RECIE
Revista Electrónica Científica de Investigación Educativa

Volumen 7, enero-diciembre 2023
ISSN: 2594-200X

Una propuesta didáctica para el cambio de base utilizando la encriptación de mensajes

A didactic proposal for the change of base, using message encryption

Andrés Hernández-Quintana • Verónica Valenzuela González • Alberto Camacho Ríos

Andrés Hernández-Quintana. Tecnológico Nacional de México, campus Chihuahua II. Es profesor de carrera en áreas de Ciencias Básicas y de la maestría en Sistemas Computacionales. Cuenta con estudios de Maestría en Dirección y Gestión Empresarial e Ingeniería en Sistemas Computacionales. Miembro del Cuerpo Académico "Educación Matemática y Educación" con clave ITCH-CA-2. Correo electrónico: andres.hq@chihuahua2.tecnm.mx. ORCID: https://orcid.org/0000-0002-3486-4400.

Verónica Valenzuela González. Tecnológico Nacional de México, campus Chihuahua II. Es profesora de carrera en áreas de Ciencias Básicas y de la Maestría en Sistemas Computacionales. Cuenta con estudios de Maestría en Educación Campo Práctica Docente e Ingeniería Industrial. Miembro del Cuerpo Académico "Educación Matemática y Educación" con clave ITCH-CA-2. Correo electrónico: veronica.vg@chihuahua2.tecnm.mx. ORCID: https://orcid.org/0000-0002-4363-4930.

Alberto Camacho Ríos. Tecnológico Nacional de México, campus Chihuahua II. Es profesor-investigador en áreas de Ciencias Básicas y de la Maestría en Sistemas Computacionales. Miembro del Sistema Nacional de Investigadores (SNI, nivel 1). Cuenta con estudios de Doctorado en Matemática Educativa. Miembro del Cuerpo Académico "Educación Matemática y Educación" con clave ITCH-CA-2. Correo electrónico: alberto.cr@chihuahua2.tecnm.mx. ORCID: https://orcid.org/0000-0002-0685-4723.

Resumen

En esta investigación se muestran los resultados de estudiantes de la asignatura de Álgebra lineal del Tecnológico Nacional de México al desarrollar un problema de aplicación de encriptación de datos que aborda los conceptos de base y cambio de base desde la perspectiva de la teoría antropológica de lo didáctico, con el objetivo de dar respuesta a las siguientes preguntas de investigación: "¿Logran los estudiantes aplicar el concepto de cambio de base en la encriptación de información?" y "¿Cuáles son los errores más comunes durante el proceso?". Se creó un programa en lenguaje Python que elabora los ejercicios de la actividad de encriptar un mensaje, a su vez este último revisa las respuestas dadas por los estudiantes. Después de analizar los resultados se encontró que los estudiantes que completaron el ejercicio correctamente y quienes solo tuvieron errores aritméticos lograron aplicar los conceptos de base y cambio de base, siendo en total el 93.5%.

Palabras clave: Matemática educativa, álgebra lineal, cambio de base, encriptación, matriz de transición.

Abstract

This research shows Tecnológico Nacional de México students results of the Linear Algebra course, in developing a data encryption application problem that addresses the concepts of basis and change of basis from the perspective of the Anthropological Theory of the Didactic, with the aim of answering the following research questions: "Are students able to apply the concept of change of basis in the encryption of information?" and "What are the most common mistakes during the process?". A program in Python language was developed to create the exercises of the encryption activity used to review the students' responses. After analyzing the results, it was found that students who completed the exercise correctly and that only had arithmetic errors, managed to apply the concepts of base and change of base, with a total of 93.5%.

Keywords: Educational mathematics, linear algebra, basis change, encryption, transition matrix.

