudiantes fueron divididos en la mitad de la población (grupo A y grupo B) y asistían en forma intercalada.

Se presentaron algunos inconvenientes que limitaron el tiempo disponible para la debida aplicación de los instrumentos, a los tres grupos de participantes. Sin embargo, la recolección de la información se llevó a cabo en el tiempo establecido. La información de las entrevistas realizadas fue inmediatamente transcrita de forma íntegra, en una base de datos Excel para la organización posterior del análisis de resultados.

3.7.3. Tercera fase: Analítica

El procedimiento de análisis se realizó de forma manual sin utilización de software para el procesamiento de datos cualitativos. El análisis de la información obtenida en los relatos fue de tipo categorial, a través de un proceso de codificación que permitió la definición de las categorías definitivas. Según Monje, (2011), este procedimiento se realiza a través de distintas etapas que permiten organizar la información y extraer los significados de las categorías que atraviesan los datos recogidos en los relatos. En los apéndices de este trabajo se presentan los procesos de codificación de las entrevistas para cada grupo analizado, en sus distintas etapas (categorización abierta, axial y selectiva), tal y como se irá describiendo en los siguientes párrafos. Dichas etapas son:

(a) Reducir los datos y codificar: Esto se refiere a establecer una estructura conceptual en el curso de cada relato, que sea sistemática y que tenga un orden. Para la Codificación Abierta se identificaron las palabras y expresiones claves a lo largo de todo el documento, las cuales fueron agrupadas en una tabla e identificadas con siglas que representan cada código; las mismas

son mostradas en el Apéndice F. Este proceso fue seguido por la Codificación Axial agrupando códigos de acuerdo a colores asignados. Dicha codificación es presentada, en el Apéndice G, y por último la Codificación Selectiva (Apéndice H), en la cual, se redujeron los códigos axiales y se obtuvo la categorización definitiva con la cual se organizó la información presentada en el capítulo de análisis de resultados.

(b) Categorización: Se refiere a definir los conceptos emergentes de la información. Cada categoría responde a un determinado concepto y se establecen los significados. La categorización permite organizar los resultados en un cuerpo coherente, lo cual permitirá definir un patrón y las características de la realidad analizada. Una vez establecida las categorías definitivas que se presentan en los resultados se generaron los códigos en vivo, también conocidos como verbatim, que expresan el contenido de la información.

(c) Análisis: A partir de las categorías que emergen del discurso, se establecen las comparaciones a partir de las categorías obtenidas en todos los relatos y se relacionan con los elementos conceptuales y empíricos. En esta fase se realizó el proceso de triangulación, en el cual se buscaron los resultados definitivos y se interpretaron para dar respuesta a los objetivos planteados.

3.7.4. Cuarta fase: Informativa

El proceso de investigación finaliza cuando los resultados son comunicados a través de un informe cualitativo, según Rodríguez-Gómez et al (2006). Esta fase consiste en la organización del trabajo de campo a través de la integración en el documento, estableciendo un cuerpo coherente relacionado con el problema planteado, los objetivos y los planteamientos teóricos, como es el caso del presente trabajo.

CAPÍTULO IV

RESULTADOS

En el presente capítulo se muestran los resultados obtenidos una vez aplicado el procedimiento de categorización en los tres grupos estudiados. Para lograr una explicación más conveniente, se procede a presentar los resultados correspondientes por grupo y posteriormente se señala la triangulación de los resultados, con sus correspondientes interpretaciones de acuerdo con la información recopilada para el estudio.

4.1. Presentación de Resultados

4.1.1 Resultados de la observación de los aspectos tecnológicos de la institución educativa.

En virtud de exponer los resultados y dar cumplimiento al objetivo sobre políticas institucionales en seguridad informática, se presenta la información obtenida de las observaciones realizadas por la investigadora, en las cuales se pudo detectar lo siguiente:

- Existe un servidor de internet, pero no se le da el uso adecuado. Este es producto del programa República Digital, que fue parte del gobierno 2016-2020, pero luego de este período no se le continuó dando seguimiento, ya que este programa fue suspendido junto con los docentes que le daban seguimiento al mismo, dejando este equipo tan valioso sin darle uso. Hasta el momento solo sirve para distribuir el internet. No obstante, ningún personal del centro educativo tiene autoridad para programarlo. Además, cuenta con una contraseña que no fue suministrada. Por su parte, el Ministerio no autoriza al Centro Educativo la manipulación del mismo, para poder implementar las medidas de seguridad requerida en la red. Sus razones son que ese servidor sólo lo programan los técnicos del Centro Sede del Ministerio de Educación en Santo Domingo.
- El Ministerio no ha dado instrucciones en el Centro con motivo de implementar medidas de seguridad Informática hasta ahora. Internamente en el Centro, en el área de informática junto con los docentes se han propuesto normativas propias del aula en cuanto a Seguridad Informática.

- El Centro Educativo paga una línea de internet a proveedores privados para todo el personal. Pese a ello, no se aprovecha lo suficiente porque se cae con frecuencia debido a la cantidad de usuarios conectados al mismo tiempo. Este servicio tampoco cumple con los requerimientos de seguridad ya que los protocolos los establece el suplidor del servicio.
- El Centro tiene establecido solamente usar el internet para conectar las pantallas digitales para que cada docente trabaje con sus alumnos. Esto no se logra en totalidad porque los alumnos que han tenido la oportunidad de ver la clave la comparten con sus compañeros y se conectan con sus dispositivos para realizar tareas, actividades sociales y lúdicas.

4.1.2 Resultados Estudiantes

Al realizarse el proceso de codificación y categorización selectiva se obtuvieron las siguientes categorías que, permitieron organizar el análisis de la información compartida por los estudiantes a través de los cuestionarios. Cabe destacar que las categorías y subcategorías fueron recuperadas de los instrumentos aplicados. Es decir, que se trata de la información aportada por el grupo de estudiantes, aun cuando, a nivel teórico existan otras categorías que pueden ser relevantes.

En la tabla 2 se presentan las categorías finales obtenidas del grupo de estudiantes y posteriormente se muestra el análisis para cada una de las categorías

Tabla 2.

Categorías estudiantes.

CATEGORÍAS	SUB-CATEGORÍAS
Seguridad informática	a. Efectividad-vulnerabilidad b. Elementos-recursos c. Acceso d. Detección-alertas
Penetración o hackeo informático	a. Intervención por contraseñas b. IP en wifi de acceso libre c. Virus informático
Discriminación de información en la red -internet	a. Filtro-investigación b. Verificación
Competencia digital del estudiante	a. Destrezas en recursos tecnológicos b. Diseño de contenidos digitales c. Estrategias de seguridad d. Uso de medios tecnológicos

Ciberseguridad y ciudadanía digital	a. Acoso-temor b. Calidad en la elaboración de contenidos c. Apoyo acompañamiento parental d. Monitoreo docente

Como parte del proceso de análisis, a continuación, se presenta la interpretación de cada categoría, acompañada de fragmentos destacados entre los estudiantes sometidos al proceso de investigación mediante las entrevistas. Ello, a fines de su mejor comprensión. Dichos fragmentos se presentan en cursivas, acompañados de la identificación del estudiante con un número, de este modo: en donde n, alude al número correspondiente de dicho estudiante.

a. Seguridad informática

Los procedimientos de seguridad informática implican acciones o estrategias para evitar situaciones que vulneren la información personal del usuario, por ello es necesario identificar que la información de la red, a la cual se está accediendo, sea verdadera o válida. Tal y como señala Gaitan (2020), la seguridad informática se refiere a los procesos de protección que se llevan a cabo en un sistema en red, los cuales implican una diversidad de acciones como respaldos de datos, disponibilidad de información, confidencialidad de usuario, e integridad, garantizando que las informaciones no sean manipuladas por terceros. Al respecto, los estudiantes destacan que, en la actualidad la tecnología está muy avanzada y el acceso a la *web* está muy generalizado.

> *"Actualmente los softwares de navegación están muy avanzados ya que estos mismos nos pueden decir si es una página segura o no. Para identificarlo es con un pequeño candado que aparece en el área de la dirección de la página."* (E.2)

No obstante, hay distintos aspectos que los hace vulnerables a la penetración y el hackeo informático;" por ejemplo, las conductas de usurpación de identidad es un aspecto que debe ser considerado como una prioridad en la seguridad, los cuales generan preocupación en el grupo para evitar situaciones que los puedan poner en riesgo.

> *"En este tiempo la tecnología está muy avanzada y muchas personas tienen acceso a la web, lo cual, conlleva muchos usuarios de poca edad que están vulnerables a ciberbullying"* (E.5).

"Se investiga bien sobre el número o nombre para no dar tus datos sin conocer realmente con quien hablas a través de la red y preguntarle en persona si conoce ese número o nombre," (E.12)

Teniendo en cuenta lo anterior, los estudiantes mencionan que existen medidas que son efectivas para lograr la seguridad en el uso de las tecnologías, por ello mencionan que, una de estas medidas de seguridad se refiere que es fundamental saber en qué páginas navegan y no siempre aceptar, acceder o dar permiso, sin antes leer las condiciones.

Del mismo modo, otro tipo de acciones que se presentaron en esta categoría es que, al instalar una *app*, consideran la necesidad de emplear una plataforma segura para evitar problemas que los vulneren. Asimismo, los estudiantes plantean la capacidad de detectar alertas de cualquier especialmente de virus, cuando se accede a páginas no seguras y respetarlas, saliendo inmediatamente de esa página.

"Para esto, tenemos que saber en qué páginas navegamos y no siempre aceptar, acceder o dar permiso sin antes leer. Lo mismo cuando instalamos una app, debemos de tomar en cuenta hasta los comentarios e instalar de una plataforma segura para evitar que se nos entre algún virus o que nos espíen." (E.6)

También consideran la importancia de filtrar informaciones; por ejemplo, estableciendo cuáles tienen fines educativos y fines comunicacionales o recreativos, y en este último grupo, consideran que se encuentran las mayores posibilidades de que se pueda acceder a páginas no seguras. Ahora bien, según se pudo evidenciar en los estudiantes hay conocimiento de estas medidas básicas de seguridad, pese a ello, al indagar, en algunas respuestas se obtuvo que no siempre se toman en cuenta estas medidas, ya sea por falta de tiempo, por confianza en los antivirus y porque confían en los sistemas de seguridad de sus celulares.

"A veces estoy apurado y no tengo tiempo de revisar la procedencia de la página, pero confío en el antivirus (...) El computador identifica enseguida cuando la página no es segura, por ejemplo: "Esta página tiene virus, cookies." (E.41)

En cuanto a las páginas académicas, los estudiantes indican que el buscador de Google es seguro y que prefieren esta opción para no tener inconvenientes, para buscar en páginas inseguras. Todo lo anterior indica que los estudiantes tienen conocimiento sobre medidas de seguridad, lo cual, en ocasiones, no es llevado a la práctica.

b. Penetración y Hackeo informático

Los estudiantes consideran que existen distintas acciones en el uso de los dispositivos tecnológicos con fines educativos, que permiten que terceros puedan penetrar en las cuentas sin consentimiento, e indican que, en ocasiones, aun tomando las medidas de seguridad, los equipos son susceptibles de penetraciones.

> *"No identifico muchas páginas falsas las cuales hackean nuestro sistema como contraseñas, usuarios, entre otros."* (E.56)

Estas situaciones ocurren con mayor frecuencia cuando se emplean las contraseñas en las computadoras de la institución y al conectarse al *wi fi* de acceso libre, a través de los teléfonos celulares. De acuerdo con las subcategorías encontradas, se plantea que, para la mayoría de los estudiantes, el acceso por entes externos ocurre de distintas formas, y es especialmente posible, a través de los celulares conectados en la red *wifi*, lo cual los hace vulnerables a cualquier ataque o que intercepten los dispositivos.

> *"A la hora en que nos conectamos a las redes wifi de libre acceso y esto permite a esa persona obtener nuestra información y usarla para cosas ilegales."* (E.3).

Por otro lado, al ingresar los datos en el navegador, aplicación o página *web*, la información queda almacenada, permitiendo el robo de la información. En la institución en estudio esto es especialmente importante ya que las contraseñas son aleatorias, y existe el riesgo de que una misma contraseña sea compartida a otra persona. Además, las contraseñas quedan guardadas en las computadoras y otras personas pueden acceder a ellas. Otra forma es el rastreo de la dirección IP, lo cual indica que la seguridad es casi nula en estas circunstancias.

> *"Al conectar a una red libre estás vulnerable a que te rastren y sepan tu ubicación. Pueden ver tu dirección IP y pueden ver todo lo que haces en tu dispositivo."* (E.17)

En esta categoría también se pudo conocer que para los estudiantes uno de los riesgos de penetración y robo de datos son los virus informáticos. Sin embargo, según señalan algunos estudiantes, es difícil conocer si una página es segura o no, ya que algunas páginas populares y con buena reputación, pueden contener virus informáticos. Por ello, afirman la importancia de identificar que las páginas sean confiables, mostrando el candado que indica la seguridad de esta e insisten en la necesidad de que los dispositivos cuentan con antivirus instalados. Al respecto,

Baca (2016), considera que la seguridad informática debe proteger la penetración de los datos, evitando los riesgos a los cuales están expuestos.

c. Discriminación de información:

Según se obtuvo en esta categoría, para los estudiantes es importante aprender a discriminar los tipos de información y las páginas que son seguras y las que pueden generar riesgos, lo cual guarda relación con lo planteado por Martínez-Béjar (2020 quienes señalan la necesidad de filtrar la información en internet entre aquellas que tienen fines educativos y las que tienen fines de comercialización.

> *"Si están citados por otro sitio con información confiable, puede ser verdadera y cierta, en cambio, si está con puntos inentendibles, faltas ortográficas o algo por el estilo, puede no ser cierta del todo."* (E.8).

En efecto, a pesar de las medidas de seguridad informática, los estudiantes reportan que nunca se está exento de riesgos al usar aparatos tecnológicos, debido a varios motivos: en primer lugar, es difícil identificar páginas falsas que hackean las cuentas. En segundo lugar, señalan que uno de los principales riesgos está en las notificaciones que solicitan guardar las contraseña. En tercer lugar, el uso de computadores compartidos permite que otros accedan a las cuentas que no han sido debidamente cerradas.

> *"Existe la posibilidad de que esas contraseñas automatizadas no sean muy seguras, ya que la misma página puede acceder a su perfil. Cualquier hacker logra tenerla, tiene acceso literalmente a todas ellas."* (E.41)

Otro de los aportes en esta categoría es que las verificaciones no son posibles al 100%. No obstante, es importante considerar indicios de confiabilidad como son el certificado, si contiene fuentes y la dirección *URL*. Por ello, consideran que la discriminación de la información consiste en aplicar filtros a los contenidos que se revisan y descartar los que se consideran inseguros. Por ello, los estudiantes consideran que es importante la investigación para saber si la información es verídica o no y si las fuentes son confiables.

d. Competencias digitales

En esta categoría se consideran las habilidades que señalan los estudiantes en el uso de las TICCAD. Es importante destacar que según lo obtenido en los cuestionarios las destrezas que reportan en los recursos tecnológicos se refieren a las habilidades para navegar de forma segura en internet y evitar vulnerabilidades, tal y como se ha expuesto en los apartados anteriores. Mencionan el uso de herramientas informáticas para la seguridad, como *VPN (virtual private network* o red privada virtual*)*. También, algunos navegadores tienen funciones de anti rastreo, bloqueadores de anuncios e ingreso en sitios que tengan el protocolo *HTTPS (Hypertext transfer protocol secure* o Protocolo seguro de transferencia de hipertexto). En algunas respuestas, además, se destaca que un grupo de estudiantes informaron desconocer sobre recursos tecnológicos necesarios para garantizar la seguridad informática.

Reche et al (2019) plantean que el aprendizaje de las competencias informacionales (CI) en los estudiantes y docentes es esencial para lograr la meta propuesta en el modelo educación por competencias y las destrezas para las fases de la evaluación de calidad, búsqueda de información y el tratamiento de comunicación de nuevos conocimientos

La mayoría de los estudiantes asoció las competencias digitales con el uso de software para el diseño de recursos digitales educativos, mencionando los siguientes: *Word, PowerPoint, Bracket*s, *PSint* y *SQL Server* que son herramientas de creación y edición de contenidos digitales como presentaciones, páginas web, diagramas, entre otros. Editores de texto como *Sublime text y Visual Studio*.También, editores de videos como *Filmora 9, Camtasia y Photoshop* para editar fotos.

Por demás, indican capacidades en el uso de medios tecnológicos de interacción educativa, entre los cuales destacan en primer lugar: *Facebook, Whatsapp, Telegram y Discord*, los cuales no son propiamente recursos educativos, sino redes sociales y de mensajería; seguido de las herramientas de Google que sí tienen utilidad educativa, tales como *Google Mail y Google classroom*. Por último, las plataformas de video llamada que fueron de gran utilidad durante el confinamiento debido a la pandemia, como *Zoom y Google Meet*. En cuanto al dispositivo tecnológico, destacan, en primer lugar, el teléfono celular, seguido de la computadora, entre las cuales destacan: las computadoras de la institución, *laptops* y computadoras personales.

e. Ciberseguridad y ciudadanía digital

En esta categoría se recogen las respuestas relacionadas con la ciudadanía digital a partir de las competencias tecnológicas, en cuanto a seguridad e informática, así como la importancia del acompañamiento de padres en el desarrollo de un comportamiento responsable y ético en internet.

En cuanto a la ciudadanía digital, destaca en primer lugar aquellas acciones negativas que exigen a los estudiantes tomar medidas de control sobre las situaciones. Es así como en esta categoría vuelve a observarse que las conductas de acoso como el *ciberbullying* y el temor a la vulnerabilidad informática son aspectos prioritarios para considerar en la ciudadanía digital y la responsabilidad en las relaciones a través de internet.

En este sentido, los estudiantes destacan que, una de las habilidades fundamentales es lograr identificar situaciones de acoso o agresión a través de las redes, que pueden poner en situación de riesgo a los niños y jóvenes.

> *"Las posibilidades de que ocurran estos acontecimientos son muchas siempre y cuando exista una comunicación a través de la red con algún desconocido (...) En la forma en que los demás se expresan, ahí te puedes dar cuenta si es posible que te hagan bullyng o sexting escolar."* (E.7).

Se destaca que, esto implica especialmente, ser consciente de aquellos casos en los cuales una persona desconocida tiene un plan de amenaza que infunde temor, si hay burlas constantes hacia alguien o se comparten imágenes o videos privados, a través de las redes. Los estudiantes consideran estas conductas como negativas y poco éticas, especialmente tomando en cuenta la ley de delitos informáticos.

Además, destacan en las respuestas suministradas, la importancia de la calidad en la elaboración de contenidos como una competencia necesaria para un comportamiento ciudadano responsable y ético. En este sentido, los estudiantes consideran tanto la calidad de la información consultada en las redes especialmente, con fines académicos, así como la calidad de la información que es creada por el estudiante para sus clases. En varias respuestas se enfatiza en la necesidad de investigar y verificar la validez de la fuente como una forma de que los contenidos sean verdaderamente útiles y permitan la formación de conocimiento.

> *"Se puede saber en lugares confiables, como haciendo múltiples investigaciones. Para saber si la información es verdadera o falsa debemos busca en varios sitios web para así saber."* (E.59)

El apoyo y acompañamiento de los padres también es destacado por la mayoría de los estudiantes. Estos indican que los padres han sido fundamentales no sólo apoyando en el logro de habilidades digitales, al suministrar el equipo tecnológico para sus clases y garantizando el acceso a internet, sino que, además, se destaca el apoyo en la realización de actividades virtuales y el acompañamiento durante distintas actividades virtuales, aunado a las presenciales. Destacan, por demás que, los padres son figuras que motivan en el logro de las tareas a través de las plataformas virtuales, lo cual indica que son una figura fundamental en el desarrollo académico, no solo proporcionando el recurso tecnológico y material sino a través de la motivación y el apoyo permanente.

"He recibido un muy buen apoyo de parte de mi familia. Durante la pandemia en las clases virtuales me animaron mucho y me motivaron a seguir." (E.36).

De esta manera, en lo señalado por los estudiantes cabe considerar lo planteado por Catalina-García et al (2018) quienes consideran que la ciudadanía digital consiste en la capacidad de ejercer los derechos participativos en los entornos virtuales, a través de la posibilidad de vincular el conocimiento ciudadano con las habilidades y requerimientos en el entorno online**.**

4.1.3. Resultados Docentes

En esta sección se presentan las categorías obtenidas en las entrevistas a los docentes, las cuales son sintetizadas en la Tabla 3.

Tabla 3.

Categorías docentes

CATEGORÍA	SUBCATEGORÍA
Seguridad informática	a. Fuente de procedencia-Instituciones b. Buscadores Oficiales c. Vulnerabilidad de contraseña d. Barra de dirección e. Antivirus de prevención de ataques
Penetración o hackeo informático	a. Sustracción de datos confidenciales b. IP en wifi de acceso libre c. Robo de identidad d. Penetración a cuenta bancaria e. Información expuesta al publico f. Plagio de documentos

Competencias en recursos educativos	a. Instrucción programada asíncrona b. Multimedia (audio, video) c. Moodle d. Video conferencia e. Gamificación y Juegos interactivos
Competencias en software y diseño de recursos digitales	a. Antivirus b. Herramientas de office c. Herramientas de google d. Herramientas educativas interactivas e. Herramientas de imagen f. Herramientas de video
Desarrollo de la ciudadanía digital en el aula	a. Aprendizaje significativo b. Aprendizaje activo c. Desarrollo de competencias tecnológicas d. Motivación, dinamismo y atención e. Aprovechamiento del tiempo y organización de las actividades

Las siguientes son las categorías finales, que se acompañan de fragmentos en cursiva de las entrevistas identificadas con el número del Docente entrevistado, de este modo: "Dn", donde la D, representa el determinante "docente" y la n, el número asignado a dicho docente entrevistado.

a. Seguridad informática

En las entrevistas, los docentes identifican varios recursos y fuentes que permiten una navegación segura en el desarrollo de las clases virtuales. Uno de los recursos es identificar la fuente de procedencia; para ello se toman medidas tales como la información sobre la veracidad de la página, especialmente en aquellas que insisten en la obtención de información o tienen muchos anuncios. Se menciona a la vez que, las fuentes institucionales, tales como el Ministerio de Educación o universidades son seguras y se suele acudir a éstas para la consulta de información.

> *"Hoy en día hay varias maneras para identificar un sitio web seguro, tales como: las páginas seguras tienen un candado identificador, además inician con https. Otra manera es a través del navegador que nos identifica si el sitio es seguro* (D.11)

Asimismo, plantean que la seguridad informática se garantiza haciendo uso de buscadores oficiales, tales como *Chrome, Mozilla o Edge*. Los docentes mencionan otras medidas que coinciden con lo expresado por los estudiantes, tales como identificar el candado de seguridad, o la identificación del navegador como sitio seguro.

Se menciona en este ámbito, la importancia de la información recibida en las capacitaciones docentes, lo cual les permite mantenerse al día en cuanto a las medidas de seguridad tecnológicas que pueden implementarse en su labor. Para los docentes es fundamental el uso de software antivirus para prevenir vulnerabilidades a la seguridad; sin embargo, la mayor insistencia es en la prevención a partir de acciones personales que prevengan y que no comprometan la seguridad.

> *"Las medidas que tomó en cuenta es informarme bien para luego proceder, ya que cuando la página no es segura te insisten mucho o no tienen conocimiento sobre lo que ofrecen*," (D.2).
>
> *"Me apoyo en la información de las capacitaciones de ministerio de educación y procuro usar páginas oficiales."* (D.7).

Sin embargo, hay un acuerdo generalizado de que la seguridad puede mejorar, lo cual coincide con lo planteado con Morales et al. (2019) sobre la importancia de reforzar la seguridad informática en las instituciones educativas y en especial en las plataformas didácticas.

b. Penetración o hackeo informático

Los docentes entrevistados están conscientes sobre las vulnerabilidades a la seguridad informática, en cuanto que las mismas pueden generar la penetración a los datos personales. En este sentido, mencionan como principal causa el uso de contraseñas inseguras, ya sea porque estas no son constantemente cambiadas o porque al ser usadas en las computadoras de la institución los estudiantes puedan acceder a ellas. Según indica Sánchez)2019) en las instituciones educativas es necesario establecer una política en la cual se inviertan recursos que garanticen la seguridad informática para la ejecución de los programas, como el caso de la criptografía para encubrir datos confidenciales, protegerlos de otros usuarios mal intencionados, y aun con acceso al documento otra persona que no sea el receptor no pueda ver o descifrar el mensaje

Por tal motivo, plantean que una medida de seguridad que debe ser implementada es no usar las contraseñas automáticas o los recordadores de contraseñas. Por otro lado, al igual que los estudiantes, consideran que las redes wifi de acceso libre son inseguras ya que permiten el *hackeo* de la información.

"Algunos estudios indican que en torno al 90% de las contraseñas utilizadas son vulnerables, por lo que los ataques más habituales tratan siempre de encontrarlas." (D.9)

Los docentes manifiestan que sus principales preocupaciones de seguridad son: que haya acceso de terceras personas a las cuentas bancarias, la sustracción de datos confidenciales y que la información personal quede expuesta al público. Por ello, señalan la importancia de acceder a páginas seguras y evitar vulneración a las contraseñas; sin embargo, cabe destacar que ninguno de estos problemas se relaciona con labores de tipo docente.

"Considero que no es seguro usar contraseñas automáticas ya que hay más facilidad de que te hackeen tus cuentas y te roben documentos, dinero o cosas personales." (D.2).

"Si una persona entra a mi pc podría hackear todo los recursos y aplicaciones que tengo sincronizada." (D.6).

Al preguntarse sobre ello, algunos docentes informan que al acceder a una red abierta en la institución o en las computadoras compartidas sienten que estos datos personales deben ser objeto de uso seguro.

"La mayor amenaza para la seguridad de las redes wi-fi gratuitas es la capacidad que tiene el hacker de interponerse entre tú y el punto de conexión." (D.9)

Otro de los aspectos importantes que destaca en esta categoría es el referido al plagio o clonación de documentos personales o académicos, lo cual es especialmente importante con los materiales que suben en los recursos educativos. Es muy importante tomar en cuenta que en el mundo académico la propiedad intelectual es fundamental, por tanto, cuando este tipo de documentos quedan expuestos al público, se corre el riesgo de que sean copiados y empleados con fines no autorizados.

"Pueden clonar la cuenta y plagiar los documentos que tengo almacenados." (D.10)

c. Competencias digitales en recursos educativos

Las competencias digitales en los docentes no se deben limitar al manejo de herramientas. Debe haber un alcance, además, a la aplicación didáctica. En esta categoría se consideran las habilidades y destrezas de los docentes en cuanto al manejo de recursos

tecnológicos con fines educativos o pedagógicos. Más allá del uso de *software* o herramientas de diseño informático, la categoría contiene la información sobre los recursos que el docente considera en la interacción en línea con los estudiantes a fin de cumplir los objetivos planteados.

Entre los recursos preferidos por los docentes se encuentra la Instrucción programada asíncrona, la cual se basa en la implementación de tutoriales y simulaciones para la presentación de contenidos que luego serán evaluados a través de distintas estrategias, ya sean virtuales o presenciales. Cabe destacar que, la instrucción programada se vale de los recursos multimedia, preferiblemente audiovisuales que permiten transmitir la información, tales como crear y compartir contenido conceptual por correo electrónico y enlaces de *drive*. Es interesante la preferencia de los docentes por esta modalidad ya que no requieren un diseño instruccional muy elaborado, sino presentar a los estudiantes la actividad a través de enlaces compartidos para acceder al recurso.

De forma complementaria, algunos docentes indican que las actividades se presentan en una plataforma virtual (con preferencia *Google classroom*), donde se colocan todos los recursos y las actividades que los estudiantes realizan para su desarrollo, como es el caso de ejercicios online o actividades lúdicas en programas educativos, los cuales siempre se encuentran disponibles al momento de acceder a la plataforma. Estas plataformas también permiten la realización de proyectos grupales y ejercicios en línea, que son las estrategias empleadas por dos profesores que mencionan usar técnicas de gamificación a través de los recursos digitales.

> *"Me apoyo en equipos como pantallas digitales y laptops. Herramientas como internet, redes sociales, plataformas digitales, todas las herramientas de google, programas como office, power point, Word, drive…"* (D.3)

> *"Uso plataformas como Moodle, google clasroom, youtube. Otras descargas gratuitas y otras en línea."* (D 8).

Solo dos docentes reportan el uso de la plataforma *Moodle* para asignar actividades, destacándose como principal ventaja, la posibilidad de que estas actividades sean colaborativas y evaluadas inmediatamente, permitiendo comprobar los resultados.

Otro recurso ampliamente utilizado, consiste en apoyar las clases presenciales con recursos tecnológicos multimedia. Entre éstos, destacan la proyección de videos y fichas con audio de *power point.* También destacan el uso de herramientas de comunicación virtual síncrona por video conferencia (*Zoom* y *Google meet*), siendo estos recursos síncronos que

fueron más empleados durante el período de confinamiento. Según indican los docentes, en la actualidad estas plataformas son empleadas para debates y exposiciones.

> *"Proyección de videos, fichas con audio de power point, crear y compartir el contenido conceptual en plataforma y por correo electrónico y enlaces de drive, ejercicios online, ejercicios lúdicos en programas y plataformas digitales."* (D.10).

Es importante destacar que según indican Hernández et al. (2016), las competencias digitales en los docentes son fundamentales para el logro de un aprendizaje activo y cooperativo en el entorno de las TICCAD, que permita a los estudiantes vincularse con las plataformas educativas digitales y adquirir nuevas habilidades gracias a la capacidad de seleccionar y transformar rápidamente dicha información según la calidad y cantidad de la misma.

d. Competencias en software y diseño de recursos digitales

Complementando la categoría anterior, y tomando en cuenta los reportes de los docentes, se indagó en las habilidades que éstos poseen con el manejo instrumental de los recursos digitales necesarios para diseñar las actividades didácticas. Vale señalar que las competencias digitales son destrezas trascendentales propias de un investigador a nivel global que se asocian al acceso a la información y el conocimiento a través de herramientas tanto tecnológicas como educativas, tomando la investigación como destreza principal que conlleva a mejorar las funciones formativas con mayor eficacia, (Rodríguez et al 2018).

En esta categoría los docentes señalan que es fundamental el conocimiento e implementación de software antivirus, como una medida que garantiza la seguridad informática, señalando que los más usados son *Avast, McAfee* y *Windows Defender*. Asimismo, según muestran las respuestas en las entrevistas, es fundamental que los docentes posean competencias en distintos software y programas. Con mayor importancia, los docentes señalan las herramientas de office: *Word, Power Point, Excel*, y las herramientas de google: *Drive, Forms, Docs, Classroom* como básicas para el trabajo didáctico que realizan ya que son las que permiten el soporte para las distintas actividades a realizar. Luego mencionan herramientas educativas que permiten la interacción y la presentación de actividades didácticas para cumplir objetivos además de facilitar la evaluación de los mismos, tales como *Hot Potatoes, Xelearning, Ardora y Quizziz*.

En cuanto a las herramientas que permiten el diseño de imágenes los docentes mencionan *Canvas* y *Power Point*, ya que no solo permite la elaboración de presentaciones sino crear recursos visuales que pueden ser útiles en las actividades lúdicas y de gamificación. Por último, señalan la importancia de tener competencias en herramientas que permitan la edición de videos, tales como *Windows Movie Maker y Filmora*, las cuales son útiles en aquellos casos en los que se preparan tutoriales u otros recursos audiovisuales.

e. Ciudadanía digital en el aula

En esta última categoría, los docentes expresan la importancia de incluir las TICCAD en el proceso de enseñanza y aprendizaje, relacionándolo con formas de interacción segura y responsable, para un buen uso de las herramientas con fines educativos. La mayoría de los docentes señalan que desarrollar en los estudiantes competencias tecnológicas es una necesidad acorde a los nuevos tiempos y a las necesidades actuales, no solo en el ámbito educativo sino también para el futuro profesional, ya que los alumnos pueden desarrollar sus competencias tecnológicas necesarias en los nuevos retos que espera el futuro. Esto coincide con lo planteado por Amador-Ortiz y Velarde-Peña (2019) al señalar que la ciudadanía digital abarca temas relacionados con los valores humanos, la conducta, la ética, aspectos culturales, sociales, además de los tecnológicos, en el cual se incluye el uso seguro de las tecnologías, trabajos colaborativos, liderazgo y responsabilidad en el quehacer.

Asimismo, según expresan los docentes, al usar las tecnologías se logra desarrollar aprendizajes significativos y se les permite a los estudiantes ser autónomos en su aprendizaje, lo cual genera una mayor capacidad en el uso responsable y eficiente de las tecnologías como herramientas para el conocimiento.

> *"Un gran impacto positivo ya que, si está bien dirigido se puede lograr el aprendizaje, además los alumnos pueden desarrollar sus competencias tecnológicas tan necesaria en los nuevos retos que espera el futuro."* (D 6).

Algunos docentes, encuentran que las tecnologías permiten que el estudiante centre su atención y motivación en los procesos, por tanto, encuentran que en estas herramientas una importante utilidad para crear contenidos relevantes que permitan a los estudiantes la

responsabilidad en una interacción segura, no solamente desde la confidencialidad de los datos sino en las interacciones sociales respetuosas e inclusivas.

En este sentido, se destaca que los audiovisuales y los videos no solo deben presentar contenidos educativos, sino que son recursos que pueden transmitir contenidos éticos y cívicos. Sin embargo, no se obtuvo información sobre estrategias específicas para promover la ciudadanía digital ni tampoco vinculación entre los contenidos vistos en clase y la participación de las familias.

Otro impacto positivo que encuentran en las TICCAD es que los estudiantes pueden aprender a organizar mejor el tiempo y sus actividades, siendo esta una destreza fundamental no solo para el trabajo académico sino para las competencias necesarias en su vida profesional y laboral.

4.1.4 Resultados Administrativos

Siguiendo un similar procedimiento para los grupos anteriores, en el caso de los administrativos se obtuvieron las categorías definitivas de la información recuperada de las entrevistas, siendo las siguientes.

Tabla 4.

Categoría personal administrativo

CATEGORÍA	SUBCATEGORÍAS
Seguridad informática	a. Verificación de fuente b. Trabajo manual para evitar penetración de información institucional c. Violación de privacidad d. Distracción
Penetración o hackeo de información	a. Intercepción de correo electrónico b. Pérdida de usuario y contraseña c. Riesgo de pérdida de información d. Contraseñas con vulnerabilidad e. Manipulación de dispositivos electrónicos
Dificultades para el uso de Tecnología	a. Brecha digital b. Docentes con tecnofobia c. Dificultad para el manejo de Moodle d. Conexión inestable internet, electricidad, telefonía

Alfabetización Digital	a. Navega en Internet b. Realiza descargas de aplicaciones y documentos c. Manejo de documentos en línea d. Manipula su cuenta en línea con contraseña segura

Las siguientes son las categorías finales, que se acompañan de fragmentos en cusiva de las entrevistas identificadas con el número del Administrativo entrevistado, de este modo: "An", donde la A, representa el determinante "administrativo" y la n, el número asignado a dicho personal admirativo entrevistado.

a. Seguridad informática

Todos los miembros del personal administrativo que fueron entrevistados en el estudio coinciden en afirmar que el uso de la tecnología en las instituciones educativas está asociado con el conocimiento de medidas de seguridad que garanticen que la privacidad y confidencialidad de los datos, tanto personales como institucionales. En este sentido, indican que el riesgo de implementar internet no es únicamente el riesgo a la seguridad si no se conocen las medidas pertinentes, sino la distracción del trabajo, ya que muchos empleados utilizan tiempo laboral para conectarse a sus redes sociales, lo cual también consideran un tema de seguridad.