Recibido: 27 de enero de 2023 | Aprobado: 28 de septiembre de 2023 | Publicado: 17 de octubre de 2023
DOI: https://doi.org/10.33010/recie.v7i0.1792

Introducción

En la educación de nivel universitario, sobre todo en aquellas carreras afines a la ingeniería, las matemáticas constituyen uno de los elementos fundamentales en el desarrollo de todo profesionista, estando directamente relacionadas con asignaturas como física, economía, investigación de operaciones, estadística, entre otras.

Dentro del estudio de diversos métodos de enseñanza resulta de especial interés la dificultad en el aprendizaje de asignaturas relacionadas con las matemáticas que presentan los estudiantes de todos los niveles y se acentúa en aquellas de nivel avanzado, las cuales forman parte del currículo en carreras de ingeniería.

Esta problemática no es ajena al Tecnológico Nacional de México (TecNM) campus Chihuahua II, donde los estudiantes que no aprueban alguna asignatura presentan dificultades de rezago, que incluso pueden llegar a la deserción (Hernández-Quintana, 2018). Las asignaturas que presentan los mayores índices de reprobación son aquellas relacionadas directamente con las matemáticas, como son Cálculo diferencial, Cálculo integral, Cálculo vectorial, Ecuaciones diferenciales y Álgebra lineal.

El Tecnológico Nacional de México (TecNM) cuenta con diferentes carreras de ingeniería. En el campus Chihuahua II se tienen aquellas de Ingeniería en Sistemas Computaciones (ISC), Ingeniería en Informática (IINF), Ingeniería en Diseño Industrial (IDI), Ingeniería Industrial (IIND) e Ingeniería en Gestión Empresarial (IGE). El curso de Álgebra lineal forma parte del tronco común en estas carreras. El programa del curso incluye una unidad dedicada al estudio de espacios vectoriales en la cual se ha detectado que los estudiantes presentan mayor dificultad para la compresión y la asimilación de los conceptos. Existen diversas investigaciones que abordan esta problemática y en ellas se hace referencia a la naturaleza abstracta y a la complejidad de estos conceptos (Guzmán y Zambrano, 2015; Parraguez y Vera-Soria, 2020; Vera y Miranda, 2014).

A finales del siglo XIX se dio inicio a la axiomatización del álgebra lineal, dando como resultado una reconstrucción teórica de los métodos para resolver problemas lineales usando los conceptos y herramientas de una nueva teoría axiomática central (Dorier y Sierpinska, 2001). Dicha reconstrucción marcó un nuevo nivel de abstracción del concepto de espacio vectorial que incluye objetos abstractos como vectores geométricos, *n*-tuplas, polinomios, series o funciones. Como resultado de la axiomatización y de los conceptos que de ella derivan la enseñanza-aprendizaje de los espacios vectoriales exige en los estudiantes un nivel elevado de razonamiento cognitivo y comprensión de procesos matemáticos.

Existen estudios que abordan el problema de enseñanza-aprendizaje desde diferentes perspectivas, es el caso de Vázquez (2019), que propone actividades didácticas que permiten analizar cómo los estudiantes se enfrentan al concepto de *espacio vectorial* desde la perspectiva de la *teoría antropológica de lo didáctico*. Parraguez y Vera-Soria (2020) indagaron cómo es el proceso de construcción del significado del acto de comprender

el concepto de base en $\mathbb{R}^2$, realizando entrevistas a estudiantes los cuales previamente abordaron actividades para la exploración del concepto. Valenzuela, Hernández-Quintana y Camacho (2021) midieron el nivel de competencia del concepto de base de un espacio vectorial usando la taxonomía SOLO, analizando las respuestas que dieron estudiantes quienes finalizaban el curso de Álgebra lineal por medio de un instrumento de evaluación diseñado exprofeso. Stewart y Thomas (2010) utilizaron la teoría APOE (Acción, Proceso, Objeto y Esquema) para indagar la comprensión del concepto de *base* en estudiantes universitarios, llegando a la conclusión de que el énfasis en los procesos matriciales no ayuda a los estudiantes a comprender el concepto de base; incluso Madrid et al. (2016) detallan las dificultades intrínsecas del concepto de espacios vectoriales que presentan los estudiantes para comprenderlo y la forma de tratar el tema en el aula, evaluando la propuesta de eliminar el tema del programa de Álgebra lineal por no tener aplicaciones y no estar vinculado con el resto del programa, así como por su carácter teórico y por dificultar la asimilación de los conocimientos.