> *"Mediante las páginas oficiales encontramos los recursos. Los riesgos son jaqueo, intervención de teléfono, robo de información, ataques cibernéticos, bullyng, sexting, distorsión, amenazas, secuestros, etc*." (A 1)

> *"El riesgo de implementar internet es el mal uso, y la distracción del trabajo."* (A 5)

Tomando en cuenta que estos profesionales se encargan de procedimientos administrativos, uno de los aspectos que destacan en las entrevistas es el hecho de que muchas de las acciones no se realizan en línea para evitar la vulnerabilidad de la información y que sea penetrados los datos institucionales, especialmente porque la institución está afiliada a una línea de internet a través de un servidor manejado por una empresa privada con mucha vulnerabilidad de datos o informaciones. Por tal motivo, en algunas áreas optan por llevar a cabo muchos procedimientos de forma manual o fuera de línea y de este modo evitar posibles penetraciones.

> *"El departamento de coordinación no maneja aparatos electrónicos solo una computadora de escritorio por lo que se trabaja manualmente* (A 4)

Trabajo en el departamento de registro. Trabajo manual utilizo libro de firmas, solicitudes de carta, etc… Implica muchos problemas por documentos que no deben salir a otro departamento." (A 7)

Asimismo, al igual que los docentes, este grupo prefiere garantizar el acceso seguro a sitios confiables, identificados con el candado o que sean páginas oficiales para obtener información. Cabe destacar que Narvaez (2019) indican que la mayoría situaciones relacionados con la seguridad se deben al factor humano, ya que la mayoría de las amenazas evidenciadas para la obtención de datos, robo de identidad, intercepción de mensajes, pérdida de información se deben al factor humano por descuido, documentos compartidos, memorias internas olvidadas o robo.

b. Penetración o hackeo de información

La mayoría de los empleados administrativos conocen los riesgos de penetración de la información cuando no se toman medidas seguras, sin embargo, en las entrevistas realizadas se pudo conocer que dos entrevistados desconocen cómo puede llevarse a cabo el hackeo de información personal o institucional. La mayoría concuerda en que, existen vulnerabilidades en el uso de los dispositivos tecnológicos de la institución que pueden permitir la penetración de la información manejada internamente.

"Las contraseñas automáticas permiten el acceso a sus credenciales con facilidad de hackeo, manipulación de dispositivos electrónicos con frecuencia." (D 9)

En el caso de la institución educativa, al recibirse el internet de un servidor privado y no un servidor institucional, hay mayor posibilidad de que la información confidencial pueda ser accedida por terceras personas; por tal motivo, muchos de los procesos académicos se llevan a cabo manualmente. Cabe destacar lo planteado por Chiliquinga (2020) quien indica que el uso de recursos digitales en las instituciones educativos permite la oportunidad a los delincuentes informáticos (hacker) de obtener informaciones personales a través de las bases de datos de los usuarios, ya que usualmente existen vulnerabilidades en la seguridad.

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.

"Una línea de internet a través de un servidor manejado por una empresa privada con mucha vulnerabilidad de datos o informaciones." (A1).

Otro 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, aun y cuando las computadoras que se manejan en las áreas administrativas son de uso particular de cada trabajador.

Asimismo, indican que existen contraseñas con vulnerabilidad, que pueden ser fácilmente ingresadas por terceras personas. Por tal motivo, se plantea que es fundamental la seguridad al manipular equipos electrónicos, asociando celulares y computadoras ya que en estos se puede penetrar la información personal.

c. Dificultades para el uso de tecnologías

En este grupo, a diferencia de los dos grupos anteriores, se identificó una categoría asociada a las dificultades para usar tecnologías en los miembros de la institución. De forma objetiva, los empleados administrativos señalan que al no estar directamente vinculados con el proceso académico han podido observar distintas problemáticas.

Como elemento resaltante, destacan la brecha digital entre estudiantes, ya que la mayoría procede de familias de escasos recursos y no tienen acceso a equipamiento tecnológico ni a internet. Por otro lado, algunos administrativos entrevistados destacan que muchos docentes tienen "tecnofobia". Es decir, que pierden interés o formación en competencias digitales, especialmente en el manejo del Moodle, lo cual permite que se trabaje con estrategias tradicionales, y este aspecto fue un punto álgido y especialmente problemático, durante la pandemia.

"Es de mucha utilidad para el desarrollo de las actividades que implementan los docentes en el aula. Algunos docentes trabajan la plataforma virtual y otros no le dan el uso adecuado." (A 2)

"En el año escolar 2020-2021 falto de conocimiento de cero manejos de plataforma Teams y Moodle, estas son las herramientas que dieron dificultades por desconocimiento de los profesores." (A3)

Desde el punto de vista institucional, destacan que la conexión inestable a internet, la inestabilidad en energía eléctrica y poca señal telefónica inciden negativamente tanto en los procesos académicos como en los procesos administrativos, así que de manera general la adaptación tecnológica no es completamente efectiva en la institución. Debe destacarse lo planteado por Gallego-Arrufat (2019) al referir que es necesario superar las limitaciones en el uso de la tecnología a fin de lograr un uso amplio, en el cual se consideran actividades tales como recuperar, evaluar, almacenar, producir, presentar, intercambiar informaciones e interactuar en redes de colaboración mediadas por Internet.

d. Alfabetización digital

A diferencia de los grupos anteriores, en el grupo de personal administrativo, no se mencionan las competencias para la ciudadanía digital, sino que se refieren a habilidades que demuestran la alfabetización digital, las cuales están relacionadas fundamentalmente al manejo seguro de los documentos administrativos y la información institucional. Cabe resaltar que, dos entrevistados manifiestan que, por la labor realizada por ellos, no se requiere de competencias digitales.

"Soy administrativa, no manejo el uso de plataformas." (A 8)

"No tengo conocimiento de dispositivos para la seguridad de mi cuenta." (A3)

En consecuencia, uno de los principales valores de la alfabetización digital es realizar descargas seguras de aplicaciones y documentos, a través de páginas confiables y usando los procedimientos que garantizan que estas aplicaciones son útiles y seguras. Otro de los valores importantes que indican la alfabetización digital son las acciones para la navegación en internet, no sólo en cuanto a seguridad de los datos, sino también, en cuanto a la verificación de las fuentes. Sánchez-Duarte (2019), expresa que los docentes y estudiantes necesitan una formación constante para lograr una verdadera alfabetización digital.

Asimismo, se plantea la importancia de los protocolos para el manejo de documentos en línea, especialmente formularios, en los cuales puede quedar expuesta información importante. Por ello, mencionan la necesidad de que las contraseñas de los correos sean seguras y no compartir claves para que solo pueda acceder el propietario y los usuarios con permiso de edición. En líneas generales, en el trabajo administrativo al no existir un proceso de formación

educativa, las competencias digitales están más relacionadas con las destrezas en el trabajo eficiente.

4.2. Triangulación de información

En esta sección se triangulan y comparan los datos obtenidos luego de la aplicación de los instrumentos de evaluación, el procedimiento de codificación de datos, categorización de los tres grupos considerados en el estudio a través de cuestionarios a estudiantes, entrevistas abiertas aplicadas a docentes, personal administrativo a fin de generar los resultados de la investigación.

Cabe destacar que en la investigación cualitativa se utiliza la triangulación de datos como un proceso heurístico, en el cual se buscan las explicaciones partir de la contrastación de la información obtenida, lo que conduce a una perspectiva más amplia del fenómeno en indagación (Aguilar y Barroso, 2015)- En el proceso de triangulación también se establecen relaciones con la literatura consultada a fin de dar respuesta a los objetivos de la investigación y llegar a conclusiones válidas sobre la información recabada.

Para proceder a la triangulación, se sistematizaron los resultados obtenidos en los tres grupos a través de las siguientes tablas:

Tabla 5. Resultados estudiantes

CATEGORÍAS	RESULTADOS ESTUDIANTES
Seguridad informática	• Los estudiantes tienen conocimiento de la existencia de medidas de seguridad informática. • No siempre toman en cuenta estas medidas, ya sea por falta de tiempo, por confianza en los antivirus o porque confían en los sistemas de seguridad de sus celulares
Penetración o hackeo informático	• La usurpación de identidad es la forma de vulneración más recurrente • Las redes wi fi abiertas y computadoras institucionales compartidas son los medios que permiten la penetración
Discriminación de información en la red-internet	• Dificultad de identificar paginas falsas que hackean información personal • Los filtros, antivirus y verificaciones no son confiables al 100%, por lo cual es necesario prestar atención al ingresar a sitios web y redes sociales.
Competencia digital del estudiante	• Algunos estudiantes expresan conocimiento de herramientas y sitios seguros a través del certificado, dirección URL y https. • Todos manifiestan conocimientos en diferentes herramientas de uso educativo: office, herramientas de Google, software de edición de imagen y video
Ciberseguridad y ciudadanía digital	• Expresan preocupación por el ciber bullying • Consideran necesaria la ética en la creación de contenido digital • Importancia del apoyo de los padres y maestros como gestores de la ciudadanía digital y el comportamiento responsable en las redes.

Tabla 6. Resultados docentes

CATEGORÍAS	RESULTADOS DOCENTES
Seguridad informática	• Verificar la fuente de procedencia de la información • Acudir a fuentes institucionales para la búsqueda de información académica • Herramientas como uso de antivirus y paginas seguras identificadas con candado. • Necesidad de mayor capacitación en el área de seguridad digital docente.
Penetración o hackeo informático	• Conciencia en cuanto a la posibilidad de ser vulnerados, especialmente a través de las redes wi fi abiertas • Evitan contraseñas automáticas y usar computadoras de uso compartido • Consideran el plagio de documentos académicos como una forma de vulneración a la confidencialidad y derechos de autor.
Competencias digitales en el empleo de recursos educativos	• Preferencia por apoyo tecnológico para las clases: power point- • Preferencia por recursos digitales asíncronos: you tube, correo electrónico, drive • Plataformas síncronas Zoom y Google meet, solo para actividades especiales.
Competencia en Diseño de recursos digitales	• Poco uso de entornos educativos para apoyar las clases. Preferencia por Google classroom y en pocos casos Moodle (solo 2 docentes). • Los docentes refieren poca capacitación en recursos digitales educativos • Utilización de herramientas de office. Menores destrezas en herramientas de video e imagen
Ciberseguridad y ciudadanía digital	• Necesidad de que las TICCAD permitan interacciones seguras • Acompañar los contenidos educativos con información que promueva la ciberseguridad.

Tabla 7. Resultados empleados administrativos

CATEGORÍAS	RESULTADOS EMPLEADOS ADMINISTRATIVOS
Seguridad informática	• Falta de privacidad y confidencialidad de información de la institución educativa • Los procesos administrativosexigen incrementar medidas de seguridad informática • No se dispone de software de seguridad institucional
Penetración o hackeo informático	• Ante los riesgos a la seguridad, muchos procesos administrativos se realizan manualmente • Vulnerabilidades por acceso a redes abiertas o servidor privado que no evita al 100% la penetración • Penetración por contraseñas inseguras y correos abiertos en computadoras compartidas.
Dificultades para el uso de tecnologías en la institución	• Se destaca que es evidente la brecha digital entre docentes y estudiantes • No hay suficiente capacitación en competencias digitales en empleados y docentes • Problemastecnológicos: internet y energía eléctrica inestables.
Alfabetización digital	• Competencias digitales básicas • Pocos conocimientos en el manejo de sistemas operativos en línea para facilitar procesos administrativos

A partir de la información recolectada, corresponde en primer lugar tomar en cuenta los resultados de la observación de las políticas institucionales en seguridad informática empleadas en el Instituto Politécnico Martina Mercedes Zouain. La ausencia de una estrategia definida para el uso seguro de las TICCAD se evidencia en la institución educativa al no contarse con una red wifi segura, sino una suministrada por una empresa privada, así como la falta de protocolos de seguridad.

Esto se relaciona con la discontinuidad del programa República Digital y a su poca efectividad, lo cual hace que las responsabilidades en el manejo seguro de las tecnologías recaigan en las prácticas de los docentes y no en una acción conjunta direccionada por instancias superiores.

Las medianas competencias digitales en docentes y administrativos dificulta una política clara hacia los estudiantes para comprometerse en actividades seguras y responsables en cuanto al uso de internet en pro de su crecimiento académico. Esta situación fue identificada por Marcelo et al (2019), quienes encontraron que existe un bajo o muy bajo nivel de competencia digital en los docentes del país, razón por la cual la integración de las tecnologías digitales en los centros educativos no es un proceso fácil, conduciendo a una baja eficacia del programa República Digital.

Al analizar las categorías obtenidas en los resultados de los tres grupos (estudiantes, docentes y administrativos), se logró apreciar que la categoría seguridad informática aparece como una prioridad, tomando en cuenta que en el uso de herramientas virtuales existe una necesidad de resguardar la información personal y que esta no sea penetrada por terceros. Sin embargo, se evidencia que es parte de decisiones obtenidas por información personal que a una política de la institución. Para ello, todos los participantes consultados emplean estrategias de prevención, siendo las principales el uso de contraseñas seguras, evitar las redes *wifi* abiertas y uso de antivirus, tal y como se observa en los resultados en los cuales los tres grupos (estudiantes, docentes y administrativos) señalan utilizar medidas para prevenir el hackeo y la penetración de información, evidenciado en las categorías “Seguridad informática” y “Penetración y hackeo de información".

Este aspecto es fundamental en el logro de competencias digitales, tal y como indica Revelo et al (2018), quien señala que las medidas de seguridad son habilidades mínimas para

lograr una adecuada interacción en la red y ser efectivos en las actividades que se realizan a través de éstas.

Otro aspecto mencionado por los tres grupos estudiados es la verificación de las fuentes consultadas, con prioridad en las páginas oficiales o institucionales y aquellas que muestran el candado de seguridad o dirección *https*., lo cual indica que existe conocimiento de las vulnerabilidades en la red por páginas inseguras y la adopción de medidas que permitan establecer criterios de selección de la información, evitando así, la penetración de datos o acceder a información falsa.

Los tres grupos coinciden en señalar las vulnerabilidades existentes cuando se comparten equipos en la institución, ya que esto puede permitir que las contraseñas queden expuestas y sea posible el hackeo de la información o el robo de datos confidenciales. En esta línea, Narváez (2019) indica que la mayoría de las amenazas evidenciadas para la obtención de datos, robo de identidad, intercepción de mensajes y pérdida de información se deben al factor humano por descuido y documentos compartidos, por ello se hace necesario que sean los propios usuarios los responsables de las acciones que minimicen los riesgos, lo cual se entiende como medidas preventivas de seguridad informática.

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 muchas 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.

Es fundamental que las instituciones garanticen la seguridad informática a través de la implementación de programas y softwares institucionales para la protección y seguridad a los usuarios en línea, en correspondencia a planteado por Chiliquinga (2020), lo cual requiere inversión en servicios digitales, equipos e internet, aspectos que posiblemente la institución no tiene al alcance.

Otra categoría que debe destacarse son las competencias digitales que en todos los grupos son de nivel adecuado, tal y como se observa en las categorías "Competencias en recursos educativos" y "Competencias en software y diseño de recursos digitales". Se ha podido identificar que cada grupo plantea el dominio de habilidades digitales según las necesidades y requerimientos en área en la cual se desarrolla. En el caso de los estudiantes, las competencias digitales se refieren fundamentalmente al uso de software para el diseño de recursos digitales educativos que les funciona para la elaboración de sus trabajos académicos, aunque también dan prioridad al uso de las redes sociales para la interacción con compañeros y docentes.

Esto es similar a lo encontrado por Fernández-Prados y Lozano-Díaz (2020) quienes observan que estudiantes universitarios españoles dedican mayor tiempo a las redes sociales, para la interacción con sus compañeros de clase, que al uso de otras plataformas educativas. De hecho, se ha identificado en los estudiantes de la institución en estudio, un uso muy extendido de los teléfonos celulares, no sólo como herramientas educativas, sino, además, como medios de interacción social, observándose que el tiempo dedicado a estas actividades supera el tiempo dedicado a las actividades académicas.

En el caso de los docentes, las competencias digitales están dirigidas a los recursos educativos, especialmente a las plataformas de Google y en menor medida al Moodle para facilitar la interacción con los estudiantes y actividades en línea. Sin embargo, se destaca también el uso de videos tutoriales y actividades a través de correo electrónico lo cual hace suponer que no hay suficientes competencias en el manejo de las plataformas educativas, las cuales no solo exigen destrezas informáticas sino una adecuada planificación de las actividades y las secuencias didácticas. Esta limitante es señalada por los empleados administrativos al indicar que muchos docentes de la institución tienen limitaciones o son renuentes en el uso de las tecnologías, lo cual incide en un bajo uso de estas herramientas.

Este problema ha sido identificado en otras investigaciones, como la de Colás-Bravo et al (2019) quienes señalan que los docentes españoles poseen un nivel medio en competencias digitales, ya que hay un uso limitado de estrategias requeridas para la educación virtual, lo cual se asocia a deficiencias en la formación de docentes en dichas competencias. Por tanto, puede afirmarse que en la institución en estudio es necesario profundizar en la capacitación docente que permitan el uso continuo y efectivo de las herramientas virtuales que permitan un mayor uso de la tecnología de uso docente según los avances y necesidades educativas y los requerimientos de la población estudiantil.

Es importante que paralelamente al desarrollo de competencias digitales, los docentes sean capaces de cumplir un diseño instruccional y planificación de actividades al implementar las plataformas virtuales, por tal motivo, se trata, además de recibir capacitación para adoptar las tecnologías, lograr que se generen habilidades para su implementación (Martínez y Melo, 2019; Marcelo et al 2019).

Como se ha señalado, en la institución existen insuficiencias en las medianas competencias digitales en los docentes, por lo que se dificulta la integración de las competencias digitales y la creación de ciudadanía digital, lo cual compromete la seguridad en las interacciones virtuales, no solo desde el punto de vista de acceso indebido (hackeo o penetración de cuentas) sino en el uso responsable de las redes (búsqueda de información confiable, evitar situaciones de ciberbullying, entre otros). Esto se pudo apreciar a través de la categoría "Competencias en recursos educativos" y "Competencias en software y diseño de recursos digitales"

En el caso de los empleados administrativos, a diferencia de los grupos anteriores, se pudo obtener que las competencias digitales no se relacionan con la aplicación de recursos educativos, sino al área laboral de desempeño, que refiere al manejo seguro de los documentos administrativos, tales como calificaciones, formularios en línea, bases de datos de estudiantes, así como la información institucional que incluye contenido financiero o relaciones de cargos de los empleados de la institución. Esto se pudo observar en la categoría "Alfabetización Digital".

Para llevar a cabo estas actividades haciendo uso de las tecnologías, los empleados requieren un nivel de alfabetización digital que permita el acceso seguro a documentos, especialmente de office, teniendo en cuenta según señala George (2020), que la alfabetización digital implica las competencias básicas para elaborar y comprender de forma eficiente, documentos y formularios a través de los medios digitales.

Ahora bien, según informan los empleados administrativos, existen las competencias instrumentales en algunos de ellos para el manejo de documentos, aunque la totalidad de los empleados no ha sido capacitada en estas competencias. En el caso de los empleados que han sido alfabetizados digitalmente, 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.

De los resultados también se destaca la categoría de ciudadanía digital, considerada como un Comportamiento ético ante las TICCAD que no sólo se refieren a proteger la privacidad en línea sino también, en el comportamiento responsable en la interacción social a través de los medios digitales (Edel, 2020).

Al respecto, el Fondo de las Naciones Unidas para la Infancia (2012), justifica la promoción de la ciudadanía digital desde un aspecto social, pues se requiere que todas las personas contribuyan en el desarrollo psicológico de niños y adolescentes. Por tal motivo, es indispensable evitar el mal manejo de la tecnología en detrimento de la niñez y la juventud, al romper las barreras de la privacidad, producir adicción a Internet o a través del ciberbullying.

En ese sentido, tanto estudiantes como docentes han señalado el rol de las familias en el proceso de ciudadanía digital, en cuanto a la participación y guía en el hogar para fomentar una interacción responsable con las TICCAD. Sin embargo, se debe destacar que en este rol también debe funcionar la institución educativa al proporcionar los aspectos necesarios para generar una relación social positiva a través de las tecnologías.

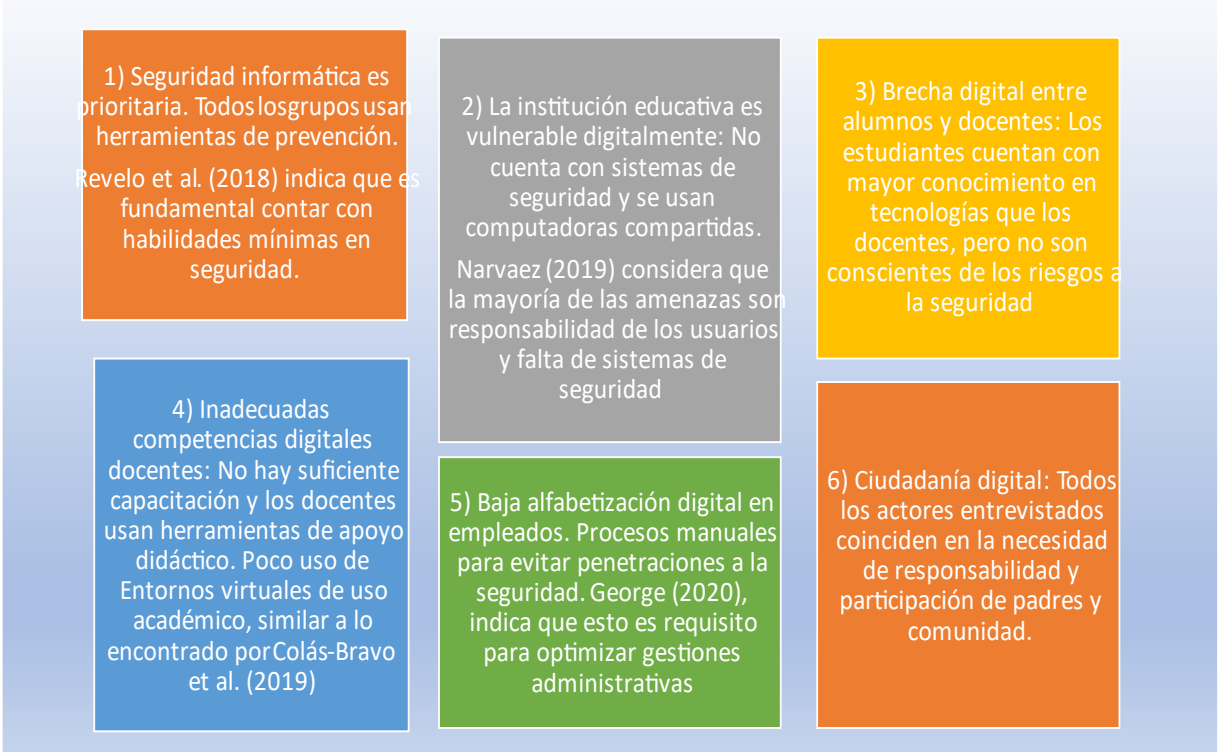
Esto significa que al tomar en cuenta el aspecto afectivo, cognitivo y ético en las personas e incentivar una mejora de su calidad en las interacciones sociales, se promulga una educación dirigida a cultivar un ciudadano digital que tenga conciencia afectiva al navegar en la red. Por ello, se espera que, en la interacción docente-estudiante, y estudiante-estudiante, se empleen las TICCAD en forma más responsable, autónoma y con la posibilidad de elegir entre lo adecuado o no para elaborar comparaciones y seleccionar lo correcto y ético entre la diversidad de opciones que ofrece el mundo digital.

Para Amador-Ortiz y Velarde-Peña (2019), este criterio abarca temas relacionados con los valores humanos, la conducta, la ética, aspectos culturales, sociales, además de los tecnológicos, en el cual se incluye el uso seguro de las tecnologías, trabajos colaborativos, liderazgo y responsabilidad en el quehacer.

Si bien en las categorías se pueden identificar destrezas en cuanto a seguridad informática y competencias digitales, el tema de la ciudadanía digital no se observó suficientemente claro. Quizá es necesario profundizar más en la responsabilidad de cada uno de los actores (institución-docente-familia) en el desarrollo de las habilidades necesarias para que los estudiantes puedan adquirir estos principios éticos tan necesarios para insertarse con seguridad y eficiencia en el mundo digital.

Para finalizar la triangulación, se presenta de forma integrada y esquemática los aspectos relevantes que resultaron coincidentes del análisis de la información obtenida en los tres grupos. A partir de esta información se da respuesta a los objetivos planteados en el capítulo de Conclusiones.

Figura 5: Resultados de la triangulación de la información según los temas comunes obtenidos para los tres grupos



CAPÍTULO V

PROPUESTA DE UN MARCO ACTUALIZADO DE LAS POLÍTICAS INSTITUCIONALES DE SEGURIDAD INFORMÁTICA DEL INSTITUTO POLITÉCNICO MARTINA MERCEDES ZOUAIN.

DEDICATORIA

A todos los hombres y mujeres que orientan sus ideales en el ámbito pedagógico, en el camino de la virtual. Son ustedes la magia que nos hace reconciliarnos con el ser humano, pese a sus fallos.

Son ustedes, el recuentro con el conocimiento, la solidaridad, la paz, la convivencia y el desinterés.

5.1. Presentación

Atender las inquietudes de los usuarios para el acceso seguro en el ámbito cibernético es de vital importancia, en la medida que no cesan de producirse rápidos y trascendentales cambios tecnológicos, muy especialmente en el dominio educativo. Por ello, las instituciones educativas están sufriendo transformaciones drásticas, urgentes e irreversibles, en el modo en que afrontan, hoy día, el proceso de enseñanza-aprendizaje, por lo cual, autoridades y profesionales de la docencia están llamados a asumir una postura de absoluta responsabilidad, mayor que en otros tiempos.

Desde esta perspectiva, se presenta la propuesta de un marco actualizado de las políticas institucionales de seguridad informática del Instituto Politécnico Martina Mercedes Zouain, cuyas bases se configuran en dar a conocer algunas medidas diseñadas por expertos en el área de las tecnologías de la informática y, por otra parte, exhortar a quienes administran la educación en el centro aludido, en afinar, sin descanso, cualquier otra alternativa de seguridad digital que bien, lleve a cabo el ensamblaje de entrega formal educativo, inmerso en un contexto axiológico que contribuya a la formación de los mejores ciudadanos de la República Dominicana.

5.2. Justificación

La propuesta se justifica en su plenitud, en la observancia del objetivo específico, Coadyuvar en la propuesta de un marco actualizado de las políticas institucionales de seguridad informática del Instituto Politécnico Martina Mercedes Zouain, contemplado en la tesis doctoral: Tecnologías de la información y competencia digital en educación secundaria: Estudio de Caso en el Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

Por un lado, permite dar complementariedad, en la ayuda recíproca entra autoridades y profesores del centro educativo y las autoridades del Ministerio de Educación de República dominicana, y así, consolidar una educación de calidad, a los estudiantes de dicho centro.

Asimismo, el éxito o los tropiezos que converjan en la aplicación de la propuesta sugerida contribuiría en la emergente cultura digital, al servicio de la educación, con lo cual, con sus mejoras constantes posibles, pudiera salir ganando el sistema educativo del país.

Sobre la base de esta concepción, se considera oportuno agregar que, a través de la presente propuesta, se establece el crecimiento individual, para la excelencia y la consciencia

moral, en la formación de un ciudadano mejor posible, a partir de los talentos y competencias personales y profesionales, con la finalidad de guiar a los usuarios digitales del centro, hacia un desempeño de calidad, mediante la puesta en práctica de un uso responsable de las tecnologías de la información.

5.3. Diseño de la propuesta

5.3.1. Denominación de la propuesta

Diseño de la propuesta de un marco actualizado de las políticas institucionales de seguridad informática dirigido a los usuarios del acceso cibernético y autoridades del Instituto Politécnico Martina Mercedes Zouain, de República Dominicana.

5.3.2. Descripción de la propuesta

Para el diseño de la propuesta se apuntaló la zona de desarrollo próximo, del Modelo Sociocultural de Vygotsky (1978) y, el aprendizaje significativo de Ausubel (1990), con cuyos basamentos teóricos se orientan a los usuarios del acceso cibernético: docentes, estudiantes y personal administrativo del Instituto Politécnico Martina Mercedes Zouain (IPMMZ), en la forma de recurrir al uso de medidas de seguridad digital. En tal sentido, de ser utilizadas dentro del centro y así, activar el avance integral, seguro y confiable, en la sociedad del conocimiento.

El desarrollo de la Propuesta debe ser considerado una innovación, en el proceso de enseñanza-aprendizaje, como a su vez, estar acorde con los cambios transformacionales que el presente siglo, se vienen realizando, en el marco de las organizaciones educativas a todo nivel.

Lo que permitiría, en este caso, a los usuarios del acceso digital del centro educativo, IPMMZ, adquirir conocimientos básicos sobre una base sólida, participando activamente en consecuencia, con los adelantos de la ciencia y las tecnologías de la informática. Desde esta perspectiva, la estructura de la Propuesta quedó integrada por cuatro (5) sesiones, las cuales se presentan a continuación.

Sesión I

Reflexiones sobre opiniones de los participantes involucrados en la investigación: Tecnologías de la información y competencia digital en educación secundaria: Estudio de Caso en el Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

Sesión II

Consciencia a autoridades.

Sesión III

Medidas de Seguridad Digital.

Sesión IV

Capacitación a los usuarios

Sesión V

Biblioteca digital

Sesión I Marco de Reflexiones

Las siguientes reflexiones propias de la autora de la investigación llevada a cabo, se sustentan sobre la base de las opiniones categoriales, sujetas al estudio. Con ellas, se intenta crear un espacio para la búsqueda y concreción de alternativas forjadas entre autoridades del centro Instituto Politécnico Martina Mercedes Zouain, República Dominicana, IPMMZ, y, las autoridades del Ministerio de Educación del país, en la buena pro del uso seguro de las tecnologías de la información, en dicho centro.

Más aún, las reflexiones son un ápice de estímulo, en la concepción de una perspectiva axiológica posible, en consideración a la reciente publicación del libro *Ethics in the Age of Disruptive Technologies: an Operational Roadmap: (Ética en las tecnologías disrurptivas: una hoja en la en la ruta operativa*), libro publicado por el Instituto de Tecnología, Ética y Cultura, (ITEC), realidad surgida de la asociación entre el Vaticano y el centro de la Universidad de Santa Clara.

En cuanto a lo referido, mis reflexiones como autora de la investigación, son las siguientes:

- Considero que es muy relevante y urgente, el establecimiento de políticas de enlace entre autoridades del centro educativo IPMMZ y el Ministerio de Educación del país, con la finalidad de poder activar el equipo servidor de internet y así, darle un uso adecuado, eficiente y eficaz.
- Opino que es recomendable, extender una solicitud al Ministerio de Educación, sobre instrucciones de medidas de seguridad y su debida implementación, o en su defecto, someter a juicio, un cuerpo de medidas de seguridad en informática, establecidas y coordinadas por el propio centro. Las cuales se presentan más adelante en la presente propuesta, como un ejercicio hacia la consecución de los objetivos proactivos, al servicio de la comunidad del IPMMZ.
- Sugiero el establecimiento de conversaciones con e suplidor de servicio de internet, de modo sistemático y constante, a fin de garantizar la utilización del recurso, por parte de toda la comunidad del IPMMZ. Es decir, los usuarios urgidos de este inestimable servicio.
- Recomiendo la educación bajo preceptos axiológicos, del uso adecuado de la internet, las claves de acceso y asimismo, la toma de consciencia, sobre la disposición del servicio, a fines educativos. Es decir, procurar la creación de una cultura en los estudiantes, a través de la capacitación y formación de valores, en beneficio de una educación de calidad, digna del IPMMZ y, en consecuencia, del país.
- Me parece pertinente una evaluación frecuente de las opiniones de los estudiantes, los docentes y muy especialmente del cuerpo administrativo del IPMMZ, respecto al uso de las tecnologías educativas y así contar con informaciones base, valiosas y vigentes, sobre el uso de dicho recurso aplicado. Es decir, tomar en cuenta los aportes opináticos de todos los usuarios del internet del centro.
- Estimo que el personal administrativo es pieza fundamental en la consideración de penetración de los datos que conllevan al riesgo de la seguridad informática, por lo que, al preferir llevar las actividades de modo manual, se están alejando de la ineludible realidad tecnológica que abraza actualmente, a los centros educativos. Es decir, los administrativos merecen ser atendidos en cuanto, a la resistencia al uso de las tecnologías de la información.

- Considero oportuno, la garantía de Programas y Software y equipos institucionales, para la protección y seguridad de los usuarios en línea. Además, inversión en servicios digitales, equipos de internet de mejor alcance, por parte de la institución.
- Pienso que el nivel de alfabetización digital, merece una atención urgente en cuanto a acceso seguro de documentos, en especial de Office (Goerge, 2020), quien considera que: "la alfabetización digital implica las competencias básicas para elaborar y comprender de forma eficiente, documentos y formularios de los medios digitales."
- Visualizo como perentorio, la intervención de actividades extracurriculares en la formación de confianza, en cuanto a (1) los estudiantes, pues reportan riesgo en la suplantación de la identidad y ciberbulling; (2) los docentes, por su temor infundado al uso del recurso de las tecnologías de la información; y, (3) los administrativos, por la desconfianza de los equipos electrónicos: celulares y computadoras, al servicio educativo.

Sesión II Consciencia a autoridades.

Sirva la presente propuesta, a la reflexión de:

- Las autoridades del centro educativo Instituto Politécnico Martina Mercedes Zouain, IPTMMZ, en la intención del logro de regulaciones en materia de seguridad informática, con el fin de enaltecer los objetivos curriculares, propuestos por dicho centro y así, contribuir a la nación, con egresados cuya formación integral, subyace en el apoyo tecnológico educativo que vino para quedarse.
- Las autoridades del Ministerio de Educación de la República Dominicana, a fin de coadyuvar con el IPMMZ, en la capacitación de ciudadanos con formación de avanzada, mediante el uso de las tecnologías de la información, sujetas a políticas gubernamentales que se correspondan con los designios de una patria educada en la vanguardia del futuro tecnológico, además considerar las necesidades del docente por área técnica o académica. Igualmente, que los facilitadores capacitadores sean profesionales calificados.
- Considero oportuno que las autoridades del Ministerio de educación autoricen al Centro Educativo a implementar una formación contínua integrándola de la forma que consideren tomando en cuenta algunas opciones:

a. Una vez al mes, el día correspondiente al grupo pedagógico, este viene establecido por medio tiempo, podrían considerar designarlo el día completo para las capacitaciones sobre las Tic, competencias digitales y los temas propios establecidos para trabajar en el grupo pedagógico, atendiendo además las necesidades de las áreas.
b. Al realizar las capacitaciones extracurriculares, pueden tener incentivos o bonificaciones que motiven al docente tanto al facilitador como participante a llevar a cabo dicha capacitación.
c. Capacitaciones en junio y agosto, al concluir la docencia del año escolar en mayo se trabajaría en junio la culminación de las evaluaciones finales y se integrarían las capacitaciones, ajustando el horario, dando prioridad a los proyectos finales de culminación del año escolar. Así mismo, en el mes de agosto realizar las capacitaciones con mayor tiempo para lograr mejores resultados.

Sesión III Medidas de Seguridad Digital.

Las medidas sobre seguridad digital expuestas a continuación, no exhaustivas y recabadas de expertos en el área y de valiosa información vía Wikipedia, no pretender ser una camisa de fuerza, en algún modo. Intentan ser un faro de luz, dentro de la propuesta, en el abanico de posibilidades alternas y más aún, un tributo a la activación en la convergencia colaborativa, entre el centro educativo IPMMZ y el Ministerio de Educación de la República Dominicana, a fin de que dicho centro cuente con medidas de seguridad digital, en tal magnitud que sus usuarios digitales rediman cualquier temor o fobia, sobre un recurso que brinda grandes beneficios a la puesta en práctica del currículo pretendido. Las medidas de seguridad virtuales son vitales en la protección de los activos digitales de la institución y en la garantía de la privacidad y seguridad de los datos de los estudiantes, Por lo que, con la implementación adecuada de estas medidas, el centro educativo IPMMZ, podría mantener su información digital segura y así, evitar, cualquier ataque cibernético.

Cabe destacar que las medidas de seguridad son acciones dirigidas para resguardar la integridad, disponibilidad y seguridad de un dato que se almacena en los sistemas interconectados: computación, teléfonos móviles, servidores, la red u otros dispositivos electrónicos.

Sobre lo expuesto, a continuación, algunas medidas:

- Disponibilidad de contraseñas bajo un protocolo de privacidad exclusivo para la institución, donde prevalezca la concepción de “contraseña fuerte” y “única”, para cada usuario o cuenta.
- Mantenimiento de cambio permanente de las contraseñas, en períodos de seis meses, para la garantía de la seguridad digital del usuario.
- Establecimiento de políticas de contraseñas seguras, mediante concepción de códigos institucionales, previamente discutidos entre las autoridades y personal de informática a disposición, en el centro educativo.
- Autenticación de factores, el cual es un determinante técnico de seguridad que incrementa un plus de confianza, en lo atinente a la autenticación tradicional de un usuario. Ejemplo de ello, la autenticación de dos factores (2FA), como la verificación de la identidad mediante la identificación del usuario y la autenticación de un dispositivo.
- Uso de clave encriptada de seguridad (Key Encription), la cual es un archivo que se utiliza para encriptar y descifrar la información, en la base de datos. Resulta relevante, la obtención de una clave encriptada de seguridad de alta calidad que, no sea vulnerable a los ataques o en manos de hackers. El cifrado de datos en reposo protege los datos guardados en la base de datos y el cifrado de datos en tránsito, protege la información que viaja, entre la base datos y los usuarios.
- Concientización de los usuarios, ya que con esta prevención se educa a los usuarios sobre las medidas de seguridad virtuales, para evitar que sean víctimas del phishing o cualquier otro tipo de ataque cibernético. Se debe enseñar a los usuarios cómo detectar los correos electrónicos maliciosos, cómo evitar compartir información confidencial y cómo reportar cualquier actividad sospechosa.
- Establecimiento de control de acceso por parte de la institución, en el sentido de implementar un control de acceso estricto a las aplicaciones que almacenan y manipulan información confidencial. Por ejemplo, los administradores deben programar un sistema de control de acceso que requiera autenticación antes de que los usuarios puedan acceder a los sistemas y aplicaciones.
- Realización de copias de seguridad periódica, la cual permite que el centro educativo garantice que pueda recuperar los datos, ante una incidencia de índole catastrófico, impidiendo la pérdida de los mismos, y permitiendo la recuperación de la normalidad en el trabajo, en un espacio de tiempo relativamente breve.

- Protección del correo electrónico. Hoy día, la mayoría de las comunicaciones de toda empresa, de lo cual no está exento el centro IPMMZ, se realizan utilizando correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda información.
- Contratación de un software integral de seguridad, mediante la adquisición de un paquete de seguridad integral que contenga antivirus, anti espías, anti malware, entre otros, y que permita proteger la información ante posibles ataques externos, a través de internet.
- Utilización de la nube, lo cual permite entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor sería responsable de dicha seguridad. La computación en la nube, conocida, además, como servicios en la nube, informática en la nube, nube de cómputo o simplemente datos servidores, "nube", es el uso de una red de servidores remoto conectados a internet para almacenar, administrar y procesar bases de datos, redes y software. En fin, se trata de una plataforma de almacenamiento de datos limitados que se aloja en la web y que ha generado importancia en diversas áreas digitales y en los sistemas de almacenamiento y manejo de datos a nivel mundial.
- Involucración de todos los usuarios, en la participación, incluyendo a los agentes externos a la institución educativa, como pueden ser representantes o familias, proveedores, entre otros. Muchas veces una organización puede tener implantados los sistemas de seguridad correctos y la brecha en la misma, se produce al relacionarse con un tercero que carece de tales medidas de seguridad.
- Monitorización continua y respuesta inmediata el registro de la gestión mediante un sistema que permita la gestión de los datos, a la vez que, la detección de aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitiría actuar rápidamente, para solventar cualquier incidencia y minimizar su repercusión desfavorable.
- Autenticación Multifactor (*MFA*): Es una forma de autentificación para el acceso a cuentas y sistemas, mediante envíos de *SMS*, autenticación de huella digitales y generadores de códigos únicos temporales, todo para reducir los accesos no autorizados provocados por ataques cibernéticos. Si se le habla y explica al personal de una institución para aplicarlo, dificultara bastante los intentos de acceso no autorizado, aunque un hacker obtenga de algún modo la contraseña.

- Firewall: Es un filtrador de redes entrantes y salientes, que controla y protege la red principal de posibles malware. Sus usos pueden ser desde bloquear el tráfico que no se autorice, hasta imponer reglas de acceso.
- Antivirus/Antimalware: Son aplicaciones que tienen como objetivo principal buscar, bloquear y eliminar las posibles amenazas para tu equipo, mayormente con servicio gratuito.
- *VPN* (Red Privada Virtual): Es un cifrado de comunicación para las redes y los dispositivos en ella, garantiza la seguridad en la información transmitida. En conexiones no seguras su uso es fundamental.
- Gestores de Contraseñas: Son aplicaciones que proporcionan seguridad para guardar tus contraseñas, te ayudan a colocarlas de forma correcta y segura.
- Encriptación de Datos: Es una manera de convertir los archivos de forma tal que solo los dispositivos permitidos puedan tener acceso a ellos. Estas informaciones se pueden encontrar en archivos, documentos, correos y la red de internet dentro de los dispositivos conectados.
- Monitorización de Red: Son aplicaciones que buscan y supervisan constantemente patrones que puedan perturbar el equipo, en el tráfico de red y actividad en tiempo real, con el fin de evitar ataques.
- En una institución educativa, se pueden implementar varios tipos de servidores para establecer medidas de seguridad informática
- Servidor de Proxy: Es un intermediario entre el usuario y la Web, que funciona como un filtrador del acceso a Internet ocultando la dirección IP del equipo y bloqueando Webs maliciosas, esto mejora la seguridad del usuario.
- Servidor de Copias de Seguridad (Backup): Es un servidor que tiene como objetivo el almacenamiento de copias de los datos, para que, en caso de pérdida o corrupción, se puedan restaurar.
- Servidor de Monitoreo de Seguridad: Es un supervisor de la red, su principal función es buscar actividades sospechosas, en caso de encontrarlas, notifica para dar una respuesta activa.
- Servidor de Autenticación de Red Inalámbrica: Es un controlador de acceso *Wi-Fi*, que prioriza solo la entrada de usuarios autorizados para conectarse mediante cifrados.

- Servidor de Correo Electrónico Seguro: Es un servidor que protege de métodos de recopilación personal engañosos, spam o malware.

Sesión IV Capacitación a los usuarios

La capacitación de los seres humanos es una herramienta primordial en la garantía de las perspectivas de eficiencia, eficacia y calidad. No escapa a esta realidad, la comunidad del IPMMZ, ya que, docentes, estudiantes y personal administrativo convergen en objetivos de formación educativa, a beneficio del país, en un futuro a corto, mediano y largo plazo.

Por ello, es de suma importancia que el centro educativo IPMMZ cuente con:

- Un profesional en informática, para atender las necesidades propias de seguridad digital y, sobre todo, que garantice a todos los usuarios digitales del centro, confianza, en el uso adecuado y seguro, de las tecnologías de la información.
- Cursos de actualización permanente, a toda la comunidad del centro educativo IPMMZ, muy especialmente a los docentes y personal administrativo y así, reducir fobias o cualquier sesgo de ignorancia que atente contra el uso de las tecnologías de la información, la red y todo lo concerniente al mundo cibernético, inevitable, en la educación contemporánea.
- Utilización de aplicaciones Informáticas integrando las TICCAD en el aula.

Aplicaciones informáticas:

Kahoot: Es una aplicación web, móvil de dinámica preguntas además de respuestas, todo de manera interactiva, dinámica para evaluar de una mejor manera a los estudiantes mediante cuestionarios y formas divertidas.

Quizlet: Es una herramienta que facilita principalmente la creación de tarjetas con el fin de revisar o repasar vocabularios u otro estilo de agrupación de palabras.

Seesaw: Es una aplicación digital útil para llevar una métrica del proceso de aprendizaje de los estudiantes, además les permite tanto a al estudiante y al docente hacer retroalimentación.

Google Classroom: Es una plataforma en donde las asignaciones de tareas se pueden entregar de varias maneras, tanto como un comentario como archivos y enlaces. Los docentes pueden tener más de un curso a la vez y los estudiantes por igual.

Duolingo: Es una app web y móvil para aprender idiomas, mediante ejercicios separados por lecciones y estos por niveles. Es un buen lugar para los que recién empiezan y para quienes tengan un conocimiento intermedio del idioma.

Nearpod: Es una plataforma en la que las presentaciones se pueden crear de maneras más dinámicas e interactivas, además de crear actividades en tiempo real para evaluarlas en ese mismo momento.

Socrative: Es una herramienta capaz de crear tanto encuestas como cuestionarios para realizarlas en el aula con seguimiento de los resultados del estudiante.

Book Creator: Una app en donde los estudiantes pueden expresar sus ideas de manera visual mediante los libros digitales, útil para actividades creativas que fomenten la creatividad.

Explain Everything: Es una plataforma apta para crear tanto ilustraciones, explicaciones y lecciones de manera animada, una buena manera para entender los conceptos abstractos.

Padlet: Es una plataforma en la que se puede colaborar en la creación de tableros virtuales que ayudan a compartir bien las ideas, para usar en conjunto con la clase para que los docentes y estudiantes colaboren entre sí.

Scratch: Es un entorno que ayuda a que los estudiantes practiquen y aprendan la lógica de programación fomentando su capacidad para resolver problemas.

Khan Academy: Es una plataforma de recursos online, en donde se ofrecen una gran diversidad de materias para aprender de forma virtual.

Wolfram Alpha: Es una herramienta que puede resolver ecuaciones complejas y ejercicios ciencíficos con su motor de búsqueda, vital para la resolución de problemas e investigaciones.

Mathway: Esta herramienta gratuita permite resolver ejercicios de álgebra, geometría y matemáticas en general, para uso de estudiantes en secundaria.

Prodigy: Es una aplicación educativa de matemáticas la cual tiene la capacidad de adaptarse al nivel del estudiante, con el fin de ayudarlo a mejorar sus habilidades de una forma dinámica.

GeoGebra: Es una herramienta que ayuda a explorar términos de algebra y geometría. Los docentes pueden hacer visualizaciones interactivas con el fin de mejorar la comprensión.

Tinkercad: Es una aplicación que permite la creación de modelos 3D o tridimensionales para fomentar el pensamiento espacial de los alumnos.

Rosetta Stone: Es una plataforma para aprender idiomas, su especialización es la pronunciación del estudiante, en donde pueden desarrollar sus habilidades lingüísticas.

MindMeister: Es una herramienta para la creación de mapas mentales, los estudiantes pueden organizar su planificación para desarrollar mejor sus ideas y hacer mejor sus proyectos.

Sesión V Biblioteca digital

La biblioteca digital es la recopilación ordenada, accesible de recursos de información en formato digital, que contiene libros electrónicos, revistas científicas, documentos académicos, videos, audios y otros materiales multimedia. Estos recursos están disponibles en línea y pueden ser consultados y descargados por usuarios a través de plataformas y sistemas de gestión de contenido digital.

¿Por qué es importante implementar una biblioteca digital en el Instituto Politécnico Martina Mercedes Zouain (IPMMZ)?

Porque fomenta la lectura, la escritura y la investigación científica entre docentes, estudiantes y personal administrativo, el cual es esencial para el crecimiento académico y el avance de la institución y de todos los involucrados.

- Los Docentes son modelo a seguir: Los docentes son modelos a seguir para los estudiantes. Participar en actividades de lectura y escritura científica demuestra compromiso con la educación y la investigación, inspirando a los estudiantes a hacer lo mismo.
- Contribución al Conocimiento: La investigación permite a los docentes contribuir al avance del conocimiento en su campo. Sus investigaciones pueden tener un impacto duradero en la comunidad académica y más allá.
- Mejora de la Enseñanza: La investigación informada mejora la calidad de la enseñanza. Al mantenerse actualizados en su área, los docentes pueden brindar a los estudiantes información actualizada y perspectivas enriquecedoras.
- Desarrollo Profesional: Participar en investigación científica fortalece el perfil profesional de los docentes. Esto puede abrir oportunidades de colaboración, presentaciones en conferencias y publicaciones.

- Inspiración para Estudiantes: Los docentes involucrados en la investigación pueden inspirar a sus estudiantes a explorar más allá de las aulas y a considerar carreras en investigación y desarrollo.
- Para el empoderamiento del aprendizaje de los estudiantes: La lectura amplía horizontes y la escritura ayuda a clarificar pensamientos. Participar en investigación brinda a los estudiantes una sensación de control sobre su propio aprendizaje.
- Descubrimiento Personal: La investigación permite a los estudiantes descubrir áreas que les apasionan y profundizar en ellas. Pueden encontrar temas que desean explorar más allá de sus tareas académicas regulares.
- Habilidades Transferibles: La investigación desarrolla habilidades como el pensamiento crítico, la resolución de problemas y la comunicación efectiva, que son valiosas en cualquier campo profesional.
- Colaboración y Redes: La investigación brinda oportunidades para colaborar con otros estudiantes, docentes e investigadores. Esto puede construir redes valiosas para el futuro.
- Preparación para Postgrados: Si los estudiantes consideran la posibilidad de realizar estudios de postgrado, la experiencia en investigación durante la educación universitaria les proporcionará una base sólida.
- Para personal administrativo el apoyo a la Excelencia Académica: Al fomentar la investigación y la lectura, el personal administrativo contribuye al crecimiento académico y a la reputación de la institución.
- Entorno de Aprendizaje enriquecido: Una cultura de investigación en la institución enriquece el entorno de aprendizaje y atrae a estudiantes y docentes motivados.
- Desarrollo Institucional: La investigación puede dar lugar a colaboraciones con otras instituciones, generando oportunidades para el crecimiento institucional y el intercambio de conocimientos.
- Promoción del Aprendizaje Permanente: Involucrarse en actividades de lectura y escritura promueve un enfoque de aprendizaje constante, lo que beneficia al personal en su desarrollo profesional.
- Impacto en la Comunidad: La investigación puede tener un impacto no solo en el ámbito académico, sino también en la comunidad local y más amplia.

Recomendaciones para implementar una Biblioteca Digital:

- Plataforma de Gestión: Selecciona una plataforma confiable y adecuada para la creación y gestión de la biblioteca digital. Puede ser un sistema de gestión de contenidos (*CMS*) especializado en bibliotecas digitales o una solución de código abierto.
- Organización y Catalogación: Crea una estructura de organización eficiente para los recursos digitales. Utiliza metadatos y categorías claras para facilitar la búsqueda y navegación de los usuarios.
- Acceso y Autenticación: Implementa un sistema de autenticación seguro para garantizar que solo los usuarios autorizados puedan acceder a los recursos. Esto puede incluir acceso a través de cuentas de usuario o a través de la red del instituto.
- Formatos de Contenido: Ofrece una variedad de formatos de contenido, como libros electrónicos en *PDF*, *EPUB* u otros formatos compatibles, artículos científicos en formato *HTML*, videos en streaming.
- Búsqueda Avanzada: Proporciona una función de búsqueda avanzada que permita a los usuarios buscar por palabras clave, autores, títulos y otros criterios relevantes.
- Interfaz Intuitiva: Diseña una interfaz de usuario intuitiva y fácil de usar. La navegación debe ser sencilla y los recursos deben ser accesibles con pocos clics.
- Actualización Regular: Mantén la biblioteca digital actualizada con nuevos recursos y materiales llamativos, interesantes. Esto puede incluir adquisiciones de libros electrónicos, revistas actualizadas y otros contenidos relevantes.
- Recursos Locales: Incluye materiales creados localmente, como proyectos de investigación de estudiantes, personal administrativo, y docentes del politécnico.
- Recursos Relevantes: Asegurar de que los recursos seleccionados sean relevantes para los programas de estudio y la investigación, especialmente de las áreas técnicas que ofrece el politécnico. Pueden incluir libros de texto, material académico, literatura científica, superación personal, ética, valores humanos, tecnología, cuidado del entorno, libros y manuales de cada área técnica, entre otros. Esto beneficia a los estudiantes de termino ya que, a través de la biblioteca y la investigación exhaustiva realizada durante los 4 años en ella, ya tiene una idea clara de sus estudios universitarios y la rama de su carrera. De igual forma se puede motivar a que cada estudiante al salir ya graduado deje un aporte a la biblioteca ya sea su propio proyecto, libro, artículo o ensayo. También si está a su alcance puede proporcionar un libro impreso a la biblioteca de su área técnica o de su preferencia.

- Promoción y Capacitación: Ofrece sesiones de capacitación a los usuarios para familiarizarlos con la plataforma y sus características. Promociona la biblioteca digital a través de canales de comunicación internos, o bien sea por las redes sociales educativas del Centro.
- Soporte Técnico: Proporcionar canales de soporte técnico para los usuarios en caso de problemas técnicos o consultas sobre el uso de la biblioteca digital.
- Derechos de Autor: Asegurar el cumplimiento con las leyes de derechos de autor al incluir materiales en la biblioteca digital. Puedes considerar la adquisición de licencias para acceder a ciertos contenidos.

Tipos de Libros y Recursos que Pueden Incluirse:

- Libros de Texto: Libros utilizados en los programas de estudio del instituto.
- Revistas Científicas: Artículos académicos y científicos relevantes para las disciplinas del instituto.
- Libros Académicos: Monografías, libros de investigación y referencias académicas.
- Literatura Local: Obras literarias de autores dominicanos o de la región.
- Recursos Técnicos: Manuales, guías y tutoriales relacionados con áreas técnicas y científicas.
- Documentos Institucionales: Informes, proyectos de investigación de estudiantes y profesores del politécnico.
- Material Audiovisual: Videos educativos, conferencias y presentaciones grabadas.
- Recursos Abiertos: Materiales de acceso abierto disponibles en línea.
- Literatura General: Novelas, cuentos cortos y otras obras literarias para el disfrute personal y cultural.
- Recursos Multidisciplinarios: Contenidos que abarquen múltiples áreas de estudio para fomentar la interdisciplinariedad.

En general, la lectura y escritura científica y la investigación enriquecen tanto a nivel personal como institucional. Destacar los beneficios y el valor que cada grupo puede obtener de estas actividades puede motivar a todos a participar activamente en la búsqueda del conocimiento y el avance académico.

Es importante destacar que la lectura de un buen libro además de moldear conocimientos, ésta permite que el individuo entre en un momento de paz interior, deseo de superación personal,

pues, transforma un momento de ira, inquietud y soledad en un momento de tranquilidad y pasión por lograr sus metas. Se puede notar que un individuo que ya ha adquirido hábito a la lectura siempre tendrá algo que leer y sobre todo escribir. Cuando la persona se acostumbra a realizar determinadas acciones cada día, esto va acumulándose en el cerebro y hace que la persona reaccione de tal forma a como está acostumbrado a vivir. Tanto así que cuando los niños llegan a la escuela con hábitos o conductas inadecuadas adquiridas en sus hogares, al docente se le dificulta adaptarlos al entorno institucional y muchas veces deben entrar a realizar un proceso de aceptación y adaptación con un profesional de la conducta, llámese psicólogo o terapeuta familiar. Las adaptaciones a ambientes positivos mantienen una salud optima y alargan la vida del ser humano. De lo contrario si el individuo arrastra pensamientos negativos no gratos para su persona pues este entra en un estado de desinterés por todas las cosas que lo rodea, puede entrar en un estado depresivo el cual no es favorable para ninguna persona.

CONCLUSIONES

En la actualidad, los niños y jóvenes del tercer milenio están inmersos en el mundo global tecnológico desde muy temprana edad, razón por la cual son llamados nativos digitales, ya que han nacido en esta era cibernética, la cual les resulta natural. Además, son identificados como homo sapiens virtuales, puesto que construyen su vida, estudian, razonan y comparten socialmente en internet.

Existe un fuerte vínculo cultural entre la tecnología virtual y la construcción de la identidad de los niños y adolescentes que repercute en el desarrollo integral y esencialmente, en los componentes cognitivos, afectivos y sociales, que se van estructurando mediante prácticas virtualizadas de relación con los otros.

En consecuencia, la educación posee un papel imprescindible para cultivar la toma de conciencia en el mundo digital, tanto al momento de incentivar sus bondades, como al detectar los peligros que existen en él. Tomando en cuenta lo anterior, se ha de pensar en una cultura digital en la que se conviva en pro de la humanidad y particularmente, en el rol primordial de la educación, con el fin de propiciar comportamientos responsables para el uso de las TICCAD.

En contraste con lo anterior, los docentes y el personal administrativo se corresponden con una inmersión a un mundo tecnológico, cibernético, con dificultades avenidas por su naturaleza de inmigrantes digitales. Lo cual descubre un profundo hiato entre ambos tipos de usuarios, nativos e inmigrantes.

Hiato afortunadamente salvable, mediante la creación de una cultura digital y una capacitación consciente, aunado a la puesta en práctica de formación y entrenamiento constante, por parte de las autoridades del Centro o por el Ministerio de Educación.

Razones por las cuales en esta investigación se planteó entre sus objetivos, estudiar la contribución de las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales (TICCAD) en el Instituto Politécnico Martina Mercedes Zouain, República Dominicana, mediante una investigación de tipo cualitativo a través del método hermenéutico dialéctico en los actores educativos del Instituto Politécnico Martina Mercedes Zouain, ubicado en Santiago, a través de entrevistas a estudiantes,

docentes y personal administrativo. En el proceso de análisis se dio respuesta a los objetivos planteados, de la siguiente manera:

El primer objetivo específico fue identificar las competencias digitales que poseen estudiantes, docentes y administrativos para el desarrollo de sus actividades específicas en la institución.

En este sentido, se obtuvo que los docentes poseen competencias digitales medias, es decir, superan el nivel de alfabetización digital que se refiere al uso y manejo de herramientas de procesamiento de texto, mas no hay suficiente nivel de uso de las plataformas educativas diseñadas para la interacción virtual. Es así que solo dos docentes utilizan el Moodle como herramienta de enseñanza, lo cual evidencia una subutilización de un recurso importante para la interacción asíncrona en los procesos de enseñanza y aprendizaje.

En el análisis de la investigación se logró precisar que el escaso uso de esta herramienta se debe a que había sido recientemente incorporada la licencia en la institución, y aún los docentes se encontraban en adaptación a esta, durante el curso del estudio.

Por el contrario, se identificó que hay una mayor utilización de las tecnologías de clases síncronas como *Zoom* y *Meet*, lo cual tiene sentido debido a la situación de la pandemia. Asimismo, hay preferencia por recursos multimedia como *Canvas* y *Power Point*, que permiten la instrucción programada asíncrona, por medio de tutoriales y simulaciones que son compartidos, a través de correo electrónico y de *Drive*.

Siguiendo esta metodología, no extraña que la mayoría de los docentes indica mayores habilidades en programas de *Google* y *Office*, por tanto, destaca la necesidad de reforzar las competencias en tecnologías educativas.

En el caso de los estudiantes, se pudo constatar que la herramienta tecnológica más utilizada es el celular, y se emplea fundamentalmente para el acceso a redes sociales y en menor medida para el cumplimiento de actividades académicas.

Por tal motivo, cuando se indagó en las habilidades de manejo de recursos digitales, la mayoría de las respuestas estuvieron focalizadas a plataformas audiovisuales. Los dispositivos tecnológicos que les siguen en uso son las computadoras institucionales compartidas y en tercer lugar las laptops personales, ambas las más utilizadas en la elaboración de actividades educativas.

Para las computadoras según ellos mismos reportan, existen competencias en otras herramientas que son útiles para sus trabajos académicos, entre las cuales destacan los recursos de Google y las herramientas multimedia. Ningún estudiante reportó ser competente en Moodle, lo cual puede ser explicado también por la reciente incorporación de la plataforma.

Cabe destacar que, por ser nativos digitales, los estudiantes no reportaron dificultades en cuanto a la adopción de las tecnologías. No obstante, si bien poseen dominio en la mayoría de las herramientas de uso académico, tienen preferencia por las plataformas multimedia y por las redes sociales con un uso fundamentalmente recreativo. Por ello se considera importante que se fortalezcan más las competencias digitales con fines educativos.

En el caso de los empleados administrativos, también se pudo constatar que no todos los empleados están alfabetizados digitalmente y solo poseen destrezas elementales en el manejo de office.

El segundo objetivo fue analizar los riesgos y vulnerabilidades que se presentan en el manejo de los sistemas tecnológicos en la institución. Todos los actores entrevistados señalan que el mayor riesgo es la penetración de los datos y el hackeo de la información personal, siendo que el problema más importante es que la institución carece de una red propia y los usuarios deben acceder a través de redes abiertas, lo cual permite que mucha información pueda quedar expuesta.

Por su parte se encontró que, el mayor riesgo para la seguridad está en el uso de las computadoras compartidas de la institución, y la inexistencia de un sistema de seguridad informático institucional haciendo inseguro el uso de estos recursos. Por ello existen opciones alternativas, que, en el caso de los estudiantes, es la preferencia al uso del celular para cualquier actividad que requiera la tecnología.

Para los estudiantes el mayor riesgo reportado es a la suplantación de identidad y al ciberbullyng, siendo esto importante, ya que, debido al elevado uso de celulares, el problema del acoso puede ser constante y reiterado.

Los docentes por su parte manifiestan como principal riesgo la posibilidad de ser hackeados en las computadoras compartidas de la institución. Fue interesante comprobar que también perciben como riesgo el plagio de información académica, siendo este un problema que está en crecimiento en la era de la tecnología.

Capta la atención la información obtenida de parte de los empleados administrativos en cuanto al alto riesgo de penetración de la información institucional, lo cual les ha llevado a tomar la decisión de realizar ciertas actividades administrativas de forma manual, evitando posibles interferencias en los procesos que pueden poner en riesgo la confidencialidad y seguridad de los datos que se manejan en la institución.

Destacan, además, otros aspectos limitantes a la seguridad informática como es la conexión inestable a internet, la inestabilidad en energía eléctrica y poca señal telefónica que inciden negativamente en la incorporación tecnológica.

En la interpretación de esta investigación, también se pudo constatar que no todos los empleados están alfabetizados digitalmente y sólo poseen destrezas elementales en el manejo de office, lo cual puede ser también otra explicación para la resistencia al uso de la tecnología para ciertos procesos.

Se puede afirmar que el mayor riesgo a la seguridad informática en la institución se identificó en el área administrativa.

El tercer objetivo planteado fue caracterizar las medidas de seguridad informática en los diferentes actores institucionales. Al analizar las categorías emergentes en los tres grupos se pudo observar que todos los participantes toman en consideración la importancia de garantizar la seguridad informática para evitar la penetración de la información personal e institucional, llevando a cabo acciones preventivas tales como el control de contraseñas, ingreso a paginas seguras, evitar acceder a redes públicas y uso de antivirus.

Sin embargo, todas estas medidas se realizan de forma individual, incluso aisladamente, mas no se identifica una acción institucional que permita un mayor control de la seguridad informática mediante el uso de softwares o redes institucionales, lo que conlleva a que la información siempre sea vulnerable cada vez que se accede a información en línea.

Al indagar en los grupos seleccionados se logró observar que existe una conciencia ética que está vinculada al uso seguro y responsable de las tecnologías, en respeto al otro. Ahora bien, desde la perspectiva de los empleados administrativos, se plantea que los docentes deben ser guías del proceso, para lo cual es necesario reducir la brecha digital que notan en la institución.

Se observa que la conciencia ética por la ciudadanía digital no ha sido reforzada a través de estrategias cognitivas, actitudinales o procedimentales que permitan la adquisición de comportamientos claros que eviten conductas tales como el ciberbullying, la usurpación de identidad, la exclusión a través de las redes en los estudiantes, y esta observancia destaca porque son los propios estudiantes quienes expresan preocupación por estas conductas tecnológicas inseguras.

En atención a lo expuesto arriba es necesario que se fortalezcan estos componentes para lograr además de un sistema informático que permita la seguridad de los datos personales, una convivencia digital adecuada y ética.

Al respecto, se destaca que no se ha producido la inversión necesaria para el logro de la infraestructura adecuada ni se tiene apoyo de instancias gubernamentales. Las inversiones brindadas por el Ministerio de Educación no son aprovechadas de forma consciente por la institución y existen algunos desacuerdos e incoherencias en la continuidad del programa República Digital que afecta el funcionamiento de la implementación segura de las TICCAD.

Por otra parte, el centro no cuenta con medidas de seguridad informática ya que la red que existe actualmente es gestionada por una empresa externa al Minerd y pagado por la institución educativa; es decir que los protocolos dependen del suplidor del servicio, mostrando deficiencias y vulnerabilidades propias de una red sin protección.

La falta de una política institucional en seguridad informática ha permitido que no se dé un uso académico e institucional a la conexión de internet, lo cual ha sido causa de muchas de las deficiencias detectadas en esta investigación.

Por último, el cuarto objetivo plantado fur coadyuvar en la propuesta de un marco actualizado de las políticas institucionales de seguridad informática del Instituto Politécnico Martina Mercedes Zouain, se presenta un cuerpo de acciones encaminadas a tal fin, en el Capítulo V, del cuerpo informativo de la presente investigación.

Se puede afirmar que a nivel de la institución en estudio aún son necesarias algunas acciones determinantes para encaminar a un sistema de seguridad informático que pueda lograrse a través del desarrollo de competencias en los actores institucionales. La voluntad y la conciencia existe, pero es fundamental reforzar estas acciones.

RECOMENDACIONES

Dicho lo anterior, las recomendaciones tras haber obtenido los resultados de la investigación son las siguientes:

- Generar un plan de seguridad informática institucional para garantizar la seguridad de los datos, especialmente en los procesos administrativos.
- Establecer planes continuos de capacitación a los docentes para fortalecer las competencias digitales.
- Fortalecer el empleo del Moodle como plataforma para los procesos educativos que permitan motivar a los estudiantes en la adquisición de competencias digitales con fines educativos.
- Desarrollar talleres para los estudiantes para fortalecer los aspectos éticos y responsables en el uso de las tecnologías, con miras a fortalecer prácticas de ciudadanía digital.

Finalmente, los resultados de esta investigación han permitido considerar la necesidad de que se amplíen los trabajos sobre seguridad informática en las instituciones educativas. No sólo trabajar los procesos de competencias digitales de forma aislada en determinados actores educativos, sino que, además, es fundamental considerar una acción integral que permita comprender los distintos factores que impiden o limitan el acceso seguro a los recursos tecnológicos educativos.

LINEAS DE INVESTIGACIONES FUTURAS

Los hallazgos se encaminan en fortalecer y/o derivar líneas de investigación enfocados en el énfasis y compromiso de los docentes para la ciudadanía digital y programas de capacitación, en competencias digitales y seguridad informática para docentes, estudiantes y empleados administrativos:

- Evaluación de las Políticas Institucionales y la integración de las TIC en la Republica Dominicana.
- Aplicaciones de la Robótica en la Educación Secundaria
- Desarrollo de Proyectos Educativos.
- Evaluación y Efectividad de Aplicaciones Informáticas para estudiantes con Dificultades de Aprendizaje.

REFERENCIAS

Acosta, T. (2020). *Lineamientos para el diseño, publicación y evaluación del contenido multimedia accesible en la Web*. Tesis Doctoral. Universidad de Alicante. https://dialnet.unirioja.es/servlet/tesis?codigo=286802

Aguilar, S. y Barroso, J. (2015). *La triangulación de datos como estrategia en investigación educativa. Píxel-Bit. Revista de Medios y Educación*, (47), 73-88. https://www.redalyc.org/pdf/368/36841180005.pdf

Aguirre, G.; Edel, R.; Esquivel, I.; Balderrama, J. (2018). *Competencias digitales en jóvenes bachilleres de Veracruz: Un acercamiento desde sus percepciones.* Congreso Innovación, tecnología y liderazgo en los entornos educativos. Miami: Humborldt International University. https://www.researchgate.net/profile/Javier-Garcia-58/publication/326493939_Eduaction_Miami_2018_-_Proceedings_Innovacion_Tecnologia_y_Liderazgo_en_los_Entornos_Educativos/links/5b510bafaca27217ffa66f03/Eduaction-Miami-2018-Proceedings-Innovacion-Tecnologia-y-Liderazgo-en-los-Entornos-Educativos.pdf

Albornoz, J., Flores-Oyarzo, G., Contreras, M., & Mujica, A. (2021). *Comportamientos interpersonales del docente asociados al compromiso académico de estudiantes de primer año de Ingeniería*. *REXE.* Revista De Estudios Y Experiencias En Educación, 19(39), 145-161. https://www.redalyc.org/jatsRepo/2431/243162775008/index.html

Altamirano, Zhirzhán, Alvarado, Ojeda, Pérez y Medina (2020), *Tecnologías de la Informática y la Comunicación (TIC) en el entorno educativo: herramientas, limitaciones y críticas*. Polo Del Conocimiento: Revista Científico - Profesional, 5(1), 52-64. https://dialnet.unirioja.es/servlet/articulo?codigo=7659385

Álvarez, J. (2018). *Diseño Instruccional e-Learning: Nuevas propuestas de valor para el éxito*. Madrid: IT Business School.

Amador-Ortiz, C. y Velarde-Peña, L. (2019). *Competencias para el uso de las TIC en estudiantes de educación superior: un estudio de caso.* RIDE. Revista Iberoamericana

para la Investigación y el Desarrollo Educativo, 10(19), e014. https://doi.org/10.23913/ride.v10i19.515

Arévalo, A. (2021). *La integración familiar y su relación con el desarrollo de las habilidades socioafectivas en estudiantes del cuarto grado de educación primaria de la Institución Educativa N° 0018 distrito de Tarapoto – 2016.* Tesis de Maestría en Ciencias de la Educación. Universidad Nacional De San Martín http://repositorio.unsm.edu.pe/handle/11458/3879C

Arguedas-Ramírez, L. (2020). *Implicaciones educativas de los hábitos de lectura en el comportamiento académico del estudiantado universitario a distancia. Revista Electrónica Calidad En La Educación Superior,* 11(1), 80-110. https://10.22458/caes.v11i1.2936

Ausubel, D. (1990). *Aprendizaje Significativo. Teorías del Aprendizaje.* México. Trillas

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

Balderas, J., Roque, R., López, A., Salazar, R. y 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. https://doi.org/10.23913/ride.v11i22.826

Barrón, M. C. (2020). *La educación en línea. Transiciones y disrupciones. En H. Casanova Cardiel (Coord.), Educación y pandemia: una visión académica* (pp. 66-74). Ciudad de México: Universidad Nacional Autónoma de México, Instituto de Investigaciones sobre la Universidad y la Educación.

Bonilla, K. y 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. https://doi.org/10.33010/ierierediech.v12i0.1102

Bustos., Gómez, Bustos y Gómez, (2018), *La competencia digital en docentes de preparatoria como medio para la innovación educativa.* CPU-E. Revista De Investigación Educativa, (26), 66-86. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-53082018000100066&lang=es

Cabero, J., Gallego, O., Puentes, A. y Jiménez, T. (2018) *La "Aceptación de la Tecnología de la Formación Virtual" y su relación con la capacitación docente en formación virtual*. EDMETIC, 7, (1), 225-241. https://doi.org/10.21071/edmetic.v7i1.10028

Cano, J. (2015*), Arquitecturas Distribuidas de Gobierno Electrónico con Ciberseguridad Critica*. Tesis Doctoral. Universidad Nacional de Educación a Distancia. https://dialnet.unirioja.es/servlet/tesis?codigo=50471

Castillo (2008) *Propuesta pedagógica basada en el constructivismo para el uso óptimo de las TIC en la enseñanza y el aprendizaje de la matemática*. Revista Latinoamericana de Investigación en Matemática Educativa 11(2): 171-194

Castillo-Fonseca, J. (2019). *Las agendas internacionales de información y su impacto en el desarrollo de la investigación archivística y bibliotecológica en México*. *En: Sánchez, Egbert (Coord.). Agendas internacionales de información y su repercusión en los Estudios de la Información. 1*61-178. Universidad Nacional Autónoma de México.