En el programa de estudios la unidad de Espacios vectoriales incluye los conceptos de Espacio vectorial, Subespacio vectorial, Combinación lineal, Espacio generado, Independencia lineal, Base, Cambio de base y Ortonormalización, entre otros. La definición de base se considera una parte fundamental en el estudio de los espacios vectoriales, en tanto su comprensión está estrechamente relacionada con las demás nociones que articulan el tema.

De acuerdo con Valenzuela-González et al. (2021), los estudiantes conocen el concepto de base desde una perspectiva algorítmica o metodológica, y logran reproducir algunos procedimientos sin tener la comprensión de los conceptos relacionados a la base de un espacio vectorial.

Si bien el álgebra lineal tiene aplicaciones en la ingeniería, la informática y la vida cotidiana, el tema de Espacios vectoriales carece de aplicaciones sencillas que pudieran ayudar al estudiante para mejorar su comprensión. Sin embargo, es posible aplicar los conceptos de *base* y *cambio de base* en algunos métodos básicos de la encriptación de datos utilizados en la criptografía. La palabra "criptografía" procede de las palabras griegas *kryptós* y *graphein*, que significan "secreto" y "escribir", respectivamente. La traducción corresponde al arte de escribir de manera secreta (Willems y Gutierrez, 2010). La encriptación o cifrado es una técnica de codificación de información cuya herramienta principal son las matemáticas (Fiarresga, 2010).

El cifrado de información es un tema de estudio común en carreras afines a la informática, sin embargo, su utilidad es cotidiana desde una conversación cifrada punto a punto, como es utilizada en la aplicación WhatsApp, o bien en sistemas de seguridad de banca electrónica, incluso al navegar en internet en las páginas más comunes se cifra la información desde el dispositivo hasta el servidor. Prácticamente cualquier comunicación que requiera un nivel mínimo de privacidad o confidencialidad utiliza

algún algoritmo de encriptación. Álvarez et al. (2021) analizan diferentes métodos de codificación con la finalidad de plantear una actividad de estudio del álgebra lineal.

En esta investigación se muestran los resultados de estudiantes al desarrollar un problema de aplicación de encriptación de datos que aborda los conceptos de base y cambio de base desde la perspectiva de la *teoría antropológica de lo didáctico* (TAD) y la *transposición informática*, con el objetivo de dar respuesta a las siguientes preguntas de investigación: "¿Logran los estudiantes aplicar el concepto de cambio de base en la encriptación de información?" y "¿Cuáles son los errores más comunes durante el proceso?".

Para plantear los problemas a resolver por cada estudiante se creó un programa en lenguaje Python que sirvió para la elaboración de los ejercicios, encriptando una pregunta, y para procesar las respuestas dadas por los estudiantes, descifrando la respuesta a la pregunta para facilitar la revisión de los problemas.

Fundamentos teóricos

Teoría antropológica de lo didáctico

En la *teoría antropológica de lo didáctico* (TAD), Chevallard (1998) define las técnicas matemáticas como elementos tecnológicos contenidos en organizaciones matemáticas (OM), también reconocidas como "praxeologías", dispuestas en el esquema [T, τ, θ, Θ]. Una OM se compone de un saber-hacer reconocido como *praxis* [T, τ] donde T representa una tarea o proyecto por resolver, τ es la técnica matemática que lleva a la resolución de la tarea T. El saber o *logos* es concebido como [θ, Θ], en el cual θ se conoce como tecnología, relacionada con teoremas, definiciones, axiomas, entre otros, en tanto Θ se muestra como la teoría que da sustento a la tecnología y al resto de los elementos de la organización.