Catalina-García, B., López de Ayala, M. y Martín, R. (2018). *Medios sociales y la participación política y cívica de los jóvenes. Una revisión del debate en torno a la ciudadanía digital*. Doxa Comunicación. Revista interdisciplinar de estudios de comunicación y ciencias sociales, (27), 81–97. https://revistascientificas.uspceu.com/doxacomunicacion/article/view/656

Clark, B. (1991) *El sistema de educación superior. Una visión comparativa de la organización académica*. México: Editorial Nueva Imagen

Colás-Bravo, P., Conde-Jiménez, J., y Reyes-de-Cózar, S. (2019). *El desarrollo de la competencia digital docente desde un enfoque sociocultural.* Comunicar, 61, 21-32. https://doi.org/10.3916/C61-2019-02

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

Dans, I.; Muñoz, P. y González, M. (2019*) Familia y redes sociales: un binomio controvertido | Aula Abierta,* 48, (2), 183-192. https://reunido.uniovi.es/index.php/AA/article/view/13311/12434

Del Barrio-Fernández (2018). *Las tecnologías de la información y la comunicación en la vida y la educación de los adolescentes.* Tesis Doctoral en Psicología. Universidad de Extremadura. https://dialnet.unirioja.es/servlet/tesis?codigo=125855

Dem, M. (2019). *La distinción aristotélica entre enérgeia y kínesis comprendida de modo intensional.* Mutatis Mutandis: Revista Internacional De Filosofía, 1(13), 29-41. https://revistamutatismutandis.com/index.php/mutatismutandis/article/view/179

Díaz, J.; Ruiz, A. y Egüez, C. (2021). *Impacto de las TIC: desafíos y oportunidades de la Educación Superior frente al COVID-19.* Revista Científica UISRAEL, 8(2), 113-134. https://doi.org/10.35290/rcui.v8n2.2021.448

Edel, R. (2020) *Entre saberes, competencias y habilidades digitales ¿en dónde estamos las y los docentes?* 6° encuentro universitario de mejores prácticas de uso de las TIC en educación. Noviembre. Universidad Autónoma de México. https://encuentro.educatic.unam.mx/educatic2020/pdf/presentacion-entre-saberes-edel.pdf

Estrada-Esponda, R., Unás-Gómez, J. & Flórez-Rincón, O. (2021). *Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá.* Revista Logos Ciencia & Tecnología, 13(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Estrada, E., Miquet, M., y Santamaría, W.. (2009). *Las fases de investigación cualitativa vinculadas al proceso de atención de enfermería.* Revista Médica Electrónica, 31(1) http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18242009000100006&lng=es&tlng=es

Fondo de las Naciones Unidas para la Infancia. (2012b). *Progreso para la infancia. Un boletín sobre los adolescentes.* UNICEF, (10). https://www.unicef.org/spanish/publications/files/unc331769_SP.pdf

Fernández, E. (2017). *Tratamiento de las competencias digitales en la Educación Superior en los estudios de Ciencias Sociales de la Universidad de Málaga*. Tesis Doctoral en Didáctica y Organización Escolar. Universidad de Málaga. https://riuma.uma.es/xmlui/handle/10630/16595

Fernández-Prados, J. y Lozano-Díaz, A. (2021) *El reto de la ciudadanía digital activa en la educación superior europea: análisis del ciberactivismo entre los estudiantes*

universitarios. EDMETIC, 10, (1), 118-134. https://dialnet.unirioja.es/servlet/articulo?codigo=7902432

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. https://repository.unad.edu.co/handle/10596/38802

Gallego-Arufat, M., Torres-Hernández, N. y Pessoa, T. (2019*) Competencia de futuros docentes en el área de seguridad digital.* Comunicar: Revista científica iberoamericana de comunicación y educación, 61. 57-67. https://dialnet.unirioja.es/servlet/articulo?codigo=7048465

Gallent, C. y Tello, I. (2017). *Percepción del alumnado de traducción de la Universidad Internacional de Valencia (VIU) sobre el ciberplagio académico*. Revista Digital de Investigación en Docencia Universitaria, 11(2), 90-117. https://dx.doi.org/10.19083/ridu.11.563

García-Valcárcel, A., Salvador, L., Casillas, S. y Basilotta, V. (2019). *Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica*. Revista de Educación a Distancia (RED), 19(61). https://doi.org/10.6018/red/61/05

García-Varcárcel, A. y Gómez-Pablos, V (2015) *Evaluación de una experiencia de aprendizaje colaborativo con TIC desarrollada en un centro de educación primaria.* EDUTEC. Revista Electrónica de Tecnología Educativa, 51, 2-12. http://www.edutec.es/revista/index.php/edutec-e/article/view/200/pdf_48

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

Gibbs, G. (2007) *El análisis de datos cualitativos en investigación cualitativa*. Madrid: Morata

Gisbert Cervera, M., González Martínez, J., & Esteve Mon, F. M. (2016*). Competencia digital y competencia digital docente: una panorámica sobre el estado de la cuestión*. Revista Interuniversitaria De Investigación En Tecnología Educativa. https://doi.org/10.6018/riite2016/257631

González–Andrío, R., Bernal, C. y Palomero, I. (2020). *Uso de las redes sociales entre los jóvenes y ciudadanía digital: análisis tras la COVID-19. REIDICS. Revista De*

Investigación En Didáctica De Las Ciencias Sociales, (7), 64-81. https://doi.org/10.17398/2531-0968.07.64

González (2018). *Habilidades digitales en jóvenes que ingresan a la universidad: realidades para innovar en la formación.* Revista Iberoamericana Para La Investigación y el Desarrollo Educativo, 8(16), 670-687. https://10.23913/ride.v8i16.363

Guaña-Moya, J. (2023). *La importancia de la seguridad informática en la educación digital: retos y soluciones*. *RECIMUNDO*, 7(1), 609-616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Habowski, A. y Conte, E. (2020). *Interacciones crítico-dialécticas con las tecnologías en la educación*. Revista Ibero-Americana de Estudos em Educação, 15, (1), pp. 266-288 https://doi.org/10.21723/riaee.v14i4.11993

Hernández, C.; Arévalo, M. y Gamboa, A. (2015) *Competencias TIC para el desarrollo profesional docente en educación básica.* Praxis & Saber,7, (14), 41-69. https://www.redalyc.org/journal/4772/477249927002/html/

Hernández-Sampieri, R., Fernández, C. y 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. https://wipolex.wipo.int/en/text/235325

Marcelo, C., Burgos, D. R., Murillo, P. y 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. https://doi.org/10.35362/rie7913322

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

Martin, M., Ibarra, F., Moreno, S. y Hernández, G. (2017). *Importancia de la investigación científica para los estudiantes en la licenciatura en sistemas administrativos de la*

Universidad de Sonora Campus Santa Ana. Revista Mexicana de Agronegocios, 41, 788-807. https://www.redalyc.org/articulo.oa?id=14153918013

Martín, S. y Lago, M. (2021). *Gestión consorciada de contenidos digitales en la Red BUCOC. Información, Cultura Y Sociedad:* Revista Del Instituto De Investigaciones Bibliotecológicas, (45), 145-156. https://www.redalyc.org/journal/2630/263069015008/

Martínez-Béjar, R. (2020). *Sociedades monitorizadas: prácticas de control social y vigilancia a través de la tecnología.* Tesis Doctoral en Sociología. Universidad de Murcia. https://dialnet.unirioja.es/servlet/tesis?codigo=289881

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

Medina, F. (2017), *Seguridad Informática: virus ransomware, el secuestro virtual de datos es Posible.* Trabajo Final de Graduación en Ingeniería en Software. Universidad Siglo 21. Córdoba, Argentina. https://repositorio.uesiglo21.edu.ar/handle/ues21/13925

Mejía-Madrid, G. (2019). *El proceso de enseñanza aprendizaje apoyado en las tecnologías de la información: modelo para evaluar la calidad de los cursos b-learning en las universidades.* Tesis Doctoral. Universidad de Alicante. https://dialnet.unirioja.es/servlet/tesis?codigo=221629

Meza, L. y Moya, M. (2020) *TIC y neuroeducación como recurso de innovación en el proceso de enseñanza y aprendizaje.* ReHuSo: Revista de Ciencias Humanísticas y Sociales. 5, 2, 85-96. https://dialnet.unirioja.es/servlet/articulo?codigo=7408907

Miguel-Vallés, E. (2017). *El desarrollo de la competencia intercultural de estudiantes en educación secundaria: un proyecto etwinning de colaboración virtual.* Tesis Doctoral en Filosofía. Universidad Autónoma de Madrid. https://repositorio.uam.es/handle/10486/682759

Molina, H. (2016). *Estudio sobre la disponibilidad de infraestructura tecnológica en los planteles educativos del sistema educativo público.* Santo Domingo, República Dominicana: Instituto Tecnológico de Santo Domingo (INTEC). https://repositoriobiblioteca.intec.edu.do/handle/123456789/2428

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

Montoya, D., Arias, J. y Avila, A. (2022) *Análisis del estado actual de la seguridad informática en tiempos de pandemia, entregando un conjunto de buenas prácticas, para fomentar la seguridad informática en las organizaciones de la ciudad de Medellín*. *Revista CIES*, 13 (1),19-41. http://revista.escolme.edu.co/index.php/cies/article/view/384/466

Mora, A., Quijije, M., Quijije, S., Macías, M., López, O., Quimiz, L., y Villacreses, L. (2019). *Formación y desarrollo de las habilidades informáticas*. Alicante: 3 Ciencias. http://dx.doi.org/10.17993/DideInnEdu.2019.44

Morales, J.; Avellán, N.; Mera, J. y Zambrano, R. (2019) *Ciberseguridad y su aplicación en las Instituciones de Educación Superior.* RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, 20 (5), 438-448. https://media.proquest.com/media/hms/PFT/1/Pc6LC?_s=o6PIxjk3FPteefQ4dWtcZnJRWjc%3D

Mujica-Sequera, R. (2020). *Fundamentos de la Tecnología Educativa*. *Revista Tecnológica-Educativa Docentes* 2.0, 8(1), 15–20. https://doi.org/10.37843/rted.v8i1.82

Muñoz, J. (2017). *CiberÉtica como ética aplicada: una introducción*. *Dilemata*, (24), 45-63. https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100

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. http://repositorio.uisrael.edu.ec/bitstream/47000/2044/1/UISRAEL-EC-SIS-378.242-2019-028.pdf http://157.100.241.244/handle/47000/2044

Ovalles, L. (2014). *Conectivismo, ¿un nuevo paradigma en la educación actual*?. *Mundo FESC*, 4(7), 72-79. https://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/24

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. 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. https://dialnet.unirioja.es/servlet/tesis?codigo=204191

Prado, M. (2021). *Enfoque axiológico en la Educación Superior mediante la interacción de los estudiantes en el Entorno Virtual de Aprendizaje*. E-Ciencias de la Información 11(1): 25-52. http://dx.doi.org/10.15517/eci.v11i1.41379

Proyecto del Instituto Politécnico Martina Mercedes Zouain 2019-2022. Original Impreso. Gurabo, Santiago, República Dominicana

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

Revelo, J. Revuelta, F. y 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. https://doi.org/10.21071/edmetic.v7i1.6910

Rodríguez, C. (2015) *Uso de las TIC para fortalecer el proceso de aprendizaje de estudiantes con Discapacidad Intelectual en la Institución Educativa Nicolás Gómez Dávila, Bogotá, Colombia. Estudio de caso.* Tesis de Grado de Maestría en Educación.

Rodríguez-Gómez, G., Gil, J. y García, E. (2006*). Metodología de la Investigación cualitativa.*

Salas, M., Romero, K. y Reinoza, M. (2020) *Teorías cognitivas. Recorrido a través de sus principales exponentes.* En: Escobar, M.G. *Psicología. Aportes a la educación y el aprendizaje*, 89-101. Sello Editorial Vicerrectorado Académico. Universidad de Los Andes.
http://bdigital2.ula.ve:8080/xmlui/bitstream/handle/654321/8928/Psicologia.pdf?sequence=1&isAllowed=y

Salazar, J., Cruz, C., Balderas, A. y Díaz, H. (2021) *La seguridad informática en las instituciones de educación superior. Tectzapic.* Revista de divulgación científica y

tecnológica, 7 (2), 72-79. https://www.eumed.net/uploads/articulos/0d3849d924bbb98a57efc5ad7dcddad4.pdf

Sánchez, E. (2019). *Diseño y caracterización de criptocircuitos seguros y resistentes a ataques físicos.* Tesis Doctoral en Ciencias Tecnológicas. Universidad de Sevilla. https://dialnet.unirioja.es/servlet/tesis?codigo=218944

Sánchez-Duarte, M. (2019). *Caracterización de las prácticas innovadoras mediadas por TIC del profesorado de posgrado: estudio de caso de la Universidad de La Sabana*. Tesis Doctoral en Ciencias Sociales. Universidad Autónoma de Barcelona Recuperado de https://www.tesisenred.net/handle/10803/669529#page=51

Silva, J. y 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. https://dx.doi.org/10.21703/rexe.20201941silva9

Verdezoto, R. y Chávez, V. (2018). *Importancia de las herramientas y entornos de aprendizaje dentro de la plataforma e-learning en las universidades del Ecuado*r. Edutec. Revista Electrónica De Tecnología Educativa, (65), 68-92. https://doi.org/10.21556/edutec.2018.65.1067

Villaman (2018) *El uso de las TIC para el aprendizaje colaborativo en la educación superior en el área de lengua española.* Tesis Doctoral en Pedagogía. Universidad de Alcalá. https://dialnet.unirioja.es/servlet/tesis?codigo=158767

Viteri, L., Valverde, M. y Torres, M. (2021). *La plataforma Moodle como ambiente de aprendizaje de estudiantes universitarios. Revista Publicando,* 8(31), 61-70. https://doi.org/10.51528/rp.vol8.id2234

Volpato, S. (2016). *El derecho a la intimidad y las nuevas tecnologías de información.* Tesis doctoral inédita. Universidad de Sevilla. https://idus.us.es/handle/11441/52298

Vygostky, L. (1978). *Teorías de la enseñanza. Modelo Sociocultural.* México. Trillas.

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

APÉNDICES

Doctorado En Ciencias De La Educación

APENDICE A. Guía de Entrevistas profesores

Entrevista sobre Competencia digital docente en Secundaria: El caso del Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

A continuación, se le harán una serie de preguntas como parte de una Investigación cuyo objetivo es dilucidar la contribución de las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales. Las respuestas son completamente confidenciales y solo le tomará unos minutos completar la entrevista. Siéntase en la libertad de contestar con completa sinceridad: no existen respuestas correctas o incorrectas.

Centro educativo: Instituto Politécnico Martina Mercedes Zouain

Regional/distrito: 08-06

Fecha: _____

Nombre: _____

Ciudad: Santiago de los Caballeros

País: República Dominicana

Materias que imparte en el área técnica de informática:

Género:

Femenino ◯

Masculino ◯

Edad promedio:

20-30 ◯

30-40 ◯

40-50 ◯

Más de 50 ◯

Formación académica:

Licenciatura ◯

Ingeniería ◯

Especialidad ◯

Magíster ◯

Doctorado ◯

1. ¿De qué manera identifican los recursos tecnológicos o sitios seguros para navegar en internet e instalar en sus dispositivos electrónicos?

2. ¿Cuáles serían las implicaciones del uso de contraseñas automáticas de sus cuentas en línea?

3. ¿Qué tipos de programas antivirus usted utiliza para prevenir los ataques informáticos?

4. ¿Cómo identifican y resuelven los problemas técnicos presentados al integrar las tecnologías en el aula?

5. ¿Cuáles serían las principales implicaciones que consideran a la hora de conectarse a redes Wifi de acceso libre al emplear internet?

6. ¿Qué tipo de tecnologías consideran como empleo pedagógico para la innovación y la calidad educativa en su planeación didáctica?

7. ¿Cómo identifica que la información de la red es verdadera o válida para la comunicación, colaboración, filtrado de contenidos digitales y publicaciones científicas?

8. ¿Cuáles estrategias tecnológicas utilizan para el desarrollo de las competencias de los alumnos?

9. ¿Cuáles herramientas tecnológicas le permiten la creación y edición de contenidos digitales?

10. ¿Qué impacto produce la aplicación de herramientas digitales en el aprendizaje del alumno?

¡Muchas gracias por su tiempo!

Doctorado En Ciencias De La Educación

APENDICE B. Cuestionario Estudiantes

Entrevista sobre Competencia digital docente en Secundaria: El caso del Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

A continuación, se le harán una serie de preguntas como parte de una Investigación cuyo objetivo es dilucidar la contribución de las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales. Las respuestas son completamente confidenciales y solo le tomará unos minutos completar la entrevista. Siéntase en la libertad de contestar con completa sinceridad: no existen respuestas correctas o incorrectas.

Centro educativo: Instituto Politécnico Martina Mercedes Zouain

Regional/distrito: 08-06

Fecha: _____

Ciudad: Santiago de los Caballeros

País: República Dominicana

Edad:

Curso:

Género:

Femenino ◯

Masculino ◯

1. ¿Cómo identificas los recursos tecnológicos seguros para navegar en internet e instalar en los dispositivos electrónicos?

2. ¿Cómo identificas los softwares innovadores o recursos tecnológicos para la generación de conocimientos en la realización de las actividades prácticas?

3. ¿Cuáles herramientas le permite la creación y edición de contenidos digitales?

4. ¿Cuáles son los riesgos de uso de contraseñas automáticas de sus cuentas en línea?

5. ¿Cuáles son los recursos o medios tecnológicos para la comunicación en las clases del Centro Educativo?

6. ¿Cuáles serían las principales implicaciones al conectarse a redes Wifi de acceso libre al emplear internet?

7. ¿Cómo identificas que la información de la red es verdadera o válida para la comunicación, colaboración, filtrado de contenidos digitales y publicaciones científicas?

8. ¿Qué mecanismos utilizas para cambiar la contraseña de tus cuentas personales y de servicios en línea?

9. ¿Cómo identificas las posibilidades de bullyng, sexting escolar o ciberbullying al establecer comunicación con desconocidos a través de la web?

10. ¿Qué tipo de apoyo ha recibido de su familia para cumplir con las actividades escolares en línea y cuales actividades has recibido en la plataforma virtual como complemento en tus clases?

¡Muchas gracias por su tiempo!

Doctorado En Ciencias De La Educación

APENDICE C. Guía de entrevista Personal Administrativo

Entrevista sobre Competencia digital docente en Secundaria: El caso del Instituto Politécnico Martina Mercedes Zouain, República Dominicana.

A continuación, se le harán una serie de preguntas como parte de una Investigación cuyo objetivo es dilucidar la contribución de las competencias digitales en el uso seguro de la tecnología de la información, comunicación, conocimiento y aprendizaje digitales. Las respuestas son completamente confidenciales y solo le tomará unos minutos completar la entrevista. Siéntase en la libertad de contestar con completa sinceridad: no existen respuestas correctas o incorrectas.

Centro educativo: Instituto Politécnico Martina Mercedes Zouain

Regional/distrito: 08-06

Fecha: _____

Ciudad: Santiago de los Caballeros

País: República Dominicana

Género:

Femenino ◯

Masculino ◯

Edad promedio:

20-30 ◯

30-40 ◯

40-50 ◯

Más de 50 ◯

Formación académica:

Licenciatura ◯

Especialidad ◯

Magíster ◯

Doctorado ◯

Otro_____

1. ¿Cuáles son los riesgos de emplear internet y cómo identificas los recursos tecnológicos seguros para navegar en internet e instalar en los dispositivos electrónicos?

2. ¿Qué procedimientos usted utiliza para crear contraseñas seguras?

3. ¿Conoce usted el procedimiento para manejar sus cuentas personales, documentos o archivos desde cualquier dispositivo electrónico?

4. ¿Cuáles han sido las principales dificultades que el Centro Educativo ha enfrentado para implementar las tecnologías y qué aplicaciones o herramientas resultan más complicadas para llevar a cabo su proceso de enseñanza aprendizaje?

5. ¿Cómo considera usted el uso de plataformas virtuales para la docencia presencial, semipresencial y virtual?

6. ¿De qué manera identifica usted los recursos tecnológicos seguros para instalar en su dispositivo electrónico?

7. ¿Cuáles son las implicaciones del uso de contraseñas automáticas de sus cuentas en línea?

8. ¿Qué medidas o elementos estratégicos emplea usted en la institución para el manejo apropiado de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales es (TICCAD)?

9. ¿Cuáles son los recursos o medios tecnológicos para la comunicación en las clases del Centro Educativo?

10. ¿Cuál es el nivel de integración de la familia en la escuela y qué medios estratégicos tecnológicos utiliza el Centro Educativo para integrar a las familias en la escuela como apoyo para reforzar las conductas inadecuadas y fomentar los valores humanos en los alumnos?

¡Muchas gracias por su tiempo!

APENDICE D Instrumento de validación

Por favor, marque con una X la respuesta escogida de entre las opciones que se presentan:

	sí	no
El instrumento contiene instrucciones claras y precisas para que los encuestados puedan responderlo adecuadamente (ver Anexo 1)		
El número de preguntas del cuestionario es excesivo		
Las preguntas constituyen un riesgo para el encuestado (en el supuesto de contestar SÍ, por favor, indique inmediatamente abajo cuáles)		

Preguntas que el experto considera que pudieran ser un riesgo para el encuestado:	
N.º de la(s) pregunta(s)	
Motivos por los que se considera que pudiera ser un riesgo	
Propuestas de mejora (modificación, sustitución o supresión)	

	Evaluación general del cuestionario			
	Excelente	Buena	Regular	Deficiente
Validez de contenido del cuestionario				

Observaciones y recomendaciones en general del cuestionario:	
Motivos por los que se considera no adecuada	
Motivos por los que se considera no pertinente	
Propuestas de mejora (modificación, sustitución o supresión)	

Identificación del experto

Nombre y apellidos	
Filiación (ocupación, grado académico y lugar de trabajo):	
e-mail	

Teléfono o celular	
Fecha de la validación (día, mes y año):	
Firma	

Muchas gracias por su valiosa contribución a la validación de este cuestionario.

APENDICE E. Programa o carrera del área de informática

PLAN DE ESTUDIOS DEL BACHILLERATO TÉCNICO EN INFORMÁTICA

Tercer Grado				Cuarto Grado			
Primer Semestre	**T**	**P**	**TH**	**Primer Semestre**	**T**	**P**	**TH**
Lengua Española	4		4	Lengua Española	2		2
Matemática	4		4	Matemática	2		2
Ciencias de la Naturaleza (Física)	3		3	Ciencias de la Naturaleza (Geología y Medio Ambiente)	2		2
Ciencias Sociales: Geografía e Historia desde mediados del Siglo XIX a mediados del Siglo XX.	3		3	Ciencias Sociales: Geografía e Historia desde mediados del Siglo XX a la actualidad.	2		2
Formación Integral, Humana y Religiosa	1		1	Formación Integral, Humana y Religiosa	1		1
Inglés Técnico I	8		8	Inglés Avanzado I	8		8
Educación Moral y Cívica	1		1	Legislación y Ética	1		1
Informática Aplicada I	1	2	3	Análisis y Diseño de Sistemas	3	3	6
Equipos y Sistemas Informáticos	2	6	8	Circuitos Lógicos	2	3	5
Algoritmos Computacionales	2	3	5	Programación II	2	7	9
				Cultura Emprendedora I	2		2
Total de Horas	**29**	**11**	**40**	**Total de Horas**	**27**	**13**	**40**
Segundo Semestre	**T**	**P**	**TH**	**Segundo Semestre**	**T**	**P**	**TH**
Lengua Española	4		4	Lengua Española	2		2
Matemática	4		4	Matemática	3		3
Ciencias de la Naturaleza (Física)	3		3	Ciencias de la Naturaleza (Geología y Medio Ambiente)	2		2
Ciencias Sociales: Geografía e Historia desde mediados del Siglo XIX a mediados del Siglo XX.	3		3	Ciencias Sociales: Geografía e Historia desde mediados del Siglo XX a la actualidad.	2		2
Formación Integral, Humana y Religiosa	1		1	Formación Integral, Humana y Religiosa	1		1
Inglés Técnico II	8		8	Inglés Avanzado II	8		8
Informática Aplicada II	1	2	3	Diseño de Páginas Web	2	7	9
Programación I	2	7	9	**Servicios de Redes Informáticas**	3	8	11
Bases de Datos Ofimáticas y Corporativas	2	3	5	**Cultura Emprendedora II**		2	2
Total de Horas	**28**	**12**	**40**	**Total de Horas**	**23**	**17**	**40**

Proyecto del centro original, impreso 2019-2022

APENDICE F. Codificación abierta

CODIFICACIÓN ABIERTA ESTUDIANTES			
Des	Discriminar elementos de seguridad en las páginas web	Ci	Capacidad de investigación.
Dmsi	Destrezas para el manejo seguro de internet	Ut	Uso de tecnología
Dms	Destreza para el manejo de sitios	Uh	Usabilidad de herramientas
Ris	Recursos para identificar la seguridad en internet	Cus	Conocimiento en el uso de softwares.
Sma	Seguridad para el manejo de aplicaciones..	Dt	Dominio de tecnología
Dns	Destreza para navegación segura.	Duv	Destreza para la utilización de virtualización.
Dc	Distinguir comentarios	Eut	Efectividad en el uso de tecnología.
Es	Elemento de seguridad	Fmi	Facilita el manejo de información.
Cin	Cifrado de información	Fgdoi	Facilita la gestión y organización de la información.
Rip	Riesgos en instalar programas.	Us	Uso de Software
Hmds	Habilidad en manejo de datos seguros.	Chd	Conocimiento de herramientas digitales
Rafs	Reconocer aplicaciones de fuentes seguras.	Cpve	Conocimiento de plataformas virtuales educativas.
Hisw	Habilidad identificar la seguridad en una web.	Mat	Mayor acceso a la tecnología.
Dns	Destreza para la navegación segura.	Dmrrus	Dispositivos con mayor rendimiento para uso de software.
Crpo	Capacidad de reconocer páginas oficiales seguras.	Ls	Licencias de software
Sma	Seguridad para el manejo de aplicaciones.	Dct	Destreza para el conocimiento tecnológico.
Imw	Identificación de malware en la web.	Ut	Uso de Tecnología
Dme	Destreza en mantenimiento a equipos	Fgi	Favorecer la gestión de la información.

Cda	Conocimiento de derechos de autor.	Chd	Conocimiento de herramientas Digitales
Ads	Almacenamiento de datos de sitios web.	Pdc	Publicación de datos confidenciales
Ap	Análisis perceptivo como destreza	Ri	Red insegura
Es	Elementos de seguridad	Ap	Acceso a privacidad
Dvissw	Detección de virus informáticos para sitios web.	Vf	Verifica fuentes
Si	Seguridad informática.	Drsi	Destreza para reconocer software innovador.
Cin	Conocimiento de información.	Ivf	Investigación de varias fuentes
Dsi	Dominio de software innovador.	Ca	Citas de autores
At	Aplicación de tecnología	I	Investigación
Pi	Prácticas innovadoras.	Pod	Página oficial del desarrollador
Smr	Softwares con mayor rendimiento	Pr	Página reconocida
Ut	Usabilidad tecnológica.	Vp	Verificación de perfil
Dct	Destreza para el conocimiento tecnológico.	Vd	Revisión del dominio
Ur	Uso de Recursos	Vurl	Verificación de URL
Dc	Diseño de contenidos	Av	Alertas de virus
Rai	Riesgo de acceso a información.	Cccf	Cambio de contraseña con frecuencia
Pcc	Pérdida de cuenta de correo.	Vi	Verificación de identidad
Hcu	Hackeo de cuentas de usuarios.	Cp	Configuración de privacidad
Pc	Pérdida de contraseña.	Dccc	Diferentes contraseñas para cada cuenta
Di	Discriminación de la información.	Cis	Contraseña igual siempre
Fi	Filtro de informaciones.	Ccc	Cambio de contraseña al compartirla
Pd	Plataformas digitales	Gm	Google Meet
Pm	Plataforma moodle.	Cm	Capacidad de memoria
Ai	Uso de internet.	Ocacc	Ocho caracteres alfanuméricos para crear cuentas

Pc	Plataforma classroom	B	Bullying
Rse	Redes sociales educativas	C	Ciberbullying
Pdi	Pantalla digital	Se	Sexting escolar
Ce	Correo electrónico	Conoci	Conocimiento de internet
Lap	Laptop	Df	Daño físico y verbal
Tel	Teléfono	Cdr	Comportamiento del desconocido en red
Z	Zoom	Ai	Acoso en internet
Im	Internet	Bu	Bloqueo de usuarios
Ade	Acceso a dispositivo electrónico	Drc	Desconocimiento de riesgos de ciberbullying
Vai	Vulnerabilidad de ataques informáticos	Cfi	Cuentas falsas en internet
Aii	Acceso ilegal de información	Apd	Aceptar personas desconocidas en redes sociales
Id	Intersección de dispositivo.	Ave	Acoso verbal
Rd	Robo de datos	Ai	Amenaza en internet
Hi	Hackeo de dispositivo	Ti	Temor en internet
Rcw	Robo de clave de wifi	Nd	Normativas de delito
Hu	Hackeo de ubicación de usuarios en línea	Aef	Apoyo económico familiar
Ad	Acceso a dispositivo	If	Internet fijo
Rd	Rastreo de dispositivos	De	Dispositivos electrónicos
Aip	Acceso a IP	Rd	Recursos didácticos
Vi	Virus informático	Am	Apoyo de maestros
De	Daño de equipo	Ae	Apoyo emocional
El	Equipo lento	Fp	Foro en plataforma
Ii	Intersección de información		
Di	Daño en sistemas		
Pd	Proporción de datos		

Mr	Mala calidad de red		
Sr	Sobrecarga de red		
Dpw	Diseño de portales web		
Rt	Revisión de tareas		
Am	Apoyo moral		
M	Motivación		
Vi	Velocidad de internet		
Hd	Herramientas digitales		
Cd	Contenidos digitales		
Pc	Proyectos colaborativos		
Pp	Páginas populares		

CODIFICACIÓN ABIERTA DOCENTES			
Fp	Fuente de procedencia	Du	Duolingo
Vp	Verificación-procedimiento	Ka	Kahoot
An	Antivirus	Of	Ofimática
Sr	Sitios reconocidos	Lp	Lenguajes de programación
Bu	Buscadores	Pa	Paint
Ie	Instituciones educativas	Qu	Quizizz
Cu	Cantidad de usuarios	Co	Computadora
		Pd	Pantalla digital
Sdc	Sustracción de datos confidenciales	Ce	Celular
Ri	Robo de identidad	Pm	Plataforma Moodle
Pcb	Penetración a cuenta bancaria	Ca	Canvas
Pp	Plagio de publicaciones	Wi	Window movie marker
He	Hackeo de equipo	Fi	Filmora
Vc	Vulnerabilidad de contraseña	Gf	Google form

Uic	Uso inadecuado de contraseña	Wo	Word
		Pp	Power Point
Da	Desconocimiento de antivirus	Ex	Excel
Apa	Antivirus de prevención de ataques	Ar	Ardora
		Ho	Hotpotatoes
Dut	Dificultades para usar las tic	Xe	Xelearning
Stae	Soporte técnico con ayuda del experto	Sc	Scratch
Ad	Analfabeto digital		
Dfc	Dificultad de falta de conexión	Ee	Eficiencia y eficacia
Pdd	Pantallas digitales defectuosas	As	Aprendizaje significativo
At	Autónomo de tic	Ap	Aprendizaje práctico
Cut	Complejidad para uso de tic	Pa	Participación activa
		Fc	Facilidad y comodidad
Ri	Redes inseguras	Dct	Desarrollo de competencias tecnológicas
Rid	Robo de identidad	Ma	Mantiene su atención
Iep	Información expuesta al publico	Mo	Motivación
Vpc	Virus en la pc	In	Interés
Hr	Hackeo en la red	At	Aprovechamiento del tiempo
Ctb	Clonación de tarjetas bancarias	Or	Organización
Dd	Distorsión de datos	Cld	Clases más dinámicas
Rl	Red lenta	Cd	Clase divertidas
		Me	Mayor entendimiento
Pd	Pizarras digitales	Aa	Atrae la atención
La	Laptop	Ht	Habilidades tecnológicas
Ce	Celular	De	Destreza
Hi	Herramientas de internet	Cs	Conocimientos significativos

Rs	Redes sociales		
Pd	Plataformas digitales	Co	Conferencias
Po	Programas de office	Ve	Videos educativos
P	Presentaciones	Pr	Presentaciones
Etw	Editor de texto Word	Pg	Proyectos grupales
Dr	Drive	Au	Audios
Yo	Youtube	Pm	Plataforma moodle
Im	Imágenes	Ce	Correo electrónico
Mo	Moodle	Gd	Google dray
Cl	Classroom	El	Ejercicios en línea
Vi	Videojuegos	Pd	Pantalla digital
Ga	Gamificación	Ev	Edición de videos
Wh	WhatsApp	Ji	Juegos interactivos
Vi	Videoconferencias	Bi	Búsqueda de información
		Tu	Tutoriales
Vfp	Verificación de la fuente de procedencia	Sp	Simulaciones de programas
Po	Páginas oficiales	Mu	Multimedios
Fc	Fuentes confiables	Ga	Gamificación
Us	Usabilidad	Bd	Barra de dirección
Ob	Objetividad	Cp	Contenidos publicados
Ri	Revistas indexadas		

CODIFICACIÓN ABIERTA ADMINISTRATIVO			
Ni	Navega en Internet	Ice	Intersección de correo electrónico
	Realiza descargas aplicaciones y documentos	Puc	Pérdida de usuario y contraseña
Pid	Penetración de información por desconocimiento	Rid	Robo de identidad y de dispositivo
		Rpi	Riesgo de pérdida de información
Cc	Crea contraseñas		
Mclca	Manipula cuentas en línea con contraseña automática	Vdr	Vulnerabilidad de datos en la red
Mdl	Manejo de documentos en línea	Ta	Talleres
		Ch	Charlas
Ucpd	Utiliza cuenta personal desde dispositivo	Jo	Jornadas de capacitación
		Cvpi	Contraseñas con vulnerabilidad por el proveedor del internet
Dmm	Dificultad para el manejo de moodle		
Bd	Brecha digital	Ui	Uso de Internet
Ed	Estudiantes desmotivados	Rs	Redes sociales
Ppc	Padres poco comprometidos	Pd	Pantallas digitales
Dt	Docentes con tecnofobia	Pm	Plataforma Moodle
Dc	Docentes cansados	Wh	WhatsApp
Dr	Docentes rezagados	Co	Computadora
Dmm	Dificultad para el manejo de Moodle		

Ci	Conexión inestable	Pif	Poca integración de la familia
As	Área con sobrepoblación	Ep	Escuela de padres
Fdrp	Falta de dispositivos para realizar practicas	Cp	Comités de padres
Cee	Carencia de energía eléctrica	Spae	Sociedad de padres amigos de la escuela
As	Aprendizaje significativo	De	Documentos escritos
Te	Trabajo en equipo	Cr	Convocatorias a reuniones
Dap	Desarrollo de actividades practicas	Ac	Actos
Cc	Complemento de la clase	Eb	Exposiciones en la bandera
Cc	Construcción de conocimientos	Di	Desconocimiento de información
Pa	Participación activa	Gwp	Grupos de WhatsApp con padres
Vf	Verificación de fuente		
An	Antivirus		
Ac	Acceso a credenciales		
Mde	Manipulación de dispositivos electrónicos		
Vp	Violación de privacidad		