El problema de aplicación propuesto para cada estudiante fue modelizado por dos organizaciones matemáticas, OM_1 y OM_2, que se describen enseguida.

La primera, OM_1, representada por [T_1, τ_1, θ, Θ], se define como:

Tipo de tarea, T_1: convertir los elementos de un vector $\bar{x}_B$ en $\mathbb{R}^3$ construidos en términos de la base B a términos de la base canónica. Por ejemplo, convertir $\bar{x}_B = \begin{pmatrix} 566 \\ 191 \\ 1008 \end{pmatrix}$ en términos de $B = \left\{ \begin{pmatrix} 0 \\ -2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\}$ a términos de la base canónica, se entiende como base canónica a la base típica o usual constituida por los vectores {i, j, k} donde $\boldsymbol{i} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \boldsymbol{j} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \boldsymbol{k} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

Técnica, τ_1: utilizar la matriz de transición $A_{B \to C}$, la cual se obtiene formando una matriz con los vectores de la base como columnas de la matriz y multiplicándola por el vector $\bar{x}_B$.

Teorema, θ: la representación de un vector con respecto a una base. Sea $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ una base de un espacio vectorial V y $\bar{x}$ un vector en V tales que $\bar{x} = c_1\bar{v}_1 + c_2\bar{v}_2 + \ldots + c_n\bar{v}_n$. Los escalares $c_1, c_2, \ldots, c_n$ se denominan coordenadas de $\bar{x}$ con respecto a la base B, $\bar{x}_B$. El vector de coordenadas de $\bar{x}_B$ es el vector $\bar{x}_B = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ (Grossman y Flores, 2012).

De dicha definición se desprende el siguiente teorema:

Teorema, θ_1: La base de un espacio vectorial es un conjunto de vectores $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ en un espacio vectorial V que genera a V y cuyos vectores son linealmente independientes. Si $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ es una base de un espacio vectorial V, entonces todo vector en V se puede escribir de una y solo una forma como combinación lineal de vectores en B (Grossman y Flores, 2012).

Teoría, Θ: Álgebra lineal.

En OM_1 la técnica se desprende de las tecnologías θ y θ_1 las cuales, a su vez, son comprendidas en un marco teórico determinado por el álgebra lineal. Algo semejante se puede afirmar de la siguiente organización matemática OM_2.

La OM_2 [T_2, τ_2, θ, Θ] se define como:

Tipo de tarea, T_2: Convertir un vector $\bar{x}_B$ en $\mathbb{R}^3$ construido en términos de la base canónica a términos de una base B. Por ejemplo, convertir $\bar{x} = \begin{pmatrix} 67 \\ 105 \\ 117 \end{pmatrix}$ en términos de la base canónica $C = \left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}$ a la base $B = \left\{\begin{pmatrix} 0 \\ -2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}\right\}$.

Técnica, τ_2: Utilizar la matriz de transición $A_{C \to B}$, la cual se obtiene formando una matriz con los vectores de la base como columnas de la matriz, calculando su inversa y multiplicándola por el vector $\bar{x}$.

Teorema, θ: La representación de un vector con respecto a una base. Sea $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ una base de un espacio vectorial V y $\bar{x}$ un vector en V tales que $\bar{x} = c_1\bar{v}_1 + c_2\bar{v}_2 + \ldots + c_n\bar{v}_n$. Los escalares $c_1, c_2, \ldots, c_n$ se denominan coordenadas de $\bar{x}$ con respecto a la base V, $\bar{x}_B$. El vector de coordenadas $\bar{x}_B$ es el vector $\bar{x}_B = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ (Grossman y Flores, 2012).

Teorema, θ_1: La base de un espacio vectorial es un conjunto de vectores $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ en un espacio vectorial V que genera a V y cuyos vectores

son linealmente independientes. Si $B = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ es una base de un espacio vectorial V, entonces todo vector en V se puede escribir de una y solo una forma como combinación lineal de vectores en B (Grossman y Flores, 2012).