APENDICE G. Codificación Axial

CODIFICACIÓN AXIAL ESTUDIANTES			
Des	Discriminar elementos de seguridad en las páginas web	Ci	Capacidad de investigación.
Dmsi	Destrezas para el manejo seguro de internet	Ut	Uso de tecnología
Dms	Destreza para el manejo de sitios	Uh	Usabilidad de herramientas
Ris	Recursos para identificar la seguridad en internet	Cus	Conocimiento en el uso de softwares.
Sma	Seguridad para el manejo de aplicaciones..	Dt	Dominio de tecnología
Dns	Destreza para navegación segura.	Duv	Destreza para la utilización de virtualización.
Dc	Distinguir comentarios	Eut	Efectividad en el uso de tecnología.
Es	Elemento de seguridad	Fmi	Facilita el manejo de información.
Cin	Cifrado de información	Fgdoi	Facilita la gestión y organización de la información.
Rip	Riesgos en instalar programas.	Us	Uso de Software
Hmds	Habilidad en manejo de datos seguros.	Chd	Conocimiento de herramientas digitales
Rafs	Reconocer aplicaciones de fuentes seguras.	Cpve	Conocimiento de plataformas virtuales educativas.
Hisw	Habilidad identificar la seguridad en una web.	Mat	Mayor acceso a la tecnología.
Dns	Destreza para la navegación segura.	Dmrrus	Dispositivos con mayor rendimiento para uso de software.
Crpo	Capacidad de reconocer páginas oficiales seguras.	Ls	Licencias de software
Da	Derecho de autor	Dct	Destreza para el conocimiento tecnológico.
Imw	Identificación de malware en la web.	Ut	Uso de Tecnología
Dme	Destreza en mantenimiento a equipos	Fgi	Favorecer la gestión de la información.
Cda	Conocimiento de derechos de autor.	Chd	Conocimiento de herramientas Digitales

Ads	Almacenamiento de datos de sitios web.	Pdc	Publicación de datos confidenciales
Ap	Análisis perceptivo como destreza	Ri	Red insegura
Es	Elementos de seguridad	Ap	Acceso a privacidad
Dvissw	Detección de virus informáticos para sitios web.	Vf	Verifica fuentes
Si	Seguridad informática.	Drsi	Destreza para reconocer software innovador.
Cin	Conocimiento de información.	Ivf	Investigación de varias fuentes
Dsi	Dominio de software innovador.	Ca	Citas de autores
At	Aplicación de tecnología	I	Investigación
Pi	Prácticas innovadoras.	Pod	Página oficial del desarrollador
Smr	Softwares con mayor rendimiento	Pr	Página reconocida
Ut	Usabilidad tecnológica.	Vp	Verificación de perfil
Dct	Destreza para el conocimiento tecnológico.	Vd	Revisión del dominio
Ur	Uso de Recursos	Vurl	Verificación de URL
Dc	Diseño de contenidos	Av	Alertas de virus
Rai	Riesgo de acceso a información.	Cccf	Cambio de contraseña con frecuencia
Pcc	Pérdida de cuenta de correo.	Vi	Verificación de identidad
Hcu	Hackeo de cuentas de usuarios.	Cp	Configuración de privacidad
Pc	Pérdida de contraseña.	Dccc	Diferentes contraseñas para cada cuenta
Di	Discriminación de la información.	Cis	Contraseña igual siempre
Fi	Filtro de informaciones.	Ccc	Cambio de contraseña al compartirla
Pd	Plataformas digitales	Gm	Google Meet
Pm	Plataforma moodle.	Cm	Capacidad de memoria
C	Citas	Ocacc	Ocho caracteres alfanuméricos para crear cuentas
Pc	Plataforma classroom	B	Bullying

Rse	Redes sociales educativas	C	Ciberbullying
Pdi	Pantalla digital	Se	Sexting escolar
Ce	Correo electrónico	Ci	Conocimiento de internet
Lap	Laptop	Df	Daño físico y verbal
Tel	Teléfono	Cdr	Comportamiento del desconocido en red
Z	Zoom	Ai	Acoso en internet
Ui	Uso de red de internet	Bu	Bloqueo de usuarios
Ade	Acceso a dispositivo electrónico	Drc	Desconocimiento de riesgos de ciberbullying
Vai	Vulnerabilidad de ataques informáticos	Cfi	Cuentas falsas en internet
Aii	Acceso ilegal de información	Apd	Aceptar personas desconocidas en redes sociales
Id	Intervencion de dispositivo.	Ave	Acoso verbal
Rd	Robo de datos	Ai	Amenaza en internet
Hi	Hackeo de dispositivo	Ti	Temor en internet
Rcw	Robo de clave de wifi	Nd	Normativas de delito
Hu	Hackeo de ubicación de usuarios en línea	Aef	Apoyo económico familiar
Ad	Acceso a dispositivo	If	Internet fijo
Rd	Rastreo de dispositivos	De	Dispositivos electrónicos
Aip	Acceso a IP	Rd	Recursos didácticos
Vi	Virus informático	Am	Apoyo de maestros
De	Daño de equipo	Ae	Apoyo emocional
El	Equipo lento	Fp	Foro en plataforma
Ii	Intersección de información	Cri	Conexión de la red de internet
Di	Daño en sistemas	Usri	Uso de Sistema de red de internet
Pd	Proporción de datos	Ri	Red de internet
Mr	Mala calidad de red		

Sr	Sobrecarga de red		
Dpw	Diseño de portales web		
Rt	Revisión de tareas		
Am	Apoyo moral		
M	Motivación		
Vi	Velocidad de internet		
Hd	Herramientas digitales		
Cd	Contenidos digitales		
Pc	Proyectos colaborativos		
Pp	Discriminar páginas populares		

CODIFICACIÓN AXIAL DOCENTES			
Fp	Fuente de procedencia	Vi	Videoconferencias
Sr	Sitios reconocidos	Tu	Tutoriales
Bo	Buscadores Oficiales	Mu	Multimedios
Ie	Instituciones educativas	Ga	Gamificación
Cu	Cantidad de usuarios	Au	Audios
Po	Páginas oficiales	Ji	Juegos interactivos
Us	Usabilidad	Pg	Proyectos grupales
Ob	Objetividad	El	Ejercicios en línea

Bd	Barra de dirección	Sp	Simulaciones de programas
Cp	Contenidos publicados	Lp	Lenguaje de programación
Ri	Revistas indexadas		
Apa	Antivirus de prevención de ataques	Pa	Paint
		Wo	Word
Sdc	Sustracción de datos confidenciales	Pp	Power Point
Ri	Robo de identidad	Ex	Excel
Pcb	Penetración a cuenta bancaria		
Vc	Vulnerabilidad de contraseña	Ka	Kahoot
Uc	Uso inadecuado de contraseña	Ho	Hotpotatoes
Da	Desconocimiento de antivirus	Xe	Xelearning
Ri	Redes inseguras	Gf	Google form
Dd	Distorsión de datos	Gd	Google drive
Iep	Información expuesta al publico	Ce	Correo electrónico
Vp	Virus en la PC		
Hr	Hackeo en la red	Wmm	Window movie marker
Ctb	Clonación de tarjetas bancarias	Ar	Ardora
Pp	Plagio de publicaciones	Fi	Filmora
		Qu	Quizizz
Dfc	Dificultad de falta de conexión	Ca	Canvas
Pdd	Pantallas digitales defectuosas	sc	Scratch

Rl	Red lenta		
Dum	Dificultad para uso de Moodle	Pee	Promueve la eficiencia y eficacia
Stae	Soporte técnico con ayuda del experto	As	Aprendizaje significativo
Cut	Complejidad para uso de tic	Ap	Aprendizaje práctico
		Pp	Participación activa
At	Autónomo de tic	Fc	Facilidad y comodidad
Bi	Búsqueda de información	Dct	Desarrollo de competencias tecnológicas
		Ma	Mantiene su atención
Du	Duolingo	Mo	Motivación
Mo	Moodle	In	Interés
cl	Classroom	At	Aprovechamiento del tiempo
		Or	Organización
		Cmd	Clases más dinámicas
Yo	Youtube	Cd	Clase divertidas
wh	WhatsApp	Me	Mayor entendimiento
		Aa	Atrae la atención
Pd	Pizarra digital	Ht	Habilidades tecnológicas
Co	Computadora	De	Destreza
Ce	Celular	Cs	Conocimientos significativos

CODIFICACIÓN AXIAL ADMINISTRATIVO			
Ni	Navega en Internet	Ice	Intersección de correo electrónico
Rdad	Realiza descargas de aplicaciones y documentos	Puc	Pérdida de usuario y contraseña
Pid	Penetración de información por desconocimiento	Rid	Robo de identidad y de dispositivo
Uci	Utiliza celular para investigar	Rpi	Riesgo de pérdida de información
Cc	Crea contraseñas	Vdr	Vulnerabilidad de datos en la red
Mdl	Manejo de documentos en línea		
Cmcl	Manipula su cuenta en línea con contraseña automática	Ta	Talleres
Dd	Digita documentos	Ch	Charlas
Dmcl	Desconocimiento de manejo de cuentas en línea	Jo	Jornadas de capacitación
Dcl	Desconocimiento de contraseñas seguras	Cvpi	Contraseñas con vulnerabilidad por el proveedor del internet
Dve	Deserción de varios estudiantes	Rre	Reflexiones o retiro espiritual
Ver	Varios estudiantes reprobados	Ui	Uso de Internet
Cp	Crea presentaciones	Rs	Redes sociales
Ucezm	Ubicación del centro educativo en zona marginada	Upd	Uso de pantallas digitales
Ucpd	Utiliza cuenta personal desde dispositivo	Pm	Plataforma Moodle
Cdt	Crea documentos de texto	Wh	WhatsApp
Sarc	Sin acceso a ruta de concho	Co	Computadora
Bd	Brecha digital	Zf	Zona fría
Ed	Estudiantes desmotivados	Pif	Poca integración de la familia
Ppc	Padres poco comprometidos	Ep	Escuela de padres
Dt	Docentes con tecnofobia	Cp	Comités de padres

Dc	Docentes cansados	Spae	Sociedad de padres amigos de la escuela
Dr	Docentes rezagados	De	Documentos escritos
Dmm	Dificultad para el manejo de Moodle	Cr	Convocatorias a reuniones
Ci	Conexión inestable	Ac	Actos
As	Área con sobrepoblación	Eb	Exposiciones en la bandera
Fdrp	Falta de dispositivos para realizar practicas	Di	Desconocimiento de información
Cee	Carencia de energía eléctrica	Gwp	Grupos de WhatsApp con padres
Pst	Poca señal telefónica	Ups	Uso de plataforma siger
As	Aprendizaje significativo	Vf	Verificación de fuente
Te	Trabajo en equipo	An	Antivirus
Dap	Desarrollo de actividades practicas	Ac	Acceso a credenciales
Cc	Complemento de la clase	Mde	Manipulación de dispositivos electrónicos
Cc	Construcción de conocimientos	Vp	Violación de privacidad
Pa	Participación activa	Gp	Grupo pedagógico

APENDICE H. Codificación Selectiva

CODIFICACIÓN SELECTIVA ESTUDIANTES		
Número	**Aproximación semántica**	**Categorías**
1	**Penetración o hackeo informático**	d. Acceso-intervención e. Virus informático f. Riesgos-discriminación
2	**Competencia digital del estudiante**	a. Conocimientos b. Habilidades-destrezas
3	**Seguridad informática**	e. Elementos-recursos f. Acceso g. Detección-alertas h. Configuración-cifrado i. Efectividad-vulnerabilidad
4	**Discriminación de información en la red -internet**	c. Capacidad- Destrezas d. Conocimiento-análisis e. Filtro-investigación f. Verifica g. Facilita-favorece h. Reconoce-cita y parafrasea
5	**Resolución de problemas técnicos**	e. Usabilidad- destreza f. Dominio-prácticas g. Almacenamiento-drive
6	**Características de los softwares y dispositivos**	a. Utilidad-usabilidad b. Lenguaje-flexibilidad c. Versión-seguridad d. Licencia e. Velocidad-dispositivo f. Eficiencia

7	**Uso de medios y recursos tecnológicos**	a. Internet b. Pantalla digital-laptop c. Googlemeet- zoom-cámaras d. Acceso-uso e. Dispositivos-teléfono f. Herramientas-sistemas- software
8	**Diseño de contenidos digitales**	h. Proyección i. Diseño-imágenes, mapas-video j. Contenidos-recursos k. Software especializado
9	**Calidad en el servicio de internet**	a. Velocidad b. Fijo c. Conexión d. Sistema e. Red-suplidor responsable f. Sobrecarga de internet
10	**Medios para la comunicación virtual**	a. Proyectos b. Foros c. Correo d. Redes-chat e. Plataforma-videoconferencias f. Aplicaciones
11	**Leyes y normativas tecnológicas**	a. Acceso b. Normativas c. Normas internacionales para la citación d. Derecho de autor
12	**Alfabetización digital**	a. Computadora b. Capacidad-conocimiento c. Antivirus d. Equipo e. Calidad-elaboración de contenidos

13	**Ciberseguridad y ciudadanía digital**	e. Bullyng-ciberbullying f. Sexting escolar g. Comportamiento antisocial h. Amenaza-daño i. Hackeo -cuentas j. Desconocimiento-virus k. Acoso-temor
14	**Tutoría**	a. Motivación b. Apoyo- acompañamiento c. Revisión d. Seguimiento-monitoreo e. Orientación-asesoría

CODIFICACIÓN SELECTIVA DOCENTES		
Número	**Aproximación semántica**	**Categorías**
1	**Seguridad en la Red**	f. Fuente de procedencia g. Sitios reconocidos h. Buscadores Oficiales i. Instituciones educativas j. Cantidad de usuarios k. Páginas oficiales l. Usabilidad m. Objetividad n. Barra de dirección o. Contenidos publicados p. Revistas indexadas q. Antivirus de prevención de ataques
2	**Hackeo de Información**	g. Sustracción de datos confidenciales h. Robo de identidad i. Penetración a cuenta bancaria j. Vulnerabilidad de contraseña k. Uso inadecuado de contraseña l. Desconocimiento de antivirus m. Redes inseguras n. Distorsión de datos o. Información expuesta al publico p. Virus en la PC q. Hackeo en la red r. Clonación de tarjetas bancarias s. Plagio de publicaciones
3	**Dificultades para Usar las TIC**	f. Dificultad de falta de conexión g. Pantallas digitales defectuosas h. Red lenta

		i. Dificultad para uso de Moodle j. Soporte técnico con ayuda del experto k. Complejidad para uso de tic
4	**Resuelve problemas Técnicos**	a. Autónomo de tic b. Búsqueda de información
5	**Medios o Recursos Tecnológicos**	a. Videoconferencias b. Tutoriales c. Multimedios d. Gamificación e. Audios f. Juegos interactivos g. Proyectos grupales h. Ejercicios en línea i. Simulaciones de programas j. Lenguaje de programación
6	**Ofimática**	a. Paint b. Word c. Power Point d. Excel
7	**Herramientas de Internet**	g. Kahoot h. Hotpotatoes i. Xelearning j. Google form k. Google drive l. Correo electrónico
8	**Diseños de Contenidos Digitales**	a. Window movie marker b. Ardora c. Filmora d. Quizizz e. Canvas f. Scratch
9	**Plataforma**	a. Duolingo b. Moodle c. Classroom
10	**Redes Sociales**	a. Youtube b. WhatsApp
11	**Dispositivos Electrónicos**	a. Pizarra digital b. Computadora c. Celular

12	**Importancia de la Tecnología en el aula**	f. Promueve la eficiencia y eficacia g. Aprendizaje significativo h. Aprendizaje práctico i. Participación activa j. Facilidad y comodidad k. Desarrollo de competencias tecnológicas l. Mantiene su atención m. Motivación n. Interés o. Aprovechamiento del tiempo p. Organización q. Clases más dinámicas r. Clase divertidas s. Mayor entendimiento t. Atrae la atención u. Habilidades tecnológicas v. Destreza w. Conocimientos significativos

CODIFICACIÓN SELECTIVA ADMINISTRATIVO		
Número	**Aproximación semántica**	**Categorías**
1	**Penetración de información por desconocimiento (Hackeo)**	f. Intersección de correo electrónico g. Pérdida de usuario y contraseña h. Robo de identidad y de dispositivo i. Riesgo de pérdida de información j. Vulnerabilidad de datos en la red k. Penetración de información por desconocimiento l. Desconocimiento de manejo de cuentas en línea m. Desconocimiento de contraseñas seguras n. Contraseñas con vulnerabilidad por el proveedor del internet o. Acceso a credenciales p. Manipulación de dispositivos electrónicos q. Violación de privacidad
2	**Dificultades para el uso de Tecnología para la Resolución de Problemas Técnicos**	e. Brecha digital f. Docentes con tecnofobia g. Docentes cansados h. Docentes rezagados i. Dificultad para el manejo de Moodle j. Conexión inestable k. Falta de dispositivos para realizar practicas l. Carencia de energía eléctrica m. Poca señal telefónica

	Identificación de Necesidades e Implicaciones del Centro Educativo para Integrar la Familia en la Escuela	a. Deserción de varios estudiantes b. Varios estudiantes reprobados c. Ubicación del centro educativo en zona marginada d. Sin acceso a ruta de concho e. Estudiantes desmotivados f. Padres poco comprometidos g. Área con sobrepoblación h. Zona fría i. Poca integración de la familia j. Desconocimiento de información
4	**Medios de Comunicación para las Clases**	a. Escuela de padres b. Comités de padres c. Sociedad de padres amigos de la escuela d. Documentos escritos e. Convocatorias a reuniones f. Actos g. Exposiciones en la bandera h. Talleres i. Charlas j. Jornadas de capacitación k. Reflexiones o retiro espiritual l. Grupos de WhatsApp con padres m. Grupo pedagógico
5	**Seguridad Informática**	a. Verificación de fuente b. Antivirus
6	**Información y Alfabetización Digital**	e. Navega en Internet f. Realiza descargas de aplicaciones y documentos g. Crea contraseñas h. Manejo de documentos en línea i. Manipula su cuenta en línea con contraseña automática j. Utiliza cuenta personal desde dispositivo
7	**Creación de Contenidos**	a. Digita documentos b. Crea presentaciones c. Crea documentos de texto d. Uso de plataforma Siger
8	**Comunicación y Recursos TIC para las Clases**	a. Utiliza celular para investigar b. Uso de Internet c. Redes sociales d. Uso de pantallas digitales e. Plataforma Moodle f. WhatsApp g. Computadora
9	**Importancia de la Plataforma MOODLE para la Docencia**	a. Aprendizaje significativo b. Trabajo en equipo c. Desarrollo de actividades practicas d. Complemento de la clase e. Construcción de conocimientos f. Participación activa

APENDICE I. Respuestas de los participantes

Respuestas de la aplicación de instrumentos de evaluación

Estudiantes

1. ¿Cómo identificas los recursos tecnológicos seguros para navegar en internet e instalar en los dispositivos electrónicos?
1. Es un poco cuesta arriba poder identificar si una página es segura o no, pero unas de las principales cosas son: es muy popular entre las personas, tiene buena reputación entre otras más. 2. Actualmente los softwares de navegación están muy avanzados ya que estos mismos nos pueden decir si es una página segura o no. Para identificarlo es con un pequeño candado que aparece en el área de la dirección de la página. 3. Certificados, HTTPS, símbolo del candado y antivirus para el navegador anunciarlos. 4. Para la instalación usamos un antivirus. Para la web nos percatamos si la URL es "https" y tenga el candadito de color verde. 5. Móviles y computadoras son seguras para navegar siempre y cuando haya acceso a internet seguro y con clave. 6. Para esto, tenemos que saber en qué páginas navegamos y no siempre aceptar, acceder o dar permiso sin antes leer. Lo mismo cuando instalamos una app, debemos de tomar en cuenta hasta los comentarios e instalar de una plataforma segura para evitar que se nos entre algún virus o que nos espíen. 7. Dependiendo si el sitio web contiene un certificado de autenticación, malware o algo anormal, es signo de que no es seguro. 8. La página debe estar verificada de forma segura. 9. Los identifico como útiles para nuestro día a día. 10. No se 11. No se 12. No se 13. En las páginas web, arriba al lado del enlace parece un candado si está cerrado la página es segura, si no, no es segura. 14. Cuando entramos a una página web segura aparece un candadito en la esquina de la URL, si este está cerrado y en verde es seguro, pero sí está en gris y abierto es inseguro. 15. Cuando es segura se muestra un candado como de privacidad. Cuando es insegura muestra un link de que si quieres salir de la página o no. 16. Primero miro los comentarios donde dicen si es segura o no seguro. Verifico si tiene muchas visitas. 17. Sabemos que la página es segura si muestra un candado cerrado, si no muestra, no es segura. 18. Se puede identificar como, por ejemplo: si tú tienes una aplicación como si quieres descargar una canción te dice, ¿Estás seguro que quieres descargar esta? 19. Investigan de esos recursos. 20. Yo diría que investigando bien esa página para que no haya problemas. 21. Lo identifico porque en el link del navegador aparece "HTTPS".

22. Investigando sobre el programa y estar de acuerdo con la página y que sea original y de confianza.
23. Bueno con el HTTPS, el nombre que tienen todas las cuentas o con el logo de la página.
24. Bueno por medio del candado en la parte del buscador, también con la publicidad si esta es mucha puede ser insegura.
25. Mediante el análisis perceptivo (revisar la extensión en caso de que sea una aplicación o la seguridad SSL si es una página web).
26. Por medio de antivirus y VPN, al igual que los certificados de seguridad de la página.
27. Antivirus y certificados de seguridad de la página.
28. A través de programas decodificadores.
29. A través de la alerta del antivirus.
30. A través de aplicaciones instaladas.
31. No sé.
32. No se
33. A través de investigación, y uso de antivirus.
34. Si un creador de contenido famoso promociona una página o aplicación, lo más seguro es que esa página o herramienta es verídica. También si una página como Wikipedia tiene buena fama lo más seguro es que sea segura.
35. No se
36. No se
37. Pues se puede decir que hoy en día identificarlos es más fácil ya que para ello hay varias apps y métodos.
38. Cuando la página me advierte sobre ésta.
39. La identifico como cuando entran a la página y me llega una notificación que dice que entro sin permiso.
40. Cuando sé que es seguro lo uso.
41. El computador identifica enseguida cuando la página no es segura, por ejemplo: "Esta página tiene virus, cookies".
42. Depende de ésta por tal razón siempre leo antes de permitir algún acceso.
43. Muchas veces tiene un candadito o te realizan una pregunta.
44. Cuando la página tiene el candado y no tenga cookies.
45. Las aplicaciones son seguras cuando solo tenemos acceso nosotros mismos mientras que otra persona no puede supervisar nada.
46. Si no presenta el candado cerrado, donde esta www.
47. Cuando son de sitios seguros o páginas reconocidas oficiales.
48. Poco conocimiento.
49. Con un antivirus.
50. La pc o dispositivo te avisa si es seguro o no en la barra donde te muestra el https.
51. Lo primero es revisar el link de cualquier página en la que entremos, ver qué tipo de HTTPS tiene todo correcto.
52. Con un candado en el URL.
53. A través de la actualización.
54. Una alerta en la parte superior derecha en un candado.
55. Identificando los recursos originales de la empresa.
56. No identifico muchas páginas falsas las cuales hackean nuestro sistema como contraseñas, usuarios, entre otros.
57. Cuando puedo utilizarlo sin errores.
58. Cuando no se presenta el uso de cookies.

59. Cuando una página comienza con HTTPS.
60. Bueno yo diría en seguridad, que hay que tener cuidado si tiene virus o no.
61. Cuando no tiene virus.
62. Cuando no presentan mensajes de alertas de virus.
63. Algunos recursos que utilizo son herramientas como VPN, también algunos navegadores tienen funciones de anti-rastreo, bloqueadores de anuncios, también otras formas de estar seguro es entrar en sitios que tengan el protocolo HTTPS.
64. Recursos tecnológicos seguros son aquellos que dependen de una seguridad informática.
65. Que en la página que uno esté navegando tenga "HTTPS", la "S" del final y cuando uno vaya a descargar algo lo haga desde una página oficial.
66. Viendo si usa HTTPS en la dirección.
67. Son seguros y confiables ya que de igual forma están en un ámbito seguro y cerrado para ti.
68. Son seguros y confiables porque te sientes en un lugar seguro y confiable para ti.
69. Pues en páginas web se identifica por la S en el HTTPS lo cual significa "security" y avisa que la página está asegurada, y un candadito que se figura al lado, dependiendo del navegador.
70. Yo lo identifico por el candado verde que aparece donde se coloca la URL.
71. Si el candadito de la parte superior izquierda está en color verde, indica que es seguro y también con HTTPS.

2. ¿Cómo identificas los softwares innovadores o recursos tecnológicos para la generación de conocimientos en la realización de las actividades prácticas?

1. Para poder identificarlo se puede apreciar que tiene mucha usabilidad y los servicios que brindan son recomendados.
2. Herramientas o dispositivos para facilitar una tarea y que el usuario se sienta cómodo al usarlo.
3. Cuando es muy utilizado por la comunidad.
4. Algunos recursos tecnológicos como los móviles y computadoras nos ayudan a generar conocimientos e informaciones en la realización de actividades prácticas.
5. Excelente, ya que, con su ayuda durante esta pandemia, la educación virtual ha sido posible para las clases, tareas y actividades.
6. Son muy buenos porque gracias a ellos tenemos un mayor acceso a la tecnología.
7. Son buenas apps.
8. Probándolo en diferentes dispositivos con distintas cantidades de memoria.
9. Su fecha de salida al mercado y así confirmar si es nueva e innovadora.
10. Investigar bien los datos necesarios.
11. Por sus nuevas funciones como software.
12. WhatsApp me ayuda a que manden información que no se de en la escuela y google Meet para entrar a Video llamadas desde casa.
13. Probándolo en diferentes dispositivos de distintos espacios de memoria.
14. Se puede identificar los softwares como unos conocimientos.
15. Viendo el número de personas que tiene copiada para evitarla.
16. Me pongo a investigar cuando necesito un nuevo software para realizar la tarea.
17. Muy utilizado y necesario.
18. Lo identificamos cuando dicho software cambia la forma en que la persona usa el PC.
19. Todos los recursos son modernos, o sea, saliéndose de lo tradicional.

20. Lo identifico bien, ya que las clases las podemos hacer desde casa si no completamos.
21. Dependiendo de las mejoras presentadas en la usabilidad, velocidad de ejecución y además mejoras significativas.
22. Si presentan ideas con mayor capacidad o mayor optimización.
23. Determinado si son efectivos y tienen más herramientas que me ayuden a desempeñarme.
24. Que son más cómodos de manejar.
25. Cuando presentan soluciones con la idea de simplificar labores a nosotros en la vida cotidiana o que simplemente nos ayuden.
26. Una gran comunicación es un gran aprendizaje así que estos equipos suministrados son un punto vital para la enseñanza.
27. Buscando información respecto al tema.
28. Si después de haber utilizado el software me quedo satisfecho con el resultado, me mantendré utilizando esa aplicación.
29. Muy buena ya que es una manera más eficaz, es fácil.
30. Excel.
31. Usamos PowerPoint, Word, para el comienzo de la clase.
32. Excel.
33. Excel, Word, PowerPoint.
34. Excel, PowerPoint.
35. No tengo conocimientos.
36. No tengo conocimientos.
37. Son aplicaciones que nos sirven como material de apoyo para desarrollar nuestro proyecto.
38. Excel y PowerPoint.
39. Lo identifico cuando son recomendables para llevar a cabo las actividades.
40. Muy bien.
41. Cuando uno no lo ha visto anteriormente.
42. En su desarrollo y ejecución.
43. Bueno yo diría que sí es un software que yo no había visto antes, lo reconozco como uno nuevo.
44. En una página web.
45. Los identifico viendo el programa y las características que tiene.
46. Que faciliten lo que hacemos.
47. Star Tor Browser, Safari y Brackets.
48. Cuando tienen una buena optimización y fluidez.
49. Cuando vemos programas los cuales no conocíamos.
50. Yo los identifico bien.
51. Cuando traen nuevas funciones necesarias.
52. Que tenga buen funcionamiento.
53. Pienso que los softwares innovadores son lo más nuevo y lo que están usando.
54. Cuando se identifican las herramientas nuevas y útiles.
55. Cuando es algo nuevo.
56. Debemos instalarlos y ver que los recursos que tienen sean nuevos y que tengan buen funcionamiento.

3. ¿Cuáles herramientas le permite la creación y edición de contenidos digitales?

1. Sublime text, Brackets y Visual Studio.

2. Blog de notas, Visual Studio, Sublime text y Brackets.
3. Editores de video, fotos y texto.
4. Editores de texto como Sublime text y Visual Studio, también editores de videos como Filmora 9 y Camtasia.
5. Algunas pueden ser Word, PowerPoint, Brackets, PSint y SQL Server que son herramientas de creación y edición de contenidos digitales como presentaciones, páginas web, diagramas, entre otros.
6. Los programas de Microsoft, herramientas de google como: Word, Excel, drive, documentos o cualquier otra app.
7. SQL Server, PowerPoint y Filmora.
8. Visual Studio, Photoshop, Word, Excel, PowerPoint.
9. En internet podemos encontrar mucha información sobre herramientas para eso.
10. Word, PowerPoint y Photoshop.
11. Entre las herramientas para crear contenidos digitales están el paquete de office.
12. PDF, Word, Excel, Brackets, entre otros.
13. Word, PowerPoint, Excel e Inshot.
14. PowerPoint y Brackets.
15. Word.
16. Word, PDF, PowerPoint y Excel.
17. Audacitu, Visual Studio Code y Filmora
18. PowerPoint, Google docs y Excel.
19. Editores de texto, multimedia y compilador de código
20. Dependiendo de qué tipo de contenido, por ejemplo: Para fotos Photoshop y para videos Filmora.
21. Photoshop, Brackets, Visual Studio, Adobe Premier, Adobe Lightroom, SQL Server, entre otros.
22. Photoshop, Premiere.
23. Word.
24. Foto edict.
25. Editores de textos y videos e imágenes.
26. Editores de texto, de video y de imagen.
27. Editores de texto, edición de foto, video y gif.
28. Depende de qué tipo de contenido porque hay demasiadas, como editores de texto, editores de imágenes, editores de video, entre muchos otros.
29. Wonder Share Filmora, Microsoft Word, PowerPoint, Visual Studio, Sublime Text, Visual Studio Code.
30. Editores de texto, video e imagen.
31. Sublime Text, Photoshop, Vidio Star.
32. En lo personal solo uso Word.
33. PowerPoint y Word.
34. No tengo conocimiento.
35. Excel, PowerPoint y Word.
36. Word, PowerPoint, Blog.
37. PowerPoint y Word.
38. Word y PowerPoint.
39. Word y PowerPoint.
40. Word, PowerPoint, otros Softwares
41. PowerPoint y Word.
42. Word, Excel, PowerPoint, entre otros.

43. PowerPoint y Word.
44. Brackets, Visual Test, Atom, SQL.
45. Brackets, sublime text.
46. PowerPoint, Word, Excel, Power Director, entre otros.
47. Facebook, Telegram y WhatsApp.
48. Las herramientas de office y los de edición.
49. Brackets.
50. Camtasia, PowerPoint y Word.
51. Word, editores de código, entre otros.
52. Filmora, PSint y Audacity.
53. Word, Canva, PowerPoint, Excel.
54. Word, Excel, PowerPoint y correo electrónico.
55. Editores de código, programas de ofimática, editores de fotos, gráficos y videos, IDE.
56. Sublime text y visual studio.
57. Office completo, sulime, brackets, visual studio y notepad.
58. Photoshop, Filmora, Adobe efects, Sony Vegas.
59. Visual studio y SQL.
60. Sublime Text, Visual Studio y SQL Server.
61. Brackets, Photoshop, Microsoft Office, Sublime Text, Lightroom, Atom y Adobe.
62. Visual Studio, Sublime Texto y Office.
63. Notepad + +, Sublime text, Paquete de Offic, Visual Studio y Brackets.

4. ¿Cuáles son los riesgos de uso de contraseñas automáticas de sus cuentas en línea?

1. Que puedan entrar fácilmente a tus cuentas y acceder más fácil a tu información.
2. Pueden perder sus cuentas, y cambiar el correo o la contraseña.
3. Que si te roban tu teléfono pueden entrar directo sin poner ninguna clave.
4. Los riesgos son aquellos que cuando uses tu teléfono te manda una notificación y en esa notificación te dice que si quieres guardar tu contraseña.
5. Qué personas maliciosas puedan acceder a ella, ya que las contraseñas que están en la nube no son 100% seguras.
6. La página puede fallar y la contraseña puede caer en manos equivocadas y pueden acceder a nuestra información.
7. Los piratas informáticos podrían atacar tu cuenta y acceder fácilmente y robar tu información a personas para usarlas o venderlas.
8. Pueden ser accesibles con facilidad y con el uso de diccionarios se des encripta.
9. Como es automática puede existir la posibilidad de que se le genere la misma contraseña a otro usuario, también es más fácil que te roben la contraseña y es menos segura.
10. Algún otro usuario puede hackear la cuenta a la cual has escogido el uso de contraseña automática.
11. Uno de los riesgos es que si alguien toca o roba uno de nuestros dispositivos electrónicos, tendría acceso a las redes sociales, cuentas de banco, entre otros.
12. La contraseña tiene que ser una que solo esa persona la sepa, de lo contrario le podrían robar su información.
13. Puede que alguien más (ya sea conocido) pueda ver su privacidad y puede que tenga la misma contraseña en otros sitios.
14. Son menos seguras, ya que la vulnerabilidad que conlleva mantenerlos guardados en el navegador, hace que algún atacante la detecte y robe más fácil a través del internet.

15. Los riesgos son que alguien podría robar tus datos o hackear tu cuenta.
16. Que me pueden robar los datos de usuario.
17. Puede ser hackeada.
18. Pueden hackearte tus redes, cualquier persona experimentada en el sistema accede sin problemas.
19. Que cualquier persona la puede tener ya que no todos los dispositivos son seguros.
20. Al estar con la misma contraseña mucho tiempo es más fácil que te hacken tu cuenta principal.
21. Uno de los riesgos es que como las contraseñas son aleatorias les puede tocar tu contraseña a otras personas.
22. Que se me pierda la contraseña o se me olvide.
23. Que si entras a un sitio web donde tienes una contraseña automática, es posible que puedan acceder los atacantes sin problemas.
24. Hackeo de tu cuenta.
25. Que pueden entrar y robar información.
26. Son fáciles de hackear.
27. Que si te roban el PC y está desbloqueado pueden entrar al google y hackear sus cuentas.
28. Que esa contraseña puede guardarse en una base de datos y los administradores pueden verla.
29. Que pueden ver lo que estás buscando.
30. Las contraseñas automáticas se encuentran en listas predeterminadas, se vuelven casi imposible para personas ajenas al hacking, pero para aquellos dedicados es bastante fácil.
31. Las contraseñas automáticas suelen estar en diccionarios de fuerza bruta y, de esa forma, penetrar tus cuentas.
32. Son pocos seguros ya que las crea una inteligencia artificial que puede ser fácilmente vulnerado.
33. Se quedan guardadas en el celular o en el equipo y las personas pueden tener acceso a esas contraseñas.
34. Que es más fácil de ser hackeado.
35. Que pueden hackear.
36. Pueden ser predecibles.
37. Estar expuestos a hackers y virus que tienen la intención de filtrar sus documentos personales.
38. Puede que la persona olvide la contraseña si no usa un Administrador de contraseñas.
39. Existe la posibilidad de que esas contraseñas automatizadas no sean muy seguras, y también existe una alta posibilidad de que se nos vaya a olvidar.
40. Que la misma página pueda acceder a su perfil.
41. Cualquier hacker logra tenerla tiene acceso literalmente a todas ellas.
42. Que pueden ser robados más fácil ya que son fáciles de decodificar.
43. Olvidarlas.
44. No tengo idea.
45. Se pueden filtrar informaciones.
46. Que nos pueden robar nuestros datos.
47. Se pueden filtrar informaciones personales.
48. Pueden ser hackeadas sus cuentas.
49. Que pueden hackear y robar todos nuestros datos.

50. Pueden obtener informaciones sobre nuestros datos personales como fotos.
51. Robo de cuenta o información personal.
52. Que cualquier persona tiene acceso a sus datos al entrar fácil.
53. Que otra persona puede entrar y hacerse pasar por nosotros.
54. Perder tus datos.
55. Que pueden obtener tu dirección IP y entrar a tu dispositivo.
56. Bueno que cualquier posible hackeo a nuestro dispositivo, al tener todo automático se llevarán nuestra información.
57. Que pueden ser hackeados.
58. Pueden entrar directamente a todos los programas sin tener que iniciar sesión.
59. Que otra persona pueda obtener tu clave.
60. Ningún riesgo hasta ahora.
61. Que me pueden hackear las redes sociales.
62. Me pueden robar la cuenta y usarla con malas intenciones.
63. Que otras personas puedan acceder a ellas.
64. Puede ser, que otros usuarios o hasta la misma persona que ha creado la plataforma o página, acceda a tu cuenta.
65. Que si te llega a difundir mi cuenta principal van a saber mis otras contraseñas.
66. Estamos expuestos a otros dispositivos y con ello a las alteraciones de contenido.
67. Pueden ser utilizadas por otras personas.
68. Que a veces se pueden perder.
69. Prácticamente las contraseñas no son seguras, y si las guardamos en el navegador, es posible que, si somos víctimas de bloqueo, nos pueden robar la contraseña.
70. Los riesgos son de que si se entran a ver en tu dispositivo de forma física o virtual pueden ver nuestros datos igualmente.
71. Es más vulnerable ya que están almacenadas.
72. Pueden acceder más fácil a tu cuenta y entrar fácilmente a tus informaciones.
73. Tu información puede ser robada fácilmente.
74. Que puede tomar acceso directo, y que cualquier cosa que pase en la cual necesite tu ayuda puede que no estés disponible y eso no es seguro.
75. Son fáciles de descifrar y da más riesgo a acceder a tu cuenta.

5. ¿Cuáles son los recursos o medios tecnológicos para la comunicación en las clases del Centro Educativo?

1. La plataforma, WhatsApp y Gmail.
2. WhatsApp, Plataforma MMZ y Telegram.
3. WhatsApp, Plataforma de clases del centro y Telegram.
4. La plataforma en Moodle y grupos de WhatsApp.
5. Milaulas, Zoom, WhatsApp, Telegram y Google Meet.
6. Los recursos tecnológicos son los teléfonos móviles, laptops y acceso a internet.
7. Virtual: Classrooom, Plataforma de milaulas, videoconferencias por Zoom y Google Meet. Presencial: Pantallas, internet y computadoras.
8. Pmmz.milaulas.com y classroom.
9. WhatsApp, Google Meet, Google Classroom y Zoom.
10. Las pantallas digitales, el internet y las laptops.
11. Teléfono, laptop, pmmz.milaulas.com y classroom.
12. Plataforma del centro, classroom y Zoom.
13. La computadora, WhatsApp, classroom, entre otros.

14. La plataforma de la institución y los dispositivos pueden ser un Smartphone o laptop.
15. La plataforma, unos de los medios tecnológicos para entrar a la plataforma es un celular o una computadora.
16. Computadora, teléfonos, classroom y WhatsApp.
17. Por los grupos de WhatsApp.
18. Laptops, pantalla digital, wifi y plataforma del politécnico.
19. Recursos: plataforma, WhatsApp, wifi, pantalla táctil, computadora y teléfono.
20. Una plataforma, WhatsApp, correo, entre otros.
21. WhatsApp y telegram.
22. PMMZ esa es la plataforma que utilizamos.
23. Las laptops del gobierno.
24. Classroom, grupo de WhatsApp y la plataforma.
25. Computadores, teléfonos, (correos electrónicos / WhatsApp, Telegram).
26. WhatsApp, Telegram y Discord.
27. WhatsApp, Telegram, Zoom y Google Meet.
28. Que son más fáciles de hackear.
29. Las computadoras, tables.
30. Computadora.
31. Laptops, pantallas táctiles.
32. Nuestras máquinas de trabajo, cuales son: Laptop.
33. Las computadoras, las pizarras electrónicas y las tablets.
34. Depende del centro educativo.
35. WhatsApp.
36. Pantallas táctiles, Laptops.
37. Pantallas táctiles, Laptops.
38. Documentos, plataforma, links, computadoras y pantallas digitales.
39. Celular y computadora.
40. Laptops o teléfonos.
41. Computadora y pantalla digital.
42. Pantalla digital y computadoras.
43. Los medios comunicativos son zoom, Google Meet, Pantalla Digital.
44. Pantalla digital y computadoras.
45. Zoom, la plataforma PMMZ, Pantalla digital y las computadoras.
46. Computadoras y pantallas digitales.
47. Para las clases utilizamos medios como la computadora, la pizarra inteligente, y entre los recursos, usamos editores de código, programas de ofimática, gestores de base de datos y editores de reporte.
48. Zoom, Google Meet, Moodle, Pantalla Digital.
49. Computadora y pantalla digital.
50. Pantalla digital.
51. WhatsApp, plataforma y classroom.
52. Plataforma de clase, WhatsApp.
53. Los recursos WhatsApp, la plataforma del centro y dispositivos como la PC del gobierno.
54. Correo, Página Web y Grupos de WhatsApp.
55. WhatsApp.
56. Google Classroom, Grupos de WhatsApp y Zoom.
57. Una plataforma y un grupo del WhatsApp.

58. Plataformas y grupos.
59. Classroom, Milaulas y WhatsApp.
60. Laptop, pantalla digital, internet y USB.
61. Pantalla y Laptop.
62. Plataforma Moodle.
63. La pizarra digital, las laptops.
64. Por la computadora o teléfono y una plataforma.
65. La plataforma del centro.
66. Pantalla digital y laptops.
67. Clasroom, Zoom, Google Meet y milaulas.
68. Las computadoras.
69. Celular y computadoras.
70. Teléfono, computador, grupos de WhatsApp y plataformas.
71. Plataforma PMMZ6 y WhatsApp.
72. WhatsApp y una plataforma online.
73. Por la plataforma y WhatsApp.
74. Telegram, página web en mil aulas y WhatsApp.
75. Celular, la computadora y la página del centro.

6. ¿Cuáles serían las principales implicaciones al conectarse a redes Wifi de acceso libre al emplear internet?

1. Acceden a tu teléfono fácil y puede traer riesgos por entrar en redes abiertas.
2. Podríamos ser vulnerables a cualquier ataque, nuestra dirección IP puede quedar guardada y en algún momento atacarnos.
3. A la hora en que nos conectamos a las redes wifi de libre acceso y esto permite a esa persona obtener nuestra información y usarla para cosas ilegales.
4. Te roben tu información o intersecten tu dispositivo.
5. Vulnerabilidad y robo de datos.
6. Las principales implicaciones serían: La vulnerabilidad de nuestros datos y el acceso que tiene un tercero al conectarse a la misma red.
7. Una de las consecuencias sería que si alguien se conecta a una red no segura puede que un usuario desconocido pueda ver sus datos, entre otras cosas.
8. Al acceder a una red de acceso libre, es posible que nos roben nuestra información porque no hay ningún tipo de seguridad.
9. No tienen seguridad por lo que son vulnerables.
10. Una es que los datos ingresados en un navegador, aplicación o página Web, se quedan guardados en la red y es muy posible que una persona con conocimientos en el tema, robe esa información.
11. Que pueden hackear tu celular por medio de la red.
12. Una implicación seria que te roben tus datos o información personal.
13. Que la gente te pueda robar tu wifi.
14. El dueño sabe tu ubicación e incluso puede hackear tu teléfono.
15. Que el dueño de la red pueda ver informaciones de nuestro teléfono.
16. Al conectar a una red libre estás vulnerable a que te rastren y sepan tu ubicación.
17. Pueden ver tu dirección IP y pueden ver todo lo que haces en tu dispositivo.
18. Se pueden rastrear o mandar un virus a su teléfono.
19. Pueden rastrear mi dirección IP.
20. Pueden tener el IP, mandar virus y pueden rastrearte.
21. Se pueden filtrar datos personales.

22. Se pueden dar casos que cuando te conectas a la red, te pueden rastrear el teléfono y también se te pueden dar casos que te avise tu antivirus.
23. Se pone lenta, a veces no funciona.
24. Qué pueden acceder hackers si son los dueños de la red abierta y dañarte tus cuentas entrándole virus y demás cosas.
25. Que la información está expuesta a hackers.
26. Carga muy lento los sitios web.
27. Pues podrían tomar la IP de mi dispositivo y podrías hacer cosas como; robar información como manipular mi dispositivo.
28. Que la seguridad es casi nula, alta probabilidad que no sea regulada.
29. Corres el riesgo de que tus datos sean interceptados.
30. Que puedan interceptar tu flujo de datos y ven tus cosas personales e importantes.
31. Robo de datos.
32. Que puede que esa red sea un fantasma y puedes ser hackeado.
33. Robo de información.
34. Que te pueden hackear y obtener tu información.
35. Te vas público hasta este proveedor.
36. Contraer alguna información que tenga procedencia anónima y esta esté programada para dañar tus sistemas.
37. Darles acceso a ciertos datos al dueño de la red.
38. Estaríamos más expuestos a ataques cibernéticos y/o robo de información.
39. Pueden acceder a tu información personal o información que tengas en el dispositivo móvil.
40. La primera implicación es que su calidad es horrible y es muy insegura y a veces ni se conectan.
41. Pues se podría decir que una red muy lenta ya que estaría sobrecargada.
42. Internet lento, virus y ver información privada.
43. El internet cuando te llegan muchos mensajes seguidos se pone más lento el internet.
44. Entrar virus y poner el wifi lento.
45. 1) El internet se pone más lento, 2) Robo de información, 3) Pasar virus.
46. Virus y se pone lento el internet.
47. Robo de información y virus.
48. Hackear, robar información, virus, entre otros.
49. Pueden publicar datos de nosotros o acceder a nuestras cuentas.
50. Se pone lento o puede pasar virus.
51. Que pueden robar tu información a través de esa red.
52. Muchas personas conectadas se pueden poner muy lento, puede provocar virus.
53. Robarte los datos.
54. Que pueden hackear tu programa.
55. Que nos puede hackear por ser una red clandestina.
56. Pueden tener acceso a nuestro dispositivo sin nuestro permiso.
57. Un virus.
58. La señal.
59. Puede filtrar tu información personal y publicarlo.
60. Puede filtrarse contenido personal.
61. No es una red segura, pueden acceder a tu aparato y ubicarte.
62. Acceder a tu privacidad.
63. Que en caso de no tener un VPN podrían estar interesados en mi información.

64. Te puede hackear el teléfono y recoger información personal.
65. Las principales implicaciones serían el riesgo de documentos.
66. Que no sea segura.
67. Te podría robar información.
68. Pueden ver tus datos.
69. La vulnerabilidad y la privacidad.
70. Puedes tener riesgo de acceder a una red libre, porque pueden acceder a tu teléfono por un descuido.
71. El dueño de la red puede acceder a tu información y usarla a su beneficio.
72. Uno al conectarse a una red libre uno es vulnerable a que nos roben nuestra información.

7. ¿Cómo identificas que la información de la red es verdadera o válida para la comunicación, colaboración, filtrado de contenidos digitales y publicaciones científicas?

1. Investigando en varias fuentes y verificar que sean de confianza.
2. Se puede identificar si entramos a varios sitios y esta la misma información o si personas de confianza comparten la información de esa página.
3. Seguir indagando para verificar que sea verdadera la información, buscar las páginas seguras educativas que sean populares.
4. Revisar en varios lugares. Los PDF son más confiables.
5. Nunca tomar lo primero que veamos, sino seguir investigando en diferentes lugares y comparar la información, si la mayoría concuerda la información es más creíble. Todo esto en páginas confiables.
6. La información a través de la red es válida ya que se utiliza como herramienta esencial para la comunicación, proyectos digitales y aporta bastante a lo que es la educación y se considera efectivo.
7. Para identificar una información en la red hay que ver quién lo publicó, donde lo hizo e indagar en otras páginas a ver si es verídica la información que proporciona el sujeto.
8. Si están citados por otro sitio con información confiable, puede ser verdadera y cierta, en cambio, si está con puntos inentendibles, faltas ortográficas o algo por el estilo, puede no ser cierta del todo.
9. Saber investigar donde puedas ver muchas personas comentando que la información es verídica.
10. En redes sociales podemos identificarlo por el tiempo de publicaciones u otras cosas.
11. Investigando a profundidad la información para verificar si es válida.
12. Buscando en las cuentas oficiales y las páginas oficiales del desarrollador.
13. Investigando entre personas y páginas o buscando los datos necesarios.
14. Investigando entre varias personas o páginas hasta que las informaciones sean las mismas.
15. Buscando la información en varios sitios web.
16. Verificando e investigando.
17. Leyendo el contenido o seguir investigando.
18. Mediante links o contraseñas pasadas por los administradores.
19. Primero se busca que sea una página reconocida y luego se verifican en otras páginas.

20. Si tiene seguridad, ejemplo si es un Facebook y alguien me escribe y entró a su perfil y me doy cuenta si con las fotos es verdadero o que tiempo tiene ese perfil.
21. No existe forma de que sea 100% veraz pero la forma más factible es revisar el dominio.
22. A pesar de no poder verificarse al 100%, indicios de fiabilidad son: El certificado, si contiene fuentes y el URL.
23. Si contiene citas, pero dentro de lo que cabe no se quede.
24. Investigando en diferentes lugares (web).
25. Viendo que su dirección sea segura.
26. Investigando en ambos lugares.
27. Aunque no hay una manera exacta, pueden certificarlos con varias fuentes distintas y viendo si los links terminan en .edu.
28. Siempre visito páginas verificadas ya que en su parte superior derecha tienen un verificador el cual nos dice si es segura o no.
29. Investigando en varias fuentes, y determinando la veracidad a través de este.
30. Comparó las informaciones con las de otras páginas webs, y si coinciden, es señal indirecta de que esa información es verídica.
31. Usar plataformas o páginas verificadas por el navegador.
32. Es recomendable usar plataformas verificadas por el navegador y que sean de fuentes confiables.
33. Por sus fuentes de origen o, mejor dicho, del autor de ella.
34. Cuando la página es segura y no tiene algún virus.
35. No tengo conocimiento.
36. Nos salen alertas.
37. Investigar en redes.
38. Mayormente investigo en diferentes sitios web y depende lo que encuentro le doy su utilidad.
39. Alertas.
40. Investigando en otras redes e informaciones.
41. Bueno cuando se ve que la plataforma es segura.
42. Investigar para ver si es seguro.
43. Cuando son páginas verificadas.
44. No siempre las informaciones son ciertas.
45. No sé.
46. Cuando no me presenta problemas al momento de abrir alguna página web.
47. Si son fuentes confiables.
48. Se puede identificar viendo los logos, la URL y sus certificados.
49. Mirando e investigando.
50. Buscando más y así poder confirmar esa información.
51. Cuando me sale que la página es segura.
52. Depende del uso.
53. Se puede saber en lugares confiables, como haciendo múltiples investigaciones.
54. Investigando sobre eso.
55. A través de investigaciones.
56. Si tiene WPA2, si la red está abierta, si ella tiene HTTPS y buscando en muchos sitios.
57. Vamos a fuentes cercanas y confirmamos si la comunicación es verdadera o falsa.
58. Bueno para saber si la información es verdadera o falsa debemos busca en varios sitios web para así saber.
59. Mediante la investigación sobre si es verídico o no.

60. Investigando más a fondo sobre el tema a tratar.

8. ¿Qué mecanismos utilizas para cambiar la contraseña de tus cuentas personales y de servicios en línea?

1. Cambio mi contraseña mensual y le pongo autenticación en dos pasos para ser más seguro.
2. Usar puntos, letras, mayúsculas, minúsculas y signos, también cambiar la contraseña cada cierto tiempo.
3. Puedo hacer un cambio cada seis meses y no utilizar nada relacionado conmigo.
4. Números, mayúsculas y cosas poco relacionadas una con otra.
5. Símbolos, letras, números y uso de mayúsculas, además cambiarlo cada 3 meses.
6. Cambio de contraseña cada 3 o 5 meses o cuando suceda algo inesperado y necesite cambiarla.
7. Utilizo tanto mi móvil como mi laptop para cambiar contraseñas de cuentas personales, entre otras cosas, también entro a mi cuenta, elijo cambiar mi contraseña, escribe la actual, la nueva y listo.
8. Antes de cambiar una contraseña debemos confirmar nuestra identidad, ya sea vía telefónica, correo u otra información.
9. Para cambiar la contraseña de una cuenta personal tenemos que entrar a: configuración, seguridad y contraseña.
10. Poner la contraseña anterior para confirmar y luego poner la nueva y repetirla.
11. A través de su configuración de privacidad, y en contraseñas para su posterior cambio.
12. Cambiar los datos mediante celular o computadora.
13. Poner la contraseña que tenía y luego aplicar la nueva contraseña.
14. Uso diferentes contraseñas en cada una de las redes, las reviso semanalmente para ver si están correctas.
15. Yo entro a Google, busco y administro mi cuenta y busco el apartado de seguridad, en esta parte me da la opción para cambiar la contraseña.
16. Siempre uso la misma pero la cambio a veces.
17. Solo cuando se la paso una cuenta a un familiar, la cambio en el momento.
18. Utilizo la misma contraseña, reviso mensual mi cuenta y reviso los dispositivos a los que mi cuenta está conectada.
19. Por ejemplo: yo entro a mi perfil de google y entro a cuenta y después a configuración, después dice contraseña y la cambio.
20. Aplicaciones seguras y buenas.
21. Yo la cambió de vez en cuando.
22. Cada 3-4 meses la cambio, directamente desde la app.
23. Cuando google no advierte que mi contraseña está en peligro, google envía una solicitud para cambiar mi contraseña rápido.
24. El apartado de seguridad de google y pensar en una contraseña más segura.
25. Entrando a mi cuenta con la contraseña anterior y luego la cambio.
26. No cambio de contraseñas.
27. Cambiar la configuración de privacidad.
28. Pues… voy a la configuración del sitio y la cambio.
29. Contraseña de respaldo, código de verificación.
30. Contraseña o, mejor dicho, código de recuperación.
31. Código de verificación.
32. No utilizo ningún mecanismo, directamente utilizo la misma contraseña (aunque no es lo recomendado).

33. Busco algo que solo yo conozca no muy aleatorio, pero tampoco tan personal.
34. Los que me dé el servicio.
35. Si deseo cambiar mi contraseña, utilizo el correo electrónico usado en esa cuenta. Para cambiarla.
36. Pido un cambio de contraseña y me mandan un correo y puedo acceder a un link para cambiarla.
37. Solicitando un cambio de contraseña, para que me llegue una nueva.
38. Si yo cambio la contraseña.
39. No utilizar mis datos a la hora de elaborar mi clave, la cambio cada año.
40. No tengo conocimiento.
41. Poner la contraseña actual y la contraseña que quieras.
42. Por medio del correo electrónico.
43. Bueno acceder a mis cuentas y desde ahí se pueden cambiar.
44. Un patrón de caracteres especializados y cada mes.
45. Ocultar el perfil.
46. En el perfil de la persona con la configuración.
47. Yo uso Google Chrome.
48. Cuenta de Google.
49. Editando el perfil, en la configuración.
50. Entrar a configuración e ir a seguridad.
51. Ir al sitio donde quiero cambiarla.
52. Las opciones presentadas.
53. La técnica que utilizo es no vincular datos personales y también mezclando caracteres como letras, números y signos.
54. En caso de un inicio de sesión extraño.
55. Utilizando más de 8 caracteres, que tenga símbolos, números y usando mayúsculas.
56. Cambiar y verificar constantemente.
57. Siempre la estoy cambiando constantemente y la ingreso sin ninguna relación sobre mí.
58. Usar contraseñas largas y con símbolos, números y letras.
59. Yo utilizo diferentes características y no la relaciono conmigo.

9. ¿Cómo identificas las posibilidades de bullyng, sexting escolar o ciberbullyng al establecer comunicación con desconocidos a través de la web?

1. Cuando le hacen una burla a una persona, crean un meme de cierta persona.
2. Acosos a personas en páginas anónimas y la propagación de información de una persona.
3. Es difícil a primera vista identificar a una persona que quiera hacernos algún mal, así que hay que prestar atención a los mensajes.
4. Las personalidades, piden fotos y videos.
5. En este tiempo la tecnología está muy avanzada y muchas personas tienen acceso a la web, lo cual, conlleva muchos usuarios de poca edad que están vulnerables a ciberbullying.
6. Las posibilidades de que ocurran estos acontecimientos son muchas siempre y cuando exista una comunicación a través de la red con algún desconocido.
7. En la forma en que los demás se expresan, ahí te puedes dar cuenta si es posible que te hagan bullyng o sexting escolar.
8. El hacer esos tipos de bullyng, yo lo veo muy mal porque no comprendo cuáles son sus motivos para eso.

9. No hablar con desconocidos y saber con quién te está hablando.
10. Si el atacante elimina los mensajes, publicaciones solo después de que un número establecido de personas lo vean, teniendo contenido que afecte a otro en un centro educativo, es signo de bullyng.
11. Pienso que está mal aparte de que ya es un delito hacer bullyng mediante la web.
12. Se investigó bien sobre el número o nombre para no dar tus datos sin conocer realmente con quien hablas a través de la red y preguntarle en persona si conoce ese número o nombre.
13. Buscando información sobre ese tema en otras fuentes.
14. Si desde un principio notas conductas agresivas de esa persona, es una forma de identificarlo.
15. Si te envías una foto, buscarla en Google Imágenes, si te sale la foto significa que es falsa.
16. Si conocemos a alguien por las redes como Facebook o Instagram que está siendo burlas.
17. Por cómo te habla esa persona.
18. Creando cuentas falsas por una red social y le mandan mensajes.
19. Cuando veo que sufre de daño físico y verbal.
20. Con las personas que se crean cuentas falsas y se hacen pasar por otras personas.
21. Se pueden dar casos que a los que le hacen bullyng, por ejemplo: yo me creo una cuenta falsa con cualquier nombre y por una aplicación puedo hacerle bullyng a una persona.
22. No burlarse y hacer bien con los demás.
23. Pues, cuando le envías algo prometedor a alguien independientemente de ser conocido o no, si lo haces es probable que pasen similitudes.
24. Cuando recientemente conoces una persona y es como grosera al principio, no se ve que es buena gente.
25. Por su comportamiento e intenciones.
26. Cuando hay una burla.
27. Cuándo se mandan fotos e informaciones no correspondientes.
28. Al ver que se está hablando de cosas personales.
29. Muy mal.
30. Dependiendo de las actitudes de la persona, no hablo con extraños.
31. Por medio de comentarios despectivos.
32. Viendo sus comportamientos a otros.
33. Las posibilidades son pocas ya que no conozco muchas personas que hayan sufrido estas cosas.
34. Positivos.
35. Algo pasado.
36. Hay muchas maneras de identificarlos
37. Muy presente ya que hoy día cualquiera te insulta y te ofende a través de diferentes redes.
38. Cuando una persona acosa a otra de manera injustificada.
39. En realidad, pienso que las posibilidades no son tan altos, pero en caso de estar frente a una de estas situaciones, solo es necesario bloquear a ese usuario.
40. En la forma que escribe, en la forma que se expresa y ver si la persona se siente cómoda en ese ambiente web.
41. 100% nadie conoce quien está detrás de una pantalla y las intenciones que tienen.
42. Pues de una manera expresiva.

43. A través de la comunicación con la otra persona.
44. Lo identifico como falta de madurez.
45. Buscando en Safari.
46. Cuando esta no tiene la información necesaria.
47. Buscando en internet.
48. Buscando en las redes.
49. Con una persona que su cuenta no tengo una foto o una persona muy misteriosa.
50. Cuentas falsas o en las que se hacen pasar por otras personas.
51. Cuando aceptas personas desconocidas quedas expuesta.
52. No tengo conocimiento
53. Te acosas verbalmente.
54. Cuando se presentan amenazas y agresiones emocionales psicológicos y físicas.
55. A través de cómo nos hablan.
56. Viendo cómo cambia algunos de los caracteres de los niños.
57. Algunos hacen bullyng a través de la llamada.
58. Cuando esa persona desconocida tiene plan de amenaza o hace que uno tenga temor.
59. En situaciones donde no me lleve bien con otra persona.
60. Como cuando alguien se burla de alguien más ya sea si es feo, sordo o flaco, también cuando se manda fotos y videos a través de alguna red y a un desconocido, pueden venir las burlas.
61. Lo identifico al anotar ya el acoso constante de palabras obscenas de una hacia otra persona.
62. Si la persona está siendo, amenazadora, insultado, entre otras cosas.
63. Cuando una persona tiene problemas.
64. La forma de hablar me puede dar cuenta quién eres y qué quieres.
65. Pues podemos saberlo al poner atención a lo que la persona con la que estamos hablando, nos dice en la conversación.
66. Muy mal, ya que existe una ley de delitos informáticos.
67. Analizando la situación y viendo si es real la persona.
68. Lo veo mal porque de ninguna forma nadie debe hacerle bullyng a nadie.
69. Eso lo veo muy mal porque el bullyng no es lo correcto.
70. Que no tenga información sobre la persona detrás de la cuenta.
71. Cuando en grupo empiezan a burlarse una persona.

10. ¿Qué tipo de apoyo ha recibido de su familia para cumplir con las actividades escolares en línea y cuales actividades haz recibido en la plataforma virtual como complemento en tus clases?

1. Mucho apoyo, ya que cuando se me pasa la hora me despertaban. Me compraban todo lo necesario, me preguntaban si había hecho la clase y también cuando me estresaba me decían que descanse un poco y que siga porque yo puedo.
2. Al principio en mi casa no había internet fijo, luego se puso internet fijo, entre muchas otras cosas.
3. Mucho, se encargaron de que tenga los dispositivos y los servicios como el internet para las clases.
4. Apoyaron con el cambio de internet.
5. Los apoyos de mi familia: me compraron un pc para estudiar. Actividades de plataforma virtual, foros, glosarios, mapas conceptuales, esquemas, manualidades y contenido audio-visual.

6. He recibido mucho apoyo de mi familia y como completo para mejorar la navegación en mis investigaciones es la conexión a internet.
7. Mi madre me ha brindado todo el apoyo posible. En cuanto a la plataforma, he recibido foros, tareas y demás por parte de los maestros.
8. Mi familia ha recibido apoyo con recursos electrónicos por parte del centro educativo. He tenido diversas clases en una plataforma virtual. El apoyo a mí fue grande y lo suficiente para seguir adelante.
9. El apoyo que he recibido es apoyo material y ayudas con mis tareas y asignaciones.
10. Mucha ayuda gracias a Dios.
11. He recibido celular, computadora, uniforme y wifi.
12. Me han ayudado bastante y estoy conforme con eso. Unas de las clases esenciales para mí por la plataforma han sido las clases de análisis y diseño de portales web y recursos multimedia.
13. Mis padres me han apoyado mucho, me han dado todo lo necesario para seguir en esta área. Hemos revivido algunas actividades, no sé cómo dar ejemplos.
14. En caso de las labores virtuales me ayudaron en la computadora y en clase presencias, me ayudan en los materiales para hace la tarea.
15. Me han apoyado dándome los recursos como el internet, celular y laptop.
16. Cuando mis papas me dicen que muestre la plataforma cuando no tengo equipo para estudiar, mi papa hace el esfuerzo de comprar una.
17. Me apoyaron con su tiempo y me compraron lo que me hacía falta, me revisan si tengo tareas.
18. Mi familia me apoyo siempre ayudándome en lo que podían, se me dañaba la laptop, me la mandaban a arreglas de inmediato.
19. Mi madre me regalo un teléfono por buena conducta.
20. Comprándome una PC y siempre preguntándome por lo que he hecho.
21. Mi padre me ayudaba mucho, me llevaba a los centros de internet.
22. Poniendo internet en la casa me han ayudado.
23. Mi familia siempre ha estado al pendiente de que, si entro a clase, o si hago mis tareas.
24. Mi papá me leva y me recoge de la escuela, me ayuda en lo que no entiendo y demás.
25. Me ha apoyado en temas muy difíciles.
26. Mi familia me brindo mucho apoyo positivo.
27. Colocar internet en la casa.
28. En todos los sentidos he recibido apoyo.
29. Financiamiento.
30. Apoyo, emocional y económico.
31. De mis padres, el internet y comprensión.
32. Mis padres me facilitan sus equipos tecnológicos.
33. Mucho apoyo, y las clases virtuales son muy difíciles.
34. Computadora.
35. Ninguna ayuda, no sé.
36. Me han apoyado mucho animándome a seguir y ayudándome a comprender, la escuela proporciona el material para estudiar.
37. Preguntándome cómo van, y en la plataforma he hecho foros.
38. Me han recordado que tenía que coger clases en esos días.
39. Apoyo moral porque me motivaron a seguir con las clases virtuales.

40. He recibido un muy buen apoyo de parte de mi familia me animaros mucho y me motivaron a seguir.
41. Pues recibo apoyo tecnológico y en la clase recibo implementaciones.
42. Me decían que me conectara. Videos y documentas.
43. Me apoyan en los estudios y comprándome útiles escolares, y en la escuela recibimos videos, tareas, etc.
44. Videos y tareas, el apoyo fue que me pusieron wifi.
45. Se suben archivos, documentos, etc. Mis padres pusieron el internet con más megas.
46. En verdad nunca me ha hecho falta el apoyo familiar, ya que gracias a Dios he recibido todo el posible internet e información.
47. Activar internet y archivos videos Archivos, tareas, videos y links, pagar internet rápido.
48. Documentos, links, videos e internet en mi casa.
49. En todos los sentidos en recibido todo el apoyo que necesito.
50. Videos, suben documentos, el acceso a internet.
51. Apoyo familiar, ya que siempre mi familia está pendiente de mí.
52. Plataforma, clases por Zoom, Classroom. Mi familia me ayuda apoyándome.
53. Todo tipo de apoyo posible.
54. Mucho apoyo, pero el económico.
55. Apoyo seguro.
56. Han estado muy activos ayudándome en todo.
57. Recibí mejor equipo para las clases.
58. Internet y útiles escolares.
59. Me ayudaron con recursos como internet, computadoras y celular.
60. Porque ellos me apoyan con lo que me asusta y eso me da interés de seguir adelante y seguir haciendo lo que me gusta, aún no he realizado actividades en la clase virtual.
61. He recibido el apoyo familiar teniendo en cuenta la instalación de Wifi.
62. En mi casa si cambio el internet a una mayor velocidad.
63. Poner internet en mi casa.
64. Las computadoras, y las informaciones presentadas.
65. Diría que completamente, porque siempre se preocupan por mí.
66. Muchísima ayuda con las clases. Compra de utilidades.
67. He recibido apoyo de internet, a través de la plataforma he recibido diapositivas y cuestionarios.
68. Me ayudan en todos los proyectos y foros.
69. Si he recibido apoyo porque siempre están conmigo en todo momento.
70. Apoyo monetario y emocional. Foros, investigaciones, PDF, exámenes, diapositivas multimedia.
71. El apoyo que recibo es la compra de los utensilios.
72. El apoyo que he recibido es económico.
73. Mis padres me ayudan en los proyectos y me llevan donde amigos para hacer las tareas.

Respuestas de la aplicación de instrumentos de evaluación

Profesores

1. ¿De qué manera identifican los recursos tecnológicos o sitios seguros para navegar en internet e instalar en sus dispositivos electrónicos?
1. De la fuente de procedencia. 2. Las medidas que tomo en cuenta es informarme bien para luego proceder, ya que cuando la página no es segura te insisten mucho o no tienen conocimiento sobre lo que ofrecen. 3. Http 4. Depende de la fuente de donde salgan los recursos. 5. El antivirus. 6. Identifico esos sitios cuando hay muchos anuncios o enlaces que llevan a otra página, de igual modo trato de usar recursos de fuentes de instituciones reconocidas. 7. Por medio de los buscadores y capacitaciones de ministerio de educación. 8. Si proceden de fuentes desconocidas por su confiabilidad, si proceden de un sitio seguro. 9. – Su creador - La cantidad de usuarios que lo utilizan. - La política de manejarse. 10. Eficiente 11. Hoy en día hay varias maneras para identificar un sitio web seguro, tales como: las páginas seguras tienen un candado identificador, además inician con https. Otra manera es a través del navegador que nos identifica si el sitio es seguro. 12. Verificando que al principio de la URL tenga un candadito. 13. - Ubicando un candado que se muestra al principio de la URL. - Información o no segura (circulo). - No seguro o peligro (triangulo). 14. Los sugeridos por los profesores de informática. Los diversos programas para uso y manejo de los participantes.
2. ¿Cuáles serían las implicaciones del uso de contraseñas automáticas de sus cuentas en línea?
1. Me pueden sustraer datos e información confidencial. 2. Considero que no es seguro ya que hay más facilidad de que te hackeen tus cuentas y te roben documentos, dinero o cosas personales. 3. Hace mi información insegura. 4. Los estudiantes podrían copiarlas y usarlas. 5. Facilidades y rapidez 6. Si una persona entra a mi pc podría hackear todo los recursos y aplicaciones que tengo sincronizada. 7. Podrían hackear las cuentas, por estar a disposición de los sitios web. 8. – Cualquier usuario puede entrar en dicha cuenta y hacer daño. - Si cambia de equipo y olvida la contraseña hay problemas.

9. – Algunos estudios indican que en torno al 90% de las contraseñas utilizadas son vulnerables, por lo que los ataques más habituales tratan siempre de encontrarlas.
10. Mayor seguridad
11. Trae varias complicaciones, ya que, si préstamos o se nos pierde el equipo, nuestras contraseñas estarían al alcance de cualquier persona.
12. De que alguien pueda ingresar y tomar la clave.
13. Una de ellas es que cualquiera puede usar ese equipo, tomar la contraseña y posteriormente darles un uso indebido.
14. Pueden hacer mal uso de los programas y además es un peligro para la ciberseguridad.

3. ¿Qué tipos de programas antivirus usted utiliza para prevenir los ataques informáticos?

1. Avast
2. Por el momento no estoy utilizando ninguno.
3. No sé su nombre.
4. Avast free.
5. Avast antivirus.
6. No tengo
7. Avast.
8. Conozco varios, pero solo he usado avast.
9. – Antispyware
    - Antimalware
    - Anti Hardware
    - Firewall
10. No lo utilizo
11. Personalmente, ninguno.
12. Mcafee
13. En mi caso uso Windows defender.
14. Avast

4. ¿Cómo identifican y resuelven los problemas técnicos presentados al integrar las tecnologías en el aula?

1. De manera directa y con la colaboración de colegas.
2. Busco ayuda del soporte técnico de la institución.
3. Autogestión.
4. Los maestros de informática están siempre dispuestos a prestar ayuda a cualquier problema con la real.
5. Intentar resolverlo y si no llamo a un experto.
6. Trato de buscar en youtube, alumnos, maestros que sepan del tema.
7. – Auxiliándome de los expertos en el área, así como de estudiantes del centro educativo.
    - Indagándome en internet o con una segunda opción de trabajo.
8. Soy autodidacta, busco información y cuando no puedo, busco ayuda con alguien capacitado.
9. No sé
    - Solucionar.
10. Busco ayuda con mis compañeros

11. Entre los problemas presentados, pueden ser: falta de conexión y PDI dañada. Al ser identificada podemos resolver teniendo descargados los recursos de la computadora, o usando otra aula con PDI.
12. Preguntándole a un técnico o informático del centro.
13. Esto depende del problema que sea, en mi caso soy técnico y lo resuelvo yo mismo, otros recurren a mi u otro compañero.
14. Tenemos tres profesores que nos acompañen en los procesos complejos.