Teoría, Θ: Álgebra lineal.

Las OM están dispuestas en seis *momentos didácticos* (Chevallard, 1999):

- El *primer momento* es el primer encuentro con un determinado tipo de tarea *T*, este primer encuentro puede tener lugar en diferentes ocasiones, en función de los entornos matemáticos y didácticos que en ellos se produce: se puede volver a descubrir un tipo de tareas.
- El *segundo momento* es el de la exploración del tipo de tarea y de la elaboración de una técnica relativa a ese tipo de tareas. El estudio y la solución de un problema va siempre a la par de la construcción de un embrión de técnica, a partir del cual puede emerger una técnica más desarrollada.
- El *tercer momento* es el de la construcción de un entorno tecnológico-teórico relativo a la organización matemática, este momento está estrechamente relacionado con cada uno de los otros momentos. Desde el primer encuentro con un tipo de tareas generalmente se relaciona con un entorno tecnológico-teórico previamente elaborado, o con indicios de un entorno por crear que dará origen a una técnica emergente. En ocasiones el tercer momento se convierte en la primera etapa de estudio.
- El *cuarto momento* es el del trabajo de la técnica τ, que debe mejorar la técnica haciéndola más eficaz y fiable, y acrecentar el dominio que se tiene de ella.
- El *quinto momento* es el de la institucionalización, la cual constituye el cierre de una situación didáctica (Brousseau, 2007), tiene por objetivo definir la OM, distinguiendo aquellos elementos que no han de ser integrados y aquellos que formarán parte de la OM de manera definitiva.
- El *sexto momento* es el de la evaluación, el cual se articula con el momento de la institucionalización. En la práctica se llega a una etapa en la cual se debe reflexionar sobre el valor de lo que se aprendió.

Es posible presentar cada momento de manera no lineal en diversos tiempos y en repetidas ocasiones a lo largo del proceso de estudio, incluso pueden presentarse simultáneamente (Bosch et al., 2006).

Transposición didáctica y transposición informática

La *transposición didáctica* (Chevallard, 1991) sobre un medio informático conduce a una transformación del conocimiento que se pretende enseñar y aporta una nueva dimensión a los entornos de aprendizaje. Esto es parcialmente sensible en el campo de las matemáticas. Por lo tanto, es importante estudiar las consecuencias de esta transposición didáctica: esto lleva de hecho a la necesidad de explicar ciertos conte-

nidos didácticos que hasta entonces eran evidentes y, en ocasiones, incluso a la creación de nuevos contenidos didácticos. El desarrollo de las tecnologías informáticas, su introducción en las escuelas y lugares de formación se acompaña de fenómenos nuevos del mismo orden que los de la transposición didáctica.

Según Balacheff (1994) la *transposición informática* se entiende como las actividades sobre el conocimiento "que permiten una representación simbólica y la implementación de esa representación por un dispositivo informático". El dispositivo se descompone en tres medios:

- El universo interno, compuesto por diversos componentes electrónicos cuya articulación e implementación permiten el funcionamiento del dispositivo electrónico, se considera también a los lenguajes de programación que dan una representación operativa de este universo.
- La interfaz, lugar de comunicación entre el usuario humano y el dispositivo informático.
- El universo externo, en el que se encuentra el operador humano y donde tiene acceso a otros dispositivos si fuera necesario.

De acuerdo con García-Cuéllar (2018), la transposición informática se enfoca en reconocer las ventajas y limitaciones de los ambientes informáticos y en cómo el conocimiento es transformado por la utilización de dichos ambientes.

Así, la transformación del conocimiento es un problema esencial y plantea la cuestión de la validez de las representaciones, así como la de la coherencia y consistencia del sistema de enseñanza. También es importante determinar qué aprendizaje permite el sistema.