5. ¿Cuáles serían las principales implicaciones que consideran a la hora de conectarse a redes Wifi de acceso libre al emplear internet?

1. Que no son realmente seguras.
2. Si la red es segura.
3. Que alguien entre a mi equipo.
4. Pueden robarte toda tu información.
5. Que sea lento
6. Que podría robar toda mi información.
7. Virus, poca garantía de seguridad.
8. Se puede infectar el equipo, se pone en riesgo la privacidad.
9. La mayor amenaza para la seguridad de las redes Wi-fi gratuitas es la capacidad que tiene el hacker de interponerse entre tú y el punto de conexión.
10. Pueden clonar la cuenta, provocar virus, plagio de documentos.
11. Nuestro equipo queda expuesto a un posible hackeo.
12. No se
13. Intersección de la red y distorsión por parte de los estudiantes.
14. El internet se cae con frecuencia.

6. ¿Qué tipo de tecnologías consideran como empleo pedagógico para la innovación y la calidad educativa en su planeación didáctica?

1. No se
2. – Las pizarras digitales.
   - Las computadoras
   - Celular.
3. - Equipos: pantallas digitales y laptops.
   - Herramientas: internet, redes sociales, plataformas digitales, todas las herramientas de google, programas como Office, Power Point, Word, Drive.
4. Pizarra Digital, el Internet, documentales en inglés, Youtube.
5. Uso obligatorio de plataforma.
6. Todo lo necesario para llevar a cabo el proceso pedagógico como, por ejemplo: youtube, presentaciones, imágenes, entre otros.
7. – Plataformas Moodle
   - Clasroom
   - Power Point
   - Laptop
8. - Uso de plataformas como Moodle, google clasroom, youtube. Otras descargas gratuitas y otras en línea.
9. – Educación online
   - Educación en el móvil
   - Aprendizaje a través de los videos juegos.

10. – Pantalla digital
    - Computadora
    - Mouse
    - Internet
11. La gamificación, ya que nuestros estudiantes aprenden jugando.
12. Computadoras y tabletas.
13. Hay usuarios dentro de estas Moodle, las herramientas de google, entre otras.
14. Videos, WhatsApp y videoconferencias.

7. ¿Cómo identifica que la información de la red es verdadera o válida para la comunicación, colaboración, filtrado de contenidos digitales y publicaciones científicas?

1. Tomando en cuenta la fuente.
2. Me informo en diferentes fuentes, tales como páginas, periódico, tv y radio.
3. Se verifican varias fuentes y el contenido en común es el objetivo.
4. Si, depende de quién publique la información.
5. Uso de fuentes confiables.
6. Sobre todo, que sea página de instituciones y plataformas reconocidas como estar alerta en los PDF y nuevas publicaciones.
7. Siendo consciente de que el portal sea seguro, por historial de comentarios y por uso frecuente.
8. – Puede que la pagina no cite fuentes
    - Que tenga mala redacción y ortografía
    - Los contactos de dichas paginas son falsos.
9. – Precisión
    - Conclusión
    - Navegabilidad y usabilidad
    - Objetividad
    - Propósitos.
10. Observando la barra de dirección.
11. Las redes están llenas de informaciones, pero no todas son verídicas, por lo que debemos siempre prestar atención de donde procesen los contenidos. Ejemplo, si es una noticia, buscar un periódico de renombre y prestar atención a lo que publican.
12. Accediendo a fuentes confiables, entre ellas, revistas indexadas.
13. Pues esto lo hacemos a través de fuentes seguras y sobre todo confiables.
14. Verificando la web donde circulan material o contenido de calidad.

8. ¿Cuáles estrategias tecnológicas utilizan para el desarrollo de las competencias de los alumnos?

1. Conferencias.
2. – Videos educativos
    - Presentaciones
    - Trabajos grupales utilizando la tecnología.
3. Proyección de videos, fichas con audio de Power Point, crear y compartir el contenido conceptual en plataforma y por correo electrónico y enlaces de drive, ejercicios online, ejercicios lúdicos en programas y plataformas digitales.
4. Presento los trabajos con mi computadora dándole las interacciones de cada tarea y se lo proyecto en la pantalla digital.
5. Videos, plataformas, etc.

6. Uso de plataforma como Moodle para asignarles actividad, como la realización de videos.
7. Diapositivas
8. Juegos, dispositivos, documentos de google, plataforma Moodle.
9. Diapositivas
10. - Asignaciones en las plataformas.
    - Búsqueda de información
    - Uso de la tecnología para comprobar resultados
    - Ayuda colaborativa.
11. – Instrucción programada
    - Tutorial
    - Simulación
    - Niveles multimedia
12. Debates, exposiciones, lluvias de ideas, resumen, síntesis, análisis de documentos, dramas, etc.
13. El uso de una plataforma virtual, donde se colocan todos los recursos y las actividades que los estudiantes realizan para el desarrollo de la misma, el uso de herramientas de gamificación.
14. –Prácticas cotidianas, ejercicios en el laboratorio, manejo de diversos programas acompañados por el docente.

9. ¿Cuáles herramientas tecnológicas le permiten la creación y edición de contenidos digitales?

1. - Aplicaciones como Duolingo y Kahoot.
2. paquete de office para Word, Excel, y Power Point.
    - Lenguajes de programación para proyectos.
3. Paint.
    - Zoom
    - Excel
    - Word
4. – Word
    - Descarga
    - Quize
5. Office, Power Point, Word y Excel.
6. – Computadora
    - Pantalla
    - Tablet
    - Celulares
7. Plataforma virtual.
8. Youtube, Power Point, Word, canvas, entre otras.
9. – Word
    - Power Point
10. – Window Movie Marker
    - Filmora
    - Microsoft Office (Word, Excel y power point)
    - Canva
    - Google form
11. – Word
    - Power Point

- Excel
- Youtube.

12. Ardora, kahoot, Hotpotatoes, Xelearning.
13. La computadora y los celulares.
14. Diversas plataformas web, google, WhatsApp.

10. ¿Qué impacto produce la aplicación de herramientas digitales en el aprendizaje del alumno?

1. Mejorar la eficiencia y eficacia.
2. El impacto que produce es que el aprendizaje es más rápido porque aprenden usualmente y luego ponen en práctica.
3. Lo hace más simple, práctico, participativo y atractivo.
4. Un impacto muy positivo para el avance de estos alumnos que van avanzando con la tecnología.
5. Facilidad y comodidad.
6. Un gran impacto positivo ya que, si está bien dirigido se puede lograr el aprendizaje, además los alumnos pueden desarrollar sus competencias tecnológicas tan necesaria en los nuevos retos que espera el futuro.
7. Mantiene su atención y motivación en los procesos.
8. – Se despierta el interés en el alumno con los audiovisuales.
   - Los videos explicativos son recursos para que ellos los observen la cantidad de veces que lo necesiten.
   - Están acorde al tiempo.
9. A través de este sistema, los profesores tienen la oportunidad de agilizar las tareas administrativas.
10. Trabajo más rápido y mejor organización.
11. Es un impacto positivo, ya que los estudiantes muestran mayor interés y el aprendizaje es más significativo.
12. Un impacto positivo porque las clases se hacen más dinámicas, divertidas y fáciles, captan más.
13. Atraer la atención de los mismos y mostrar interés en las clases.
14. -Grandes aprendizajes.
    -habilidades tecnológicas en los estudiantes
    -Destreza
    Conocimientos significativos.

Respuestas de la aplicación de instrumentos de evaluación

Administrativo

1. ¿Cuáles son los riesgos de emplear internet y cómo identificas los recursos tecnológicos seguros para navegar en internet e instalar en los dispositivos electrónicos?
1. Mediante las páginas oficiales encontramos los recursos. Los riesgos son jaqueo, intervención de teléfono, robo de información, ataques cibernéticos, bullying, sexting, distorsión, amenazas, secuestros, etc. 2. Podemos tener riesgo de que otra persona tenga acceso a nuestros datos personales ya sean contraseñas, por lo del hakeo. 3. Que se entren a mi dispositivo. 4. No conozco. 5. El riesgo de implementar internet es el mal uso, y la distracción del trabajo. 6. No sé 7. Riesgo personal y riesgo a la sociedad. 8. Haqueos de cuenta a través de dispositivos electrónicos. 9. No tengo conocimiento. 10. No sé 11. El mal manejo al uso del internet. 12. No sé 13. No sé
2. ¿Qué procedimientos usted utiliza para crear contraseñas seguras?
1. Usando combinaciones de palabras alfabéticas, numéricas, guiños y cambiándola cada cierto tiempo. 2. Creo contraseñas con datos numéricos y letras. 3. Creo contraseñas con datos numéricos y letras. 4. Contraseñas con datos numéricos. 5. Utilizo números, letras mayúsculas y minúsculas, acompañado de signos. 6. Dato personal, numérico y alfabético. 7. Números y letras. 8. Red oculta. 9. No sé 10. Que sea información personal para así no se vea fácil para otros. 11. No sé 12. No sé 13. No sé
3. ¿Conoce usted el procedimiento para manejar sus cuentas personales, documentos o archivos desde cualquier dispositivo electrónico?
1. Conocimiento del manejo de cuentas en línea automática. 2. Regular. 3. Realiza transacciones con cuentas automáticas.

4. No utilizo cuentas en línea, se me dificulta su uso y olvido fácilmente.
5. Si.
6. Para procedimiento de manejar cuentas personales o documentos todo depende de cuál es su uso que voy a hacer. Si tengo que usar internet y guardar documentos o hacer documentos.
7. Si se puede conectar desde cualquier dispositivo.
8. Si utilizo mi cuenta de mi dispositivo.
9. A través de una contraseña personal.
10. No tanto.
11. No sé
12. No sé
13. No sé

4. ¿Cuáles han sido las principales dificultades que el Centro Educativo ha enfrentado para implementar las tecnologías y qué aplicaciones o herramientas resultan más complicadas para llevar a cabo su proceso de enseñanza aprendizaje?

1. La plataforma es Moodle.
2. Estudiantes de bajos recursos sin internet.
3. Estudiantes con poco interés para aprender.
4. Padres irresponsables y que no ayudan a sus hijos a hacer las tareas.
5. Profesores rezagados, cansados y con tecnofobia.
6. Durante el año escolar 2020-2021 las dificultades que tienen los estudiantes es la falta de conocimiento sobre el manejo de las plataformas y los contenidos a trabajar, las complicadas Moodle y teams, el internet es inestable para la cantidad de personas.
7. Dificultades: el año escolar 2020-2021 falta de conocimiento de cero manejos de plataforma Teams y Moodle, estas son las herramientas que dieron dificultades.
8. Poca conectividad y sobrepoblación.
9. Las dificultades principales son: falta de dispositivos, internet y capacitación.
10. La dificultad con el internet, los estudiantes no podían conectarse a internet.
11. La conexión a internet.
12. Problemas con el internet no es muy bueno.
13. El internet no es bueno, los estudiantes no tienen computadoras que le faciliten el proceso, algunos tienen otros no.

5. ¿Cómo considera usted el uso de plataformas virtuales para la docencia presencial, semipresencial y virtual?

1. Permite aprendizaje significativo.
2. Ahorro de tiempo y dinero (aprovechamiento de tiempo).
3. Trabajo en equipo, investigación
4. Dominio tecnológico
5. Es de mucha utilidad para el desarrollo de las actividades que implementan los docentes en el aula. Algunos docentes trabajan la plataforma virtual y otros no le dan el uso adecuado.
6. Muy importante porque pueden ser un complemento a tu clase o ayuda.
7. Considero la modalidad presencial por las razones de que se tienen que esforzar más los alumnos al realizar sus actividades.

8. Me parecen de gran utilidad, porque hace que los estudiantes sean capaces de construir conocimientos e involucrarse activamente en el proceso de enseñanza aprendizaje, y promueve la participación activa.
9. No sé
10. Excelente y muy asertiva.
11. Soy administrativa, no manejo el uso de plataformas.
12. Trabajo con el Sigerd donde se registran todos los estudiantes del centro, los empleados.
13. Un método para facilitar al docente y al estudiante, y a larga distancia pueden trabajar sin necesidad de estar presente físicamente.

6. ¿De qué manera identifica usted los recursos tecnológicos seguros para instalar en su dispositivo electrónico?

1. Verificación de la fuente o páginas oficiales mediante actividades.
2. No tengo conocimiento.
3. No sé
4. No sé
5. Verificar que sean de páginas confiables.
6. No tengo conocimiento.
7. No tengo conocimiento sobre esto.
8. Utilizo un usuario, contraseña y antivirus.
9. No sé
10. No sé
11. No sé
12. No sé
13. No sé

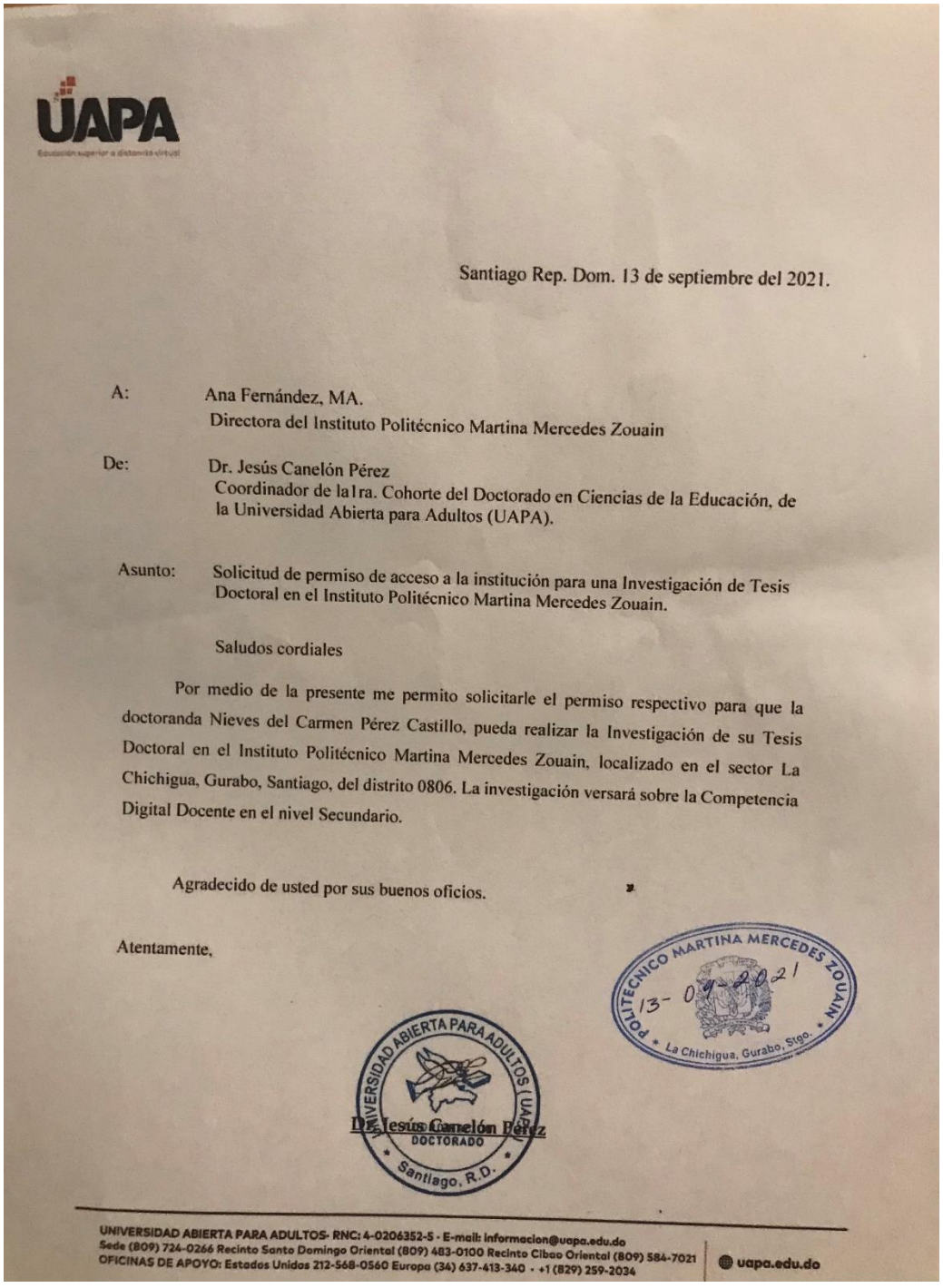
7. ¿Cuáles son las implicaciones del uso de contraseñas automáticas de sus cuentas en línea?

1. Acceso a sus credenciales con facilidad jaqueo, manipulación de dispositivos electrónicos con frecuencia.
2. Violación a mi privacidad.
3. Cualquier persona puede hacer llamadas telefónicas desde mi teléfono. Pueden entrar a mi cuenta o correo electrónico.
4. Pérdida del aparato electrónico.
5. Pérdida de contactos.
6. Pérdidas de las cuentas de correo y otras aplicaciones.
7. Robo de dinero e identidad.
8. Más fácil y rápido para tener acceso a las cuentas, pero mayor riesgo de que terceros puedan violar la privacidad de las mismas.
9. Mi implicación es que pueden ver mi dato personal.
10. Riesgo de perder informaciones confidenciales e identidades.
11. Implica muchos problemas por documentos que no deben salir a otro departamento.
12. Se corre el riesgo de que entre a su cuenta.
13. Que tiene más facilidad para entrar.

8. ¿Qué medidas o elementos estratégicos emplea usted en la institución para el manejo apropiado de las tecnologías de la información, comunicación, conocimiento y aprendizaje digitales es (TICCAD)?
1. Una línea de internet a través de un servidor manejado por una empresa privada con mucha vulnerabilidad de datos o informaciones. 2. Charlas, uso de proyecciones sobre temas a tratar, se realizan actividades como charlas con especialistas en las diferentes áreas. 3. En el departamento de psicología utilizamos proyector y computadora para realizar charlas a los estudiantes y padres. 4. El departamento de coordinación no maneja aparatos electrónicos solo una computadora de escritorio por lo que se trabaja manualmente. 5. Usar contraseñas para cuidar la seguridad de la información. 6. Trabajo como recepción, copiado, teléfono, libro de visitas, libro de firma. 7. Trabajo en el departamento de registro. Trabajo manual utilizo libro de firmas, solicitudes de carta, etc. 8. Computadoras, impresoras y otros. 9. No sé 10. No sé 11. No sé 12. No sé 13. No sé
9. ¿Cuáles son los recursos o medios tecnológicos para la comunicación en las clases del Centro Educativo?
1. - Internet 2. Pantallas digitales (PDI) 3. Plataforma Moodle 4. WhatsApp 5. Llamadas directas, WhatsApp, televisores digitales, internet. 6. – Pantalla digital. 7. Televisión. 8. Internet 9. WhatsApp 10. Teléfono. 11. WhatsApp y llamadas telefónicas, correos electrónicos, blog. 12. Dispositivos móviles, pc. 13. Bocina, computadora, televisión.
10. ¿Cuál es el nivel de integración de la familia en la escuela y qué medios estratégicos tecnológicos utiliza el Centro Educativo para integrar a las familias en la escuela como apoyo para reforzar las conductas inadecuadas y fomentar los valores humanos en los alumnos?
1. - Nivel de integración es muy bajo, poco apoyo por parte de la familia. 2. El medio de WhatsApp, llamadas y Moodle. 3. El centro hace reuniones escuela de padres durante el primer año escolar.

4. El nivel de integración de la familia es inestable ya que algunos padres no asumen su rol. Los padres cuando se convocan a reuniones quizás un 40% asisten.
5. Nivel de integración de la familia es muy pobre, hay muy poca integración de los padres con la escuela.
   Cuando se convocan a las diferentes reuniones los padres no asisten al centro.
   El principal medio es se creó la escuela de padres para integrar a la familia con la escuela.
   También están los comités de padres por curso como otra manera de interacción.
   Sociedad de padres y amigos de la escuela.
6. Por medio de comunicación, documentos escritos o avisos de convocatorias para reuniones, talleres, eventos, apoyo de la familia en el centro educativo es poco no hay mucha integración por parte de los padres.
7. Se trabaja directamente con la sociedad de padres, y las cosas a considerar directamente con el departamento de psicología y orientación.
8. Actos para que los estudiantes tengan conocimiento de la historia dominicana en una reunión familiar.
9. Actos con estudiantes, docentes en la bandera, exposiciones sobre temas de las familias, reuniones de padres y orientadores, etc.
10. No tengo conocimiento.
11. Se forman grupos de WhatsApp con los padres, para estar más comunicados.
12. Regular es la interpretación y el medio vía WhatsApp.
13. Las computadoras o plataformas, celulares, etc.

APÉNDICE J Solicitud de consentimiento



UAPA
Educación superior a distancia virtual

Santiago Rep. Dom. 13 de septiembre del 2021.

A: Ana Fernández, MA.
Directora del Instituto Politécnico Martina Mercedes Zouain

De: Dr. Jesús Canelón Pérez
Coordinador de la1ra. Cohorte del Doctorado en Ciencias de la Educación, de la Universidad Abierta para Adultos (UAPA).

Asunto: Solicitud de permiso de acceso a la institución para una Investigación de Tesis Doctoral en el Instituto Politécnico Martina Mercedes Zouain.

Saludos cordiales

Por medio de la presente me permito solicitarle el permiso respectivo para que la doctoranda Nieves del Carmen Pérez Castillo, pueda realizar la Investigación de su Tesis Doctoral en el Instituto Politécnico Martina Mercedes Zouain, localizado en el sector La Chichigua, Gurabo, Santiago, del distrito 0806. La investigación versará sobre la Competencia Digital Docente en el nivel Secundario.

Agradecido de usted por sus buenos oficios.

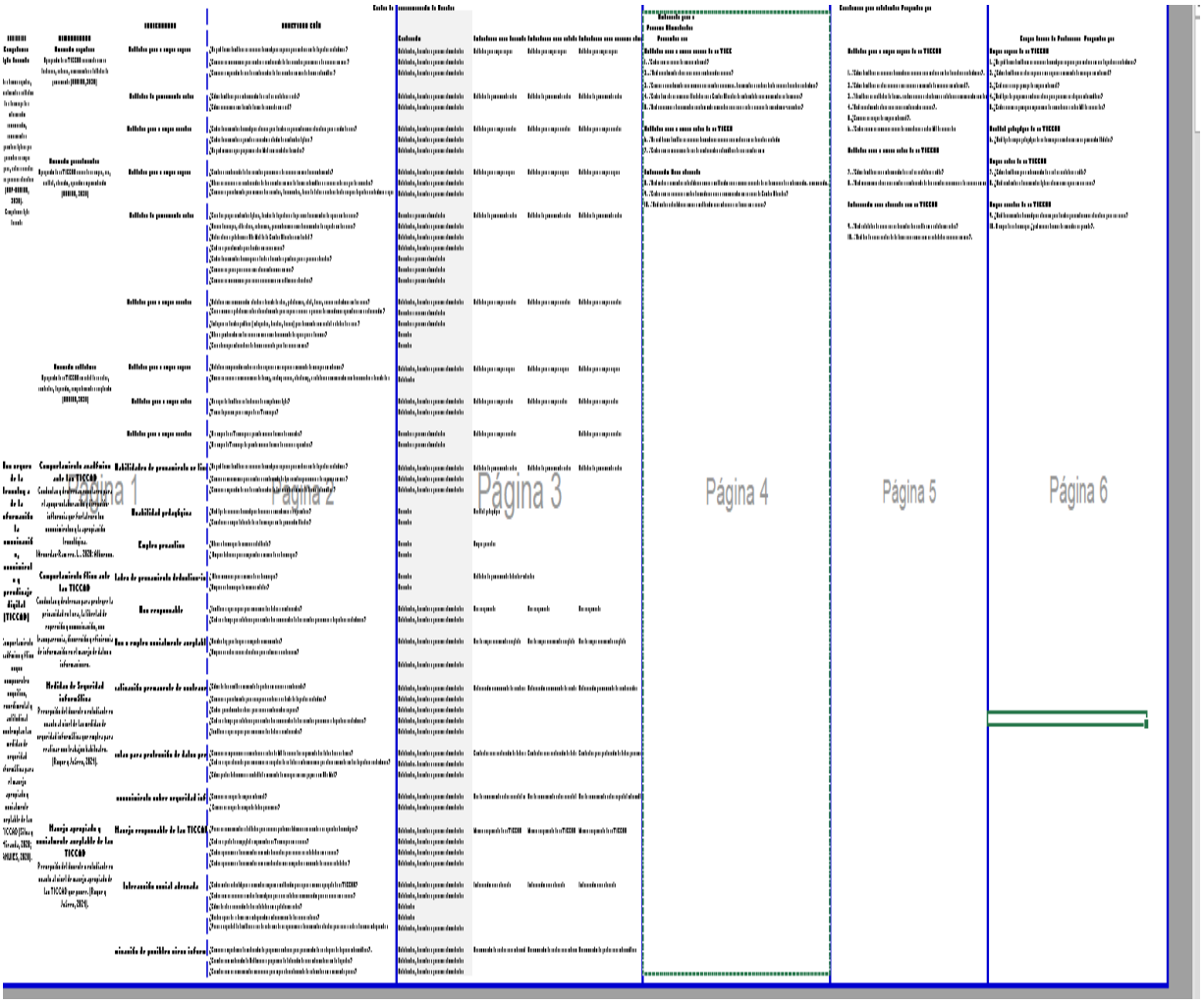
Atentamente,

POLITECNICO MARTINA MERCEDES ZOUAIN
13-09-2021
La Chichigua, Gurabo, Stgo.

UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA)
DOCTORADO
Santiago, R.D.

Dr. Jesús Canelón Pérez

APENDICE K Cuadro de categorías (operacionalización de variables)



VARIABLES	DIMENSIONES	INDICADORES
Competencia digital docente Es el dominio cognitivo, procedimental y actitudinal de la tecnología de la información comunicación, conocimiento y aprendizaje digitales que garantiza su empleo seguro, crítico y creativo de los procesos educativos (SEP-ANUIES, 2020). Competencia digital docente	**Dimensión cognitiva:** Apropiación de las TICCAD relacionada con las destrezas, saberes, conocimientos y habilidades de pensamiento (ANUIES,2020)	**Habilidades para el empleo seguro** **Habilidades de pensamiento crítico** **Habilidades para el empleo creativo**
	Dimensión procedimental: Apropiación de las TICCAD acerca de su empleo, uso, usabilidad, utilización, aplicación e implementación (ANUIES, 2020)	**Habilidades para el empleo seguro** **Habilidades de pensamiento crítico** **Habilidades para el empleo creativo**
	Dimensión actitudinal: Apropiación de las TICCAD en virtud de los actos, conductas, disposición, comportamiento y aceptación (ANUIES,2020)	**Habilidades para el empleo seguro** **Habilidades para el empleo crítico** **Habilidades para el empleo creativo**
Uso seguro de la tecnología de la información la comunicación, conocimiento y aprendizaje digital (TICCAD) Comportamiento académico y ético cuyos componentes cognitivo, procedimental y actitudinal contemplan las medidas de seguridad informática para el manejo apropiado y socialmente aceptable de las TICCAD (Silva y Miranda, 2020; ANUIES, 2020).	**Comportamiento académico ante las TICCAD** Conductas y destrezas escolares para el apoyo-colaboración y dirección-influencia que fortalecen los conocimientos y la apropiación tecnológica. (Arguedas-Ramírez, L., 2020; Albornoz, J., Flores-Oyarzo, G., Contreras, M., & Mujica, A., 2021)	**Habilidades de pensamiento crítico** **Usabilidad pedagógica** **Empleo proactivo**
	Comportamiento ético ante las TICCAD Conductas y destrezas para proteger la privacidad en línea, la libertad de expresión y comunicación, con transparencia, discreción y eficiencia de información en el manejo de datos o informaciones. (Muñoz, J., 2017).	**Habilidades de pensamiento deductivo-inductivo** **Uso responsable** **Uso o empleo socialmente aceptable**
	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. (Roque y Juárez, 2021).	**Actualización permanente de contraseñas.** **Conductas para protección de datos personal** **Nivel de conocimiento sobre seguridad informática**
	Manejo apropiado y socialmente aceptable de las TICCAD Percepción del docente o estudiante en cuanto al nivel de manejo apropiado de las TICCAD que posee. (Roque y Juárez, 2021).	**Manejo responsable de las TICCAD** **Interacción social adecuada** **Discriminación de posibles virus informáticos**

REACTIVOS GUÍA
¿De qué forma identificas los recursos tecnológicos seguros para instalar en tu dispositivo electrónico ?
¿Conoces los mecanismos para cambiar la contraseña de tus cuentas personales y de servicios en línea ?
¿Conoces la implicación del uso de contraseñas de tus cuentas en línea de forma automática ?
¿Cómo identificas que la información de la red es verdadera o valida?
¿Cómo seleccionas una fuente formal de consulta en la red?
¿Cuáles herramientas tecnológicas utilizarias para diseñar las presentaciones atractivas para el salón de clase?
¿Cuáles herramientas le permite la creación y edición de contenidos digitales ?
¿De qué manera logra programar sitios Web con carácter formativo?
¿Cambias la contraseña de tus cuentas personales y de servicios en línea frecuentemente?
¿Utilizas los usuarios y las contraseñas de tus cuentas en línea de forma automática o la colocas cada vez que te conectas?
¿Conoces el procedimiento para manejar tus cuentas, documentos, bases de datos o archivos desde cualquier dispositivo electrónico o lugar que te
¿Crea tus propios contenidos digitales, diseños de diapositivas o blogs como herramientas de apoyo en tus clases?
¿Realizas descargas, edita videos, reflexiones, presentaciones como herramientas de soporte en tus clases?
¿Sabes utilizar la plataforma o Sitio Web de tu Centro Educativo con facilidad ?
¿Cuál es el procedimiento para diseñar un curso masivo?
¿Cuáles herramientas tecnologicas le facilita al docente a planificar para el proceso educativo?
¿Conoces los pasos para crear una videoconferencia en línea?
¿Conoces los mecanismos para crear evaluaciones en softwares educativos?
¿Establece una comunicación efectiva a través de sitios, plataformas, chat, foros, correo electrónico en tus clases?
¿Crea y maneja la plataforma virtual adecuadamente para explicar y evaluar el proceso de enseñanza aprendizaje en la virtualización ?
¿Integras los diseños gráficos (infografías, tarjetas, flayers) para transmitir con claridad el objetivo de la clase ?
¿Utiliza la gamificación en tus clases en línea como herramienta de apoyo para la docencia?
¿Crea videojuegos interactivos de forma correcta para tus clases en línea?
¿Establece comparación entre los sitios seguros y no seguros al momento de navegar en interner?
¿Analiza las causas y consecuencias del bullyng, sexting escolar, ciberbullyng, al establecer comunicación con desconocidos a través de la Web?
¿Es capaz de identificar las destrezas de competencia digital?
¿Tienes disposicion para el empleo de las Tecnologías?
¿Si el empleo de las Tecnologías le permite nuevas formas de enseñar?
¿Si el empleo de Tecnología te permite nuevas formas de evaluar el aprendizaje?
¿De qué forma identificas los recursos tecnológicos seguros para instalar en tu dispositivo electrónico ?
¿Conoce los mecanismos para cambiar la contraseña de tus cuentas personales y de servicios en línea ?
¿Conoces la implicación del uso de contraseñas de tus cuentas en línea de forma automática ?
¿Qué tipo de recursos tecnológicos favorece la enseñanza y el aprendizaje?
¿Consideras el empleo deliberado de las tecnologías en tu planeación didactica?
¿Utilizas la tecnologías de manera autodidacta?
¿ Empleas tutoriales para comprender el manejo de las tecnologías?
¿ Utilizas manuales para el manejo de las tecnologías?
¿Empleas las tecnologías de manera intuitiva?
¿identificas el lugar seguro para almacenar tus datos y contraseñas?
¿Cuál es el tiempo que estableces para cambiar tus conraseñas de tus cuentas personales y dispositivos electrónicos?
¿Diseñas blog para divulgar o compartir conocimientos?
¿Empleas las redes sociales educativas para estimular la colaboracion?
¿Cómo te haz sentido al momento de perder un usuario y contraseña?
¿Conoces el procedimiento para recuperar archivos si se daña tu dispositivo electrónico?
¿Cuáles procedimientos utilizas para crear contraseñas seguras?
¿Cuál es el tiempo que estableces para cambiar tus conraseñas de tus cuentas personales y dispositivos electrónicos?
¿identificas el lugar seguro para almacenar tus datos y contraseñas?
¿Conoces las implicaciones al conectarse a redes de Wifi de acceso libre exponiendo tus datos hacia los demas?
¿Cuál es el lugar adecuado para almacenar los respaldos de los datos o informaciones que utilizas amenudo en tus dispositivos electrónicos?
¿Cómo puedes determinar la confiabilidad al momento de navegar en una pagina o un Sitio Web?
¿Conoces los riesgos de emplear internet?
¿ Conoce los riesgos de compartir datos personales?
¿Posee los conocimientos o habilidades para resolver problemas técnicos en cuanto a los aparatos tecnológicos?
¿Cuál es el grado de complegidad al implementar las Tecnologías en la escuela?
¿Cuáles aplicaciones o herramientas son más favorables para realizar las actividades en la escuela?
¿Cuáles aplicaciones o herramientas son consideradas mas complicadas al momento de realizar actividades ?
¿Cuáles medios estratégicos o elementos emplean la institución para lograr el manejo apropiado de las TICCAD?
¿Cuáles son los recursos o medios tecnológicos por el cual establece comunicación para las clases en la escuela?
¿Cómo ha sido la valoración de tus actividades en la plataforma virtual?
¿Recibes apoyo de la familia en la integración o intervencion de tus clases virtuales?
¿Posee la capacidad de identificar el uso de cada una de las aplicaciones o herramientas utilizadas para llevar a cabo la docencia integrando la
¿Conoces la importancia de instalación de programas antivirus para prevención de los ataques de haquers informáticos?.
¿Cuentas con instalación de Softwares o programas de detección de virus informaticos en tu dispositivo?
¿Cuentas con los conocimientos necesarios para limpiar adecuadamente tu ordenador en el momento preciso?

Clasificación	Indicadores para docentes	Indicadores para estudiantes	Indicadores para personal administrativo
Estudiantes, docentes y personal administrativo	Habilidades para empleo seguro	Habilidades para empleo seguro	Habilidades para empleo seguro
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Habilidades para el empleo creativo	Habilidades para el empleo creativo	Habilidades para el empleo creativo
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Habilidades para el empleo seguro	Habilidades para el empleo seguro	Habilidades para el empleo seguro
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Docentes y personal administrativo	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Docentes y personal administrativo			
Docentes y personal administrativo			
Docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Habilidades para el empleo creativo	Habilidades para el empleo creativo	Habilidades para el empleo creativo
Docentes y personal administrativo			
Docentes y personal administrativo			
Docentes			
Docentes			
Estudiantes, docentes y personal administrativo	Habilidades para el empleo seguro	Habilidades para el empleo seguro	Habilidades para el empleo seguro
Estudiantes			
Estudiantes, docentes y personal administrativo	Habilidades para el empleo crítico	Habilidades para el empleo crítico	Habilidades para el empleo crítico
Estudiantes, docentes y personal administrativo			
Docentes y personal administrativo	Habilidades para el empleo creativo		Habilidades para el empleo creativo
Docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico	Habilidades de pensamiento crítico
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Docentes	Usabilidad pedagógica		
Docentes			
Docentes	Empleo proactivo		
Docentes			
Docentes	Habilidades de pensamiento deductivo-inductivo		
Docentes			
Estudiantes, docentes y personal administrativo	Uso responsable	Uso responsable	Uso responsable
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Uso de empleo socialmente aceptable	Uso de empleo socialmente aceptab	Uso de empleo socialmente aceptable
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Actualización permanente de contraseí	Actualización permanente de contras	Actualización permanente de contraseñas
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Conductas para protección de datos pe	Conductas para protección de datos	Conductas para protección de datos persona
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Nivel de conocimiento sobre seguridad	Nivel de conocimiento sobre segurid	Nivel de conocimiento sobre seguridad inform
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Manejo responsable de las TICCAD	Manejo responsable de las TICCAD	Manejo responsable de las TICCAD
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Interacción social adecuada	Interacción social adecuada	Interacción social adecuada
Estudiantes, docentes y personal administrativo			
Estudiantes			
Estudiantes			
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo	Discriminación de posibles virus inform	Discriminación de posibles virus info	Discriminación de posibles virus informáticos
Estudiantes, docentes y personal administrativo			
Estudiantes, docentes y personal administrativo			

Entrevista para el Personal Administrativo **Preguntas guía**
Habilidades para el empleo seguro de las TICCAD
1. ¿Cuáles son los riesgos de emplear internet?
2..¿Qué procedimiento utilizas para crear contraseñas seguras?
3. ¿Conoce el procedimiento para manejar sus cuentas personales, documentos o archivos desde cualquier dispositivo electró
4. ¿Cuáles han sido las principales dificultades que el Centro Educativo ha enfrentado para implementar las tecnologías?
5. ¿Qué aplicaciones o herramientas resultan más complicadas para llevar a cabo el proceso de enseñanza-aprendizaje?
Habilidades para el empleo crítico de las TICCAD
6. ¿De qué forma identifica los recursos tecnológicos seguros para instalar en su dispositivo
7. ¿Cuáles son las implicaciones del uso de contraseñas automáticas de sus cuen
Interacción Social adecuada
8. ¿Qué medios o elementos estratégicos emplea la institución para el manejo apropiado de las tecnologías de la información,
9. ¿Cuáles son los recursos o medios tecnológicos para la comunicación en las clases del Centro Educativo?
10. ¿Qué medios estratégicos emplea la institución para integrar a las familias en la escuela?

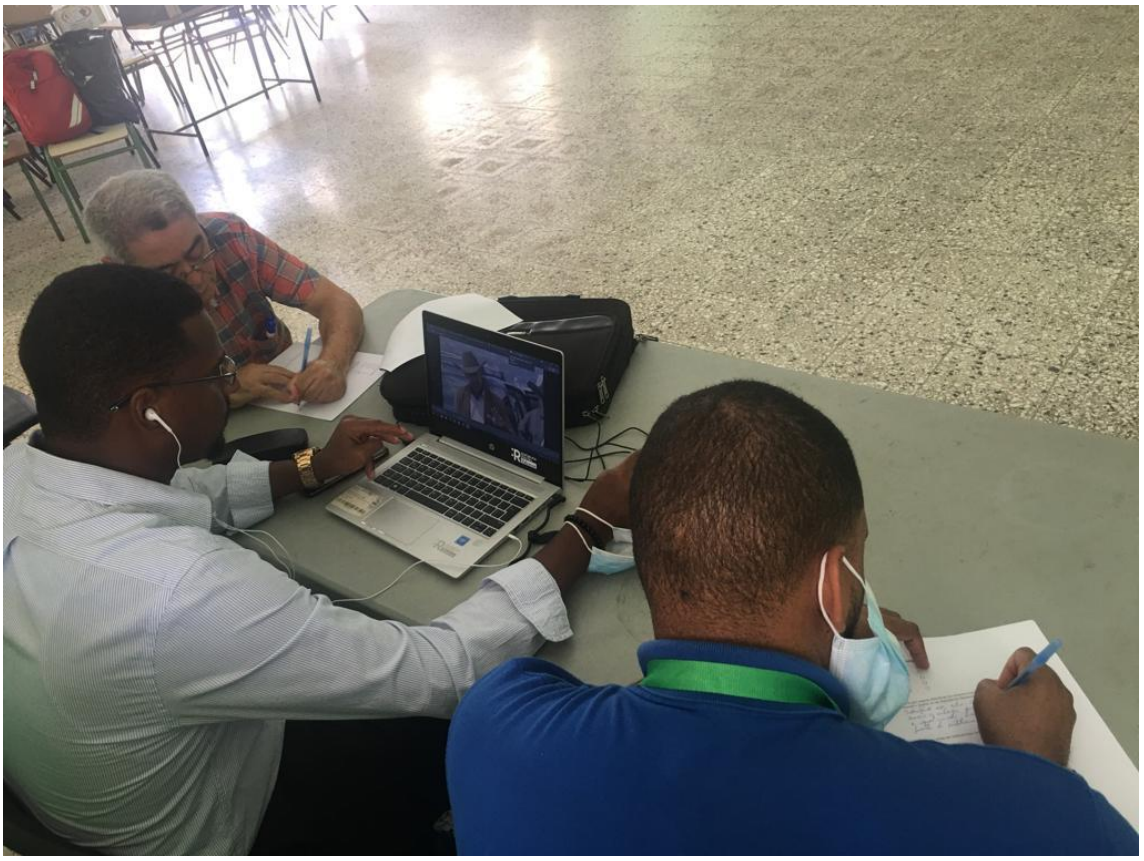
Cuestionario para estudiantes Preguntas guía
Habilidades para el empleo seguro de las TICCAD
1. ¿Cómo identificas los recursos tecnológicos seguros para instalar en tus dispositivos electrónicos?
2.¿Cómo identificas los sitios seguros y no seguros al momento de navegar en internet?.
3. ¿Identificas las posibilidades de bullyng, sexting escolar o ciberbullying al establecer comunicación c
4.¿Qué procedimiento utilizas para crear contraseñas seguras?.
5.¿Conoces los riesgos de emplear internet?.
6. ¿Cuáles serían los principales riesgos de conectarse a redes Wifi de ac
Habilidades para el empleo crítico de las TICCAD
7. ¿Cómo identificas que la información de la red es verdadera o válida?
8. ¿Qué mecanismos utilizas para cambiar la contraseña de tus cuentas personales y de servicios en
Interacción social adecuado con las TICCAD
9. ¿Qué actividades de apoyo por los docentes has recibido en la plataforma virtual?
10. ¿Qué tipo de apoyo recibes de tu familia para cumplir con las actividades escolares en línea?.

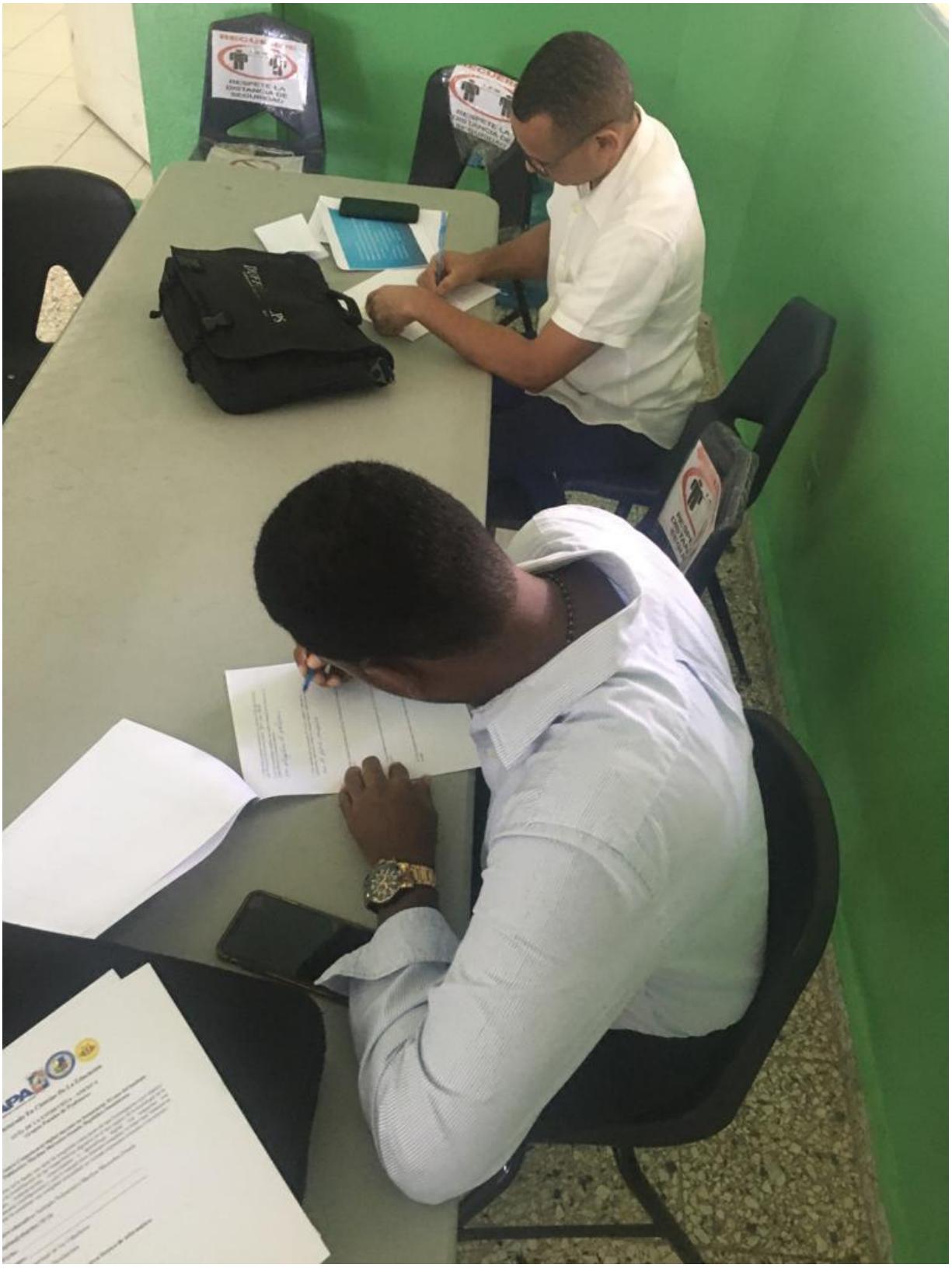
Grupos Focales de Profesores Preguntas guía
Empleo seguro de las TICCAD
1. ¿De qué forma identifican los recursos tecnológicos seguros para instalar en sus dispositivos electrónico
2. ¿Cómo identifican los sitios seguros y no seguros al momento de navegar en internet?
3.¿Cuál sería el riesgo principal de emplear internet?
4.¿Qué tipos de programas antivirus utilizas para prevenir los ataques informáticos?
5.¿Cuáles serían las principales implicaciones de conectarse a redes Wifi de acceso libre?
Usabilidad pedagógica de las TICCAD
6. ¿Qué tipo de empleo pedagógico de las tecnologías consideran en su planeación didáctica?
Empleo crítico de las TICCAD
7. ¿Cómo identifican que la información de la red es verdadera o válida?
8. ¿Qué contenidos o herramientas digitales utilizan como apoyo en sus clases?
Empleo creativo de las TICCAD
9. ¿Qué herramientas tecnológicas utilizarían para diseñar presentaciones atractivas para sus clases?
10. El empleo de las tecnologías ¿qué nuevas formas de enseñar les permite?.

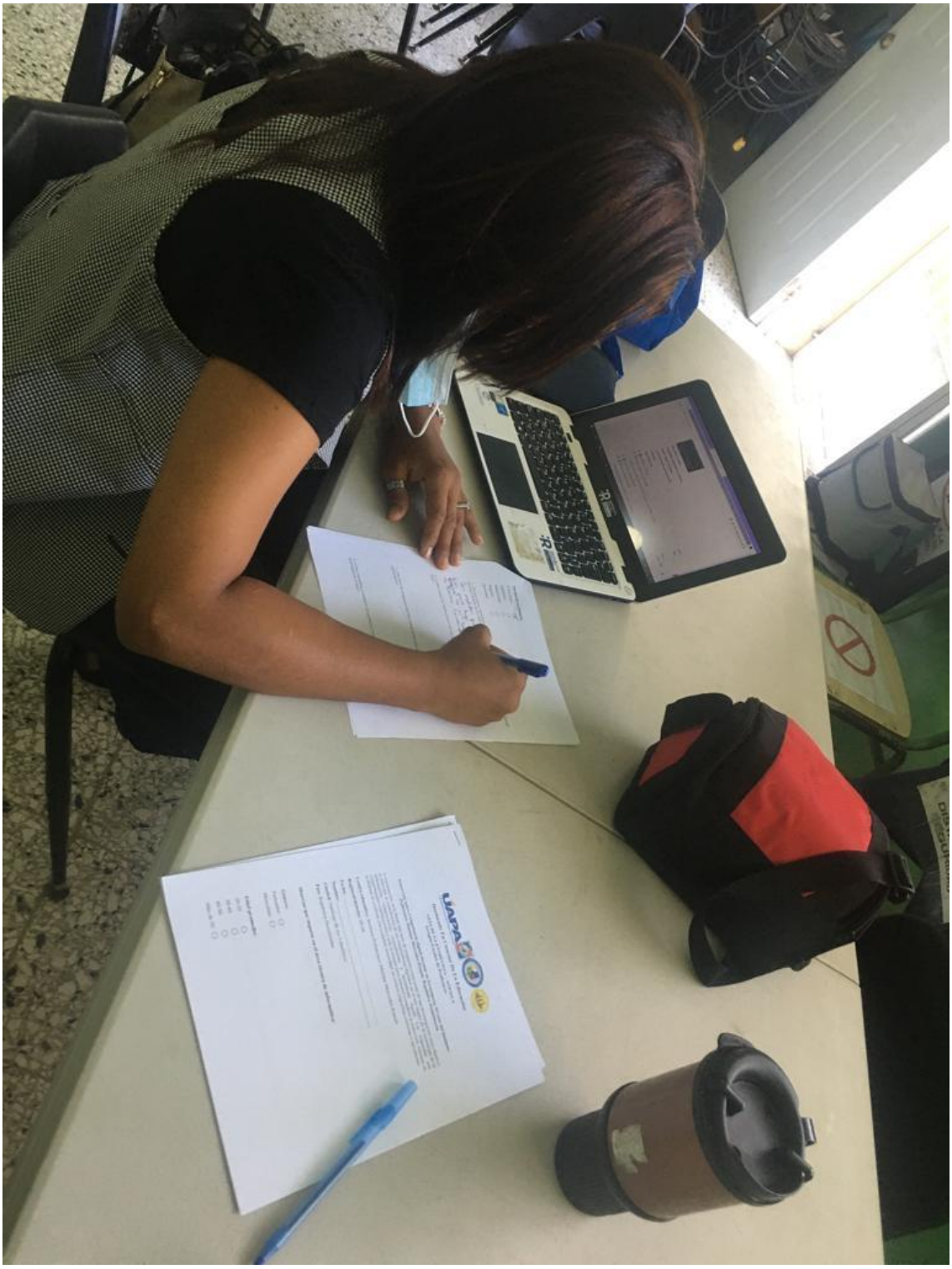

POLITECNICO 'LA CHICHIGUA'
GURABO
MARTINA MERCEDES ZOUAIN


HICHIGUA
S ZOUAIN
TOMÁS RICHARDO
PRESIDENTE
SALIDA DE EMERGENCIA

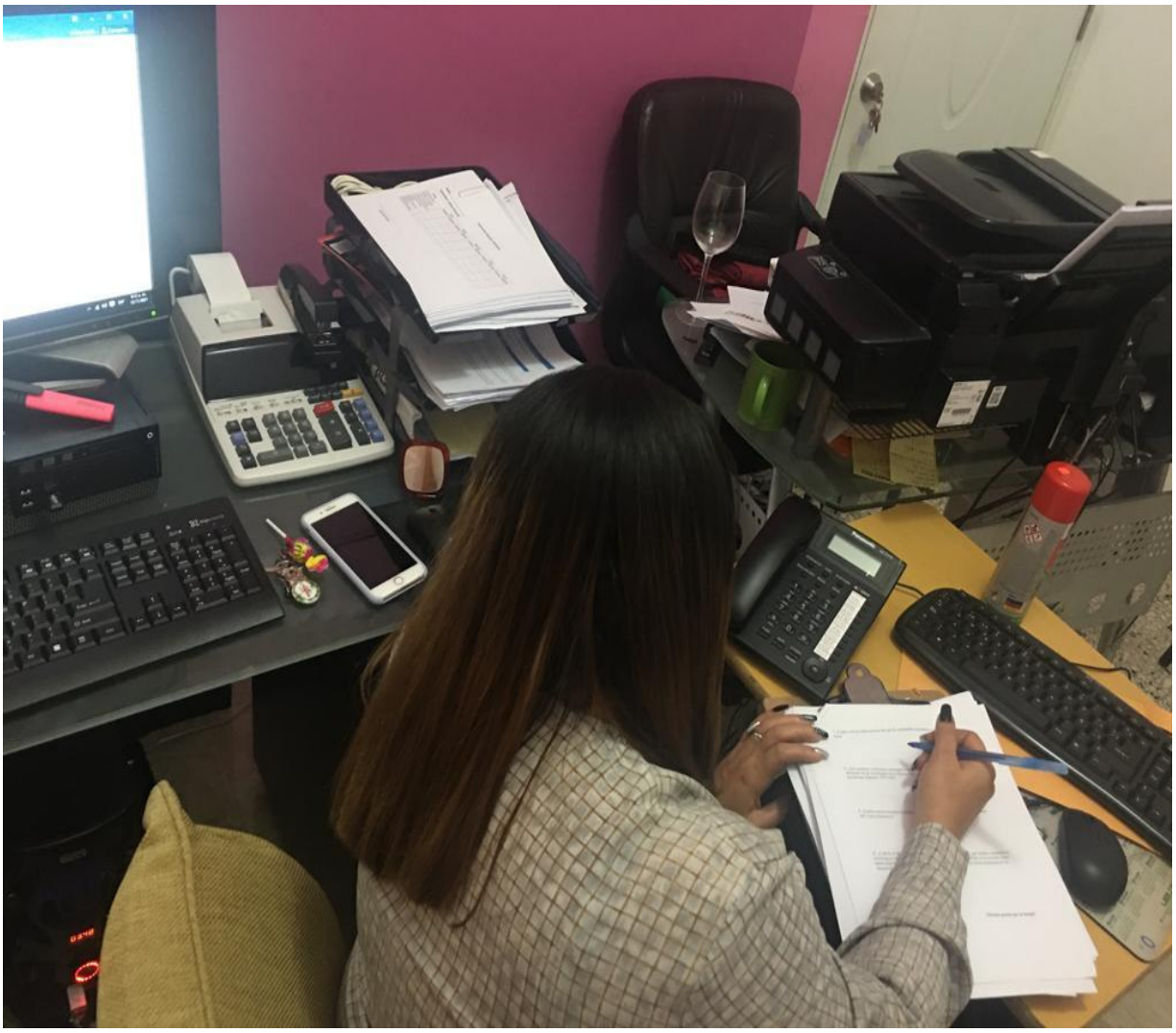

Valores
Disciplina
Respeto
Scarlyn Rodriguez
Brenda Paulino

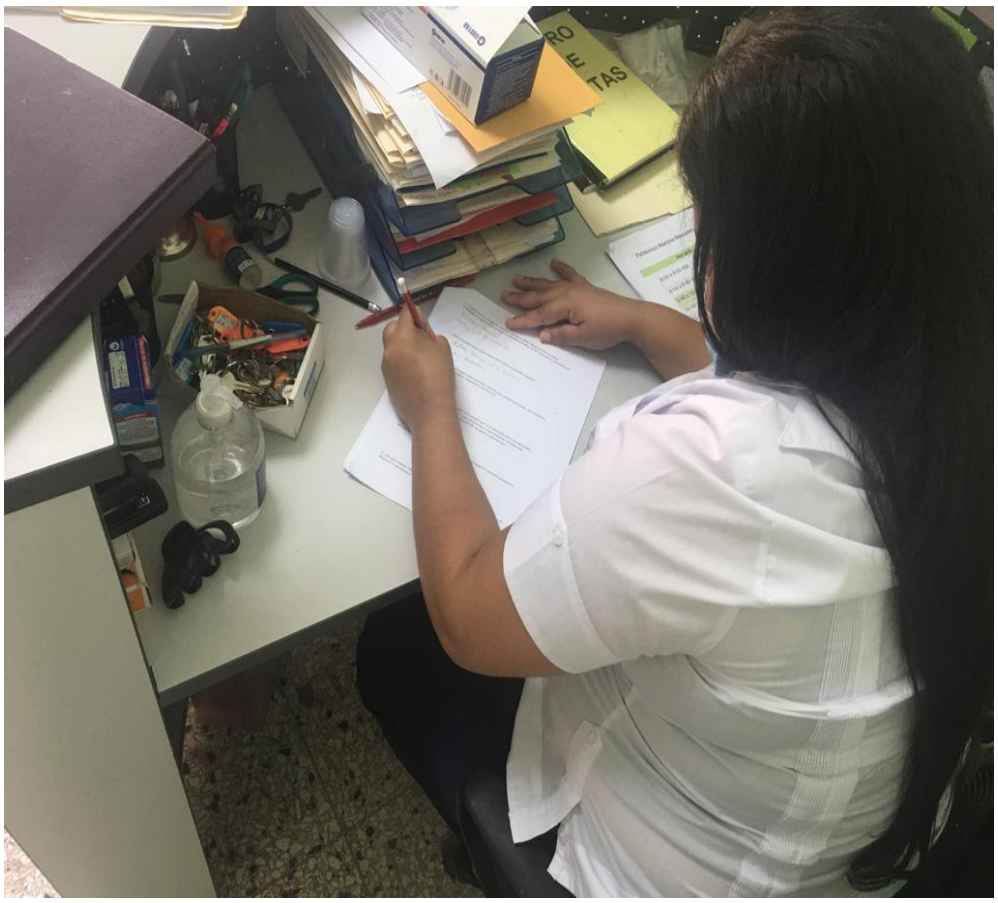


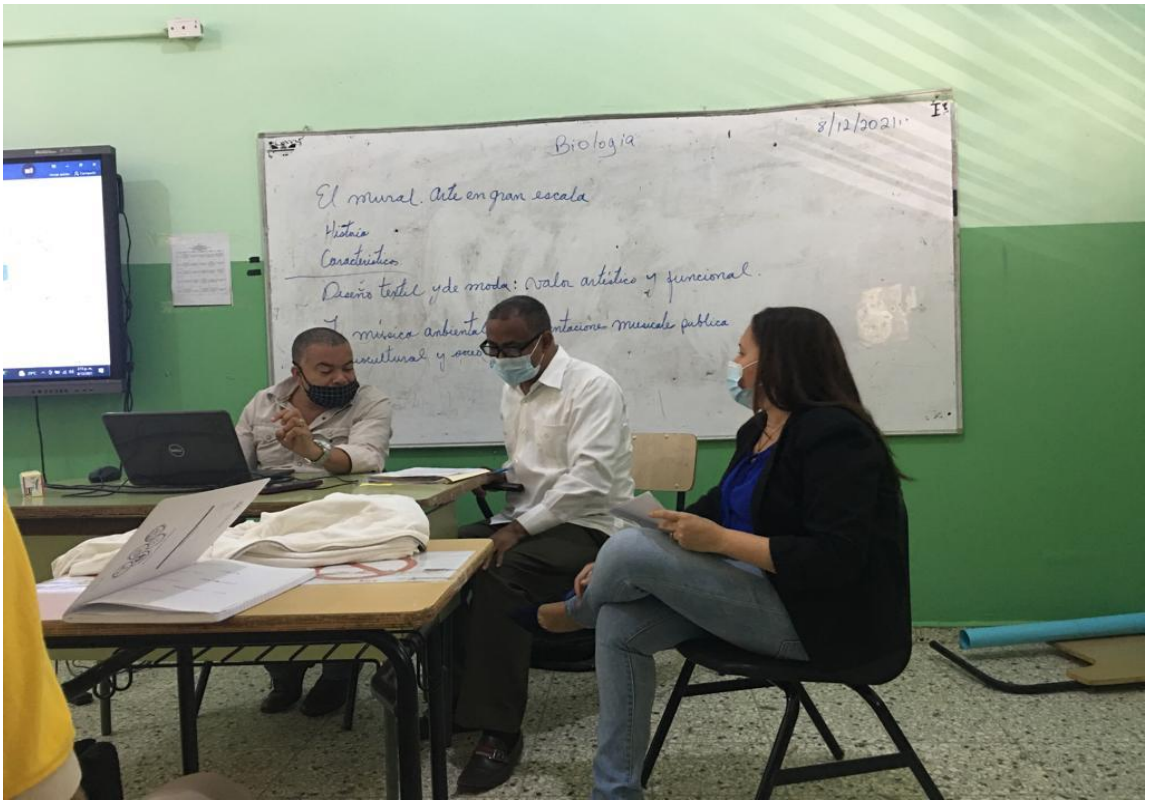


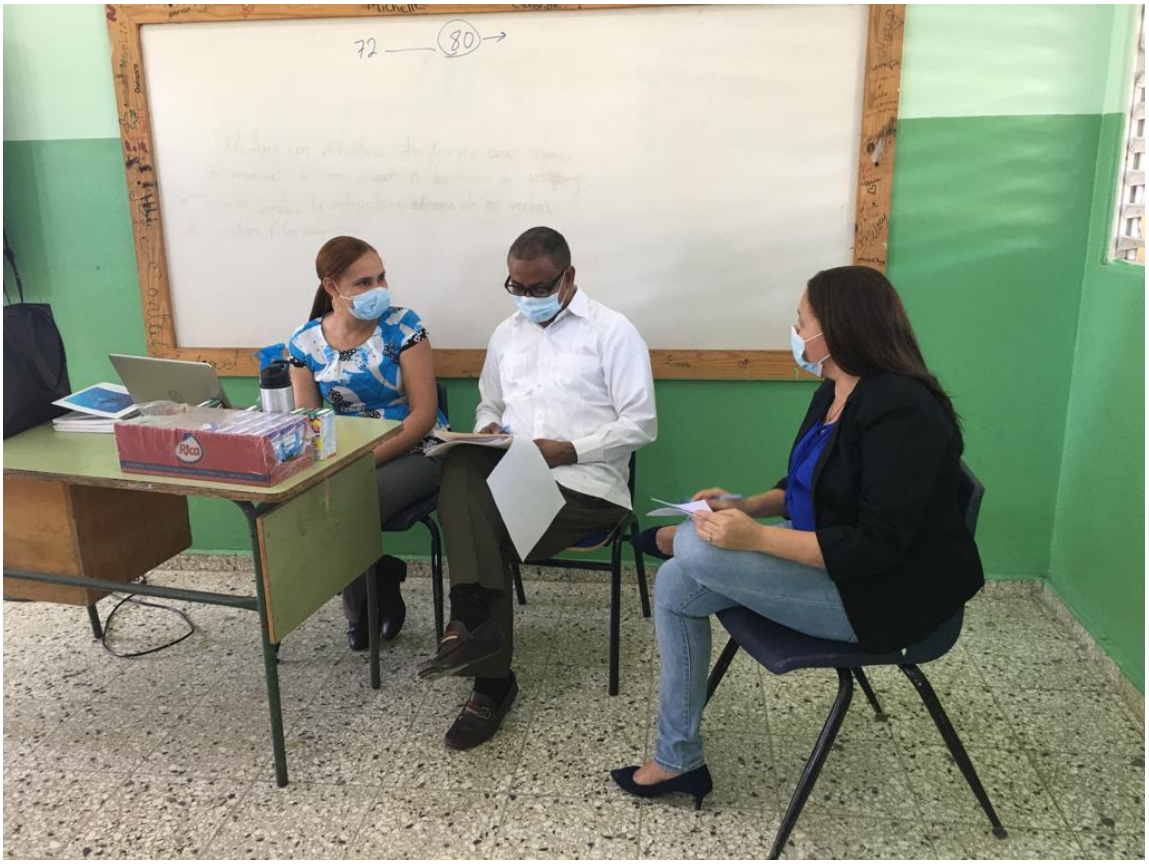



BIENVENIDOS

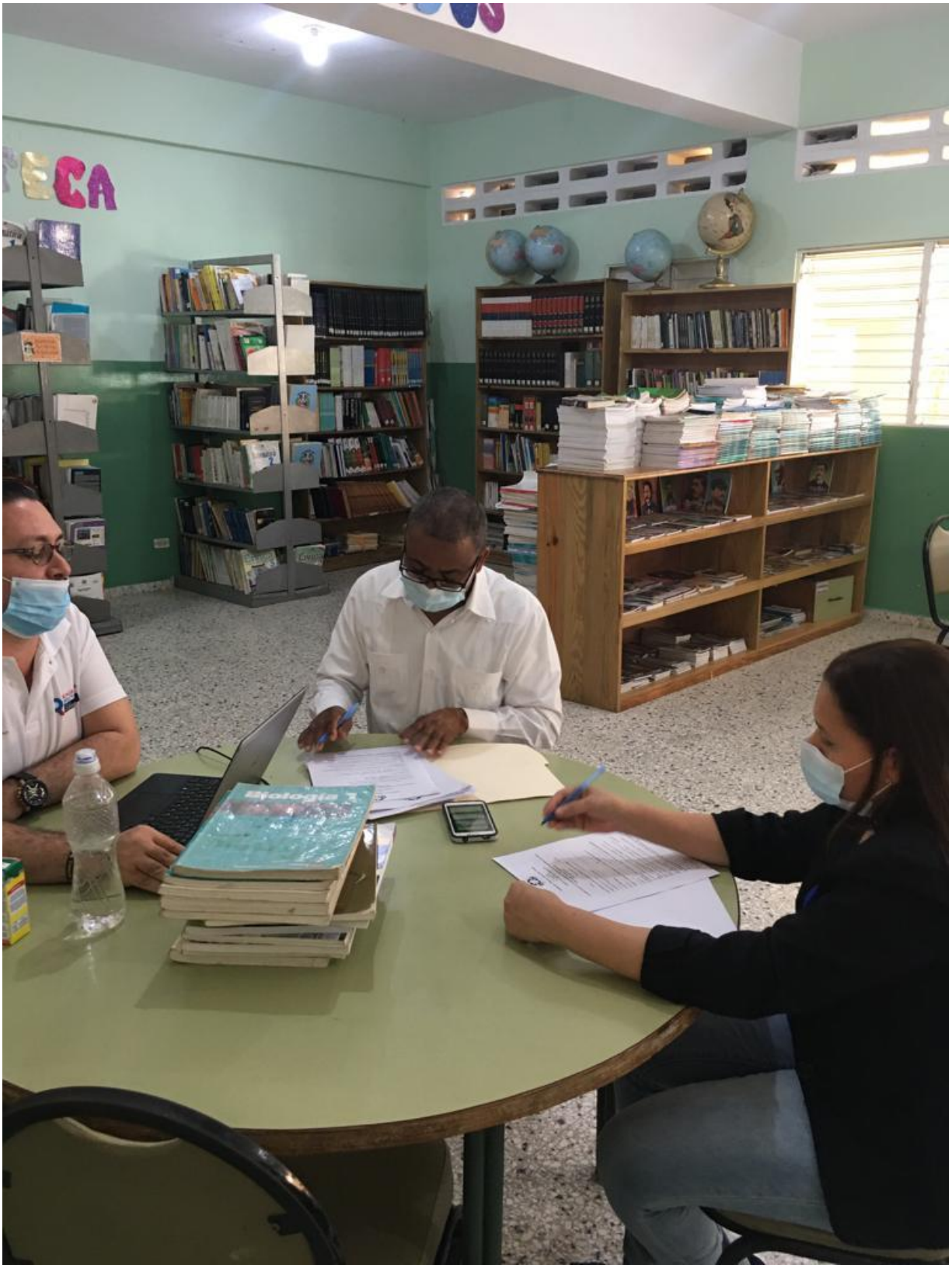





Biología
8/12/2021
El mural. Arte en gran escala
Historia
Características
Diseño textil y de moda: Valor artístico y funcional


72
80


BIBLIOTECA


Biología

AUTORIZACIÓN OFICIAL

VICERRECTORÍA DE INVESTIGACIÓN, INNOVACIÓN Y POSTGRADO

DOCTORADO EN CIENCIAS DE LA EDUCACIÓN

CARTA AUTORIZACIÓN PARA USO, REPRODUCIÓN Y DIVULGACIÓN DE OBRA CIENTÍFICA CA-VIIP-UIFP-03

Yo, Nieves del Carmen Pérez, suscribo la siguiente autorización en fecha 18 de octubre 2023 con el fin de que se realice la reproducción, uso, comunicación y publicación de esta obra en los siguientes términos:

1. Autorizo de manera pura y simple a la UNIVERSIDAD ABIERTA PARA ADULTOS, UAPA, con el fin de que se utilice la Tesis titulada:
2. TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA:
   ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA DOMINICANA
3. Que dicha autorización recaerá en especial sobre los derechos patrimoniales de reproducción de la obra, por cualquier medio, con fines educativos o comerciales, transformación de la obra, a través del cambio de soporte físico, digitalización, traducciones, adaptaciones o cualquier otra forma de generar obras derivadas.

4. Declaro que la tesis es original y que es de mi creación exclusiva, no existiendo impedimento de ninguna naturaleza para la cesión de derechos que estoy haciendo, respondiendo además por cualquier acción de reivindicación, plagio u otra clase de reclamación que al respecto pudiera sobrevenir.

5. Que dicha autorización se hace a título gratuito.

6. Que los derechos morales del (o de la) autor(a) sobre la Tesis corresponden exclusivamente al (a la) AUTOR (A) y en tal virtud, a la UNIVERSIDAD ABIERTA PARA ADULTOS, UAPA, se obliga a reconocerlos expresamente y a respetarlos de manera rigurosa.

7.

Autor(a)

DEPARTAMENTO DE BIBLIOTECA

Plantilla de depósito de las obras digitales para su almacenamiento en el Repositorio Académico Institucional.

Por este medio el (los) autor (es) Nieves del Carmen Pérez

autoriza(n) a la Universidad Abierta para Adultos (UAPA) publicar en el Repositorio Académico Institucional su obra titulada: TECNOLOGÍAS DE LA INFORMACIÓN Y COMPETENCIA DIGITAL EN EDUCACIÓN SECUNDARIA: ESTUDIO DE CASO EN EL INSTITUTO POLITECNICO MARTINA MERCEDES ZOUAIN, REPÚBLICA

Siguiendo los términos y condiciones establecidos en este documento.

Términos y Condiciones de Publicación

1. Estará registrada bajo las Licencias Creative Conmons: Atribución -No comercial- Sin obras derivadas. Esta licencia permite copiar, distribuir, exhibir y ejecutar la obra. Todo ello a condición de que se atribuya la autoría sobre la obra en la forma en que haya sido especificada por el(los) autor(es) o el licenciante; no se use comercialmente; y que no se produzcan obras derivadas sobre la original.
2. El acceso a la obra será libre, permitiendo su consulta y descarga, pero no su modificación.
3. Las opiniones contenidas en la presente obra son de exclusiva responsabilidad de su(s) autor(es). UAPA, como institución, no se responsabiliza de los conceptos que aquí se emiten.

Tipo de obra digital Marcar con un (✓) cotejo el recuadro.

✓	Tesis		Revista		Conferencia
	Informe final de grado		Boletín		Memoria de evento
	Libro		Artículo científico		Ponencia en evento
	Objetos de aprendizaje		Multimedia		Otros.Especifique:_____

Autorizado y entregado en la ciudad de Santiago, República Dominicana a los 18 días del mes de octubre del año 2023

_____
Autor(a) de la obra

_____ _____
Instancia Gestora Director /Encargado del Departamento de Biblioteca