Metodología

Esta actividad de aprendizaje se compone de las siguientes etapas:

- *Diseño de la actividad*: se estructuró el procedimiento para la encriptación y desencriptación de información usando el cambio de base.
- *Desarrollo del programa*: se elaboró un programa en lenguaje Python para generar los ejercicios encriptados y leer las respuestas de los estudiantes.
- *Aplicación de la actividad a los estudiantes*: cada estudiante recibió un archivo de texto con un problema diferente para su resolución.
- *Revisión y análisis de los resultados*: se utilizó el programa para leer los archivos de texto que entregaron los estudiantes con sus respuestas, se analizaron las respuestas y sus procedimientos para determinar los posibles errores y retroalimentar al estudiante.
- *Segunda entrega*: los estudiantes realizaron la corrección del ejercicio.
- *Revisión y análisis de la segunda entrega*: se utilizó nuevamente el programa para evaluar las respuestas de los alumnos.

Revista Electrónica Científica de Investigación Educativa
Volumen 7, enero-diciembre 2023, e1792

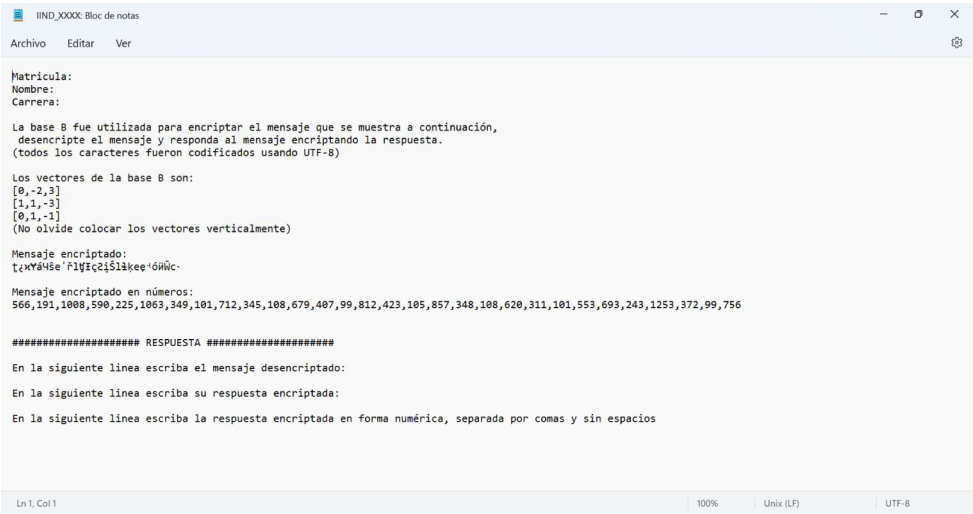
La actividad didáctica se aplicó a 46 estudiantes de las carreras de Ingeniería en Gestión Empresarial, Ingeniería en Diseño Industrial, Ingeniería Industrial e Ingeniería en Sistemas Computacionales, durante el periodo comprendido en los semestres agosto-diciembre 2021 y febrero-junio 2022.

La metodología de cifrado utilizada en la actividad es similar al método de Hill, descrito por Ibáñez (2017). Sin embargo, se optó por utilizar la codificación UTF-8 para cambiar cada carácter a un número, dado que dicha codificación tiene 1920 caracteres y evita operaciones adicionales al cambio de base. Este método de codificación puede considerarse una encriptación de llave privada, el emisor y el receptor deben conocer la llave para cifrar y descifrar el mensaje. En nuestro caso la llave privada son los vectores que constituyen una base B para $\mathbb{R}^3$, el emisor cambia los vectores de la base canónica a la base B utilizando la llave privada que son los vectores de la base para formar una matriz de transición que cifre el mensaje. De la misma manera el receptor utiliza los vectores de la base para construir una matriz de transición que cambie los vectores en términos de la base B a la base canónica.

Tomando como referencia la transposición informática, los autores diseñaron un programa en lenguaje Python para generar los ejercicios de aplicación que resolvieron los estudiantes, para ello, cada uno recibió un archivo de texto único como el que se muestra en la Figura 1.

A continuación se presenta la resolución del ejercicio aplicado siguiendo la metodología que el estudiante debería desarrollar, resolviendo el problema generado previamente por el programa desarrollado en Python, mostrado en la Figura 1.

Figura 1
Archivo de texto con problema de aplicación para el estudiante



Captura de pantalla del archivo proporcionado al estudiante.

Fuente: Construcción personal

El alumno debe:

1. Agrupar los números en ternas para formar los vectores en $\mathbb{R}^3$, obteniendo diez vectores que se encuentran escritos en términos de la base B.

$$\bar{x}_{1B} = \begin{pmatrix} 566 \\ 191 \\ 1008 \end{pmatrix}, \bar{x}_{2B} = \begin{pmatrix} 590 \\ 225 \\ 1063 \end{pmatrix}, \bar{x}_{3B} = \begin{pmatrix} 349 \\ 101 \\ 712 \end{pmatrix}, \bar{x}_{4B} = \begin{pmatrix} 345 \\ 108 \\ 679 \end{pmatrix},$$

$$\bar{x}_{5B} = \begin{pmatrix} 407 \\ 99 \\ 812 \end{pmatrix}, \bar{x}_{6B} = \begin{pmatrix} 423 \\ 105 \\ 857 \end{pmatrix}, \bar{x}_{7B} = \begin{pmatrix} 348 \\ 108 \\ 620 \end{pmatrix}, \bar{x}_{8B} = \begin{pmatrix} 311 \\ 101 \\ 553 \end{pmatrix},$$

$$\bar{x}_{9B} = \begin{pmatrix} 693 \\ 243 \\ 1253 \end{pmatrix}, \bar{x}_{10B} = \begin{pmatrix} 372 \\ 99 \\ 756 \end{pmatrix}.$$

2. Agrupar los vectores $\bar{v}_1$, $\bar{v}_2$ y $\bar{v}_3$ de la base en forma vertical para formar la matriz de transición de la base B a la base canónica $A_{B\to C}$.

$$\bar{v}_1 = \begin{pmatrix} 0 \\ -2 \\ 3 \end{pmatrix}, \ \bar{v}_2 = \begin{pmatrix} 1 \\ 1 \\ -3 \end{pmatrix}, \bar{v}_3 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$$

$$A_{B\to C} = \begin{pmatrix} 0 & 1 & 0 \\ -2 & 1 & 1 \\ 3 & -3 & -1 \end{pmatrix}$$

3. Multiplicar cada vector $\bar{x}_{iB}$ en términos de la base B por la matriz de transición $A_{B\to C}$ para cambiar dichos vectores a términos de la base canónica.

$$\bar{x}_1 = A_{B\to C} \cdot \bar{x}_{1B} = \begin{pmatrix} 0 & 1 & 0 \\ -2 & 1 & 1 \\ 3 & -3 & -1 \end{pmatrix} \begin{pmatrix} 566 \\ 191 \\ 1008 \end{pmatrix} = \begin{pmatrix} 191 \\ 67 \\ 117 \end{pmatrix}.$$

Al realizar la multiplicación de cada uno de los vectores del ejercicio por la matriz de transición, estos quedan de la siguiente manera:

$$\bar{x}_2 = \begin{pmatrix} 225 \\ 108 \\ 32 \end{pmatrix}, \bar{x}_3 = \begin{pmatrix} 101 \\ 115 \\ 32 \end{pmatrix}, \bar{x}_4 = \begin{pmatrix} 108 \\ 97 \\ 32 \end{pmatrix}, \bar{x}_5 = \begin{pmatrix} 99 \\ 97 \\ 112 \end{pmatrix}, \bar{x}_6 = \begin{pmatrix} 105 \\ 116 \\ 97 \end{pmatrix},$$

$$\bar{x}_7 = \begin{pmatrix} 108 \\ 32 \\ 100 \end{pmatrix}, \bar{x}_8 = \begin{pmatrix} 101 \\ 32 \\ 77 \end{pmatrix}, \bar{x}_9 = \begin{pmatrix} 243 \\ 110 \\ 97 \end{pmatrix}, \bar{x}_{10} = \begin{pmatrix} 99 \\ 111 \\ 63 \end{pmatrix}.$$

4. Desagrupar los vectores para crear una secuencia de números que contiene la pregunta:

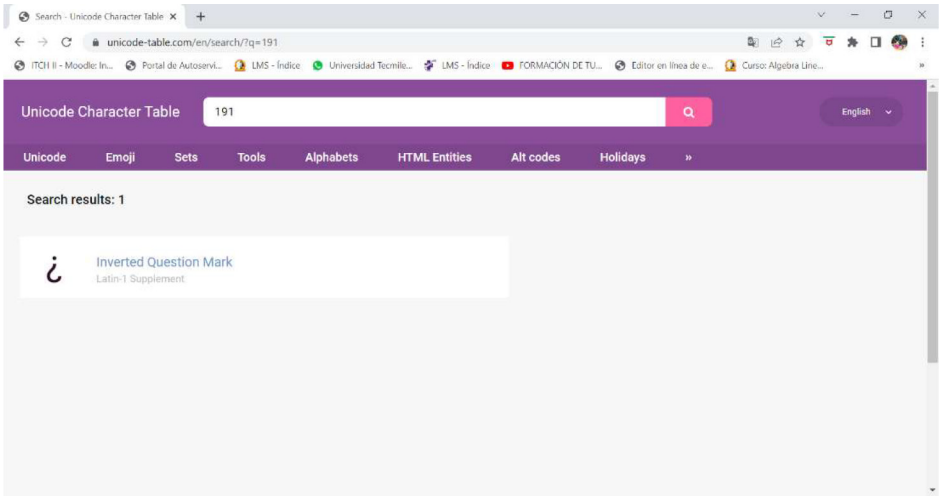
> 191,67,117,225,108,32,101,115,32,108,97,32,99,97,112,105,116,97,108,32,100,101,32,77,243,110,97,99,111,63

5. Utilizando la codificación UTF-8, convertir cada número de los vectores al carácter que le corresponde. El conjunto de caracteres formará la pregunta desencriptada. Para ello el estudiante utilizará la herramienta colocada en la página web https://unicode-table.com/ (*Unicode character table*, 2012), que recientemente fue sustituida por la página http://symbl.cc/ (Symbl, 2022),

Revista Electrónica Científica de Investigación Educativa
Volumen 7, enero-diciembre 2023, e1792

en la cual buscará los números de cada vector, obteniendo el carácter que le corresponde, como se muestra en la Figura 2.

Figura 2
Búsqueda en página Unicode table



Captura de pantalla de la página.

Fuente: unicode-table.com

De esta manera, cada número se convertirá en un carácter:

191 = ¿, 67 = C, 117 = u, 225 = á, 108 = l, 32 = espacio, 101 = e, 115 = s, 32 = espacio, 108 = l, 97 = a, 32 = espacio, 99 = c, 97 = a, 112 = p,105 = i, 116 = t, 97 = a, 108 = l, 32 = espacio, 100 = d, 101 = e, 32 = espacio, 77 = M, 243 = ó, 110 = n, 97 = a, 99 = c, 111 = o, 63 = ?

Revelando la pregunta: "¿Cuál es la capital de Mónaco?".

6. Responder a la pregunta y cambiar cada carácter de la respuesta al número que le corresponde según la codificación UTF-8, buscando el número en la página *Unicode character table* y anotando el carácter correspondiente.

   La respuesta a la pregunta sería:

   Ciudad de Mónaco

   Al cambiar cada carácter quedarían las siguientes cifras:

   67, 105, 117, 100, 97, 100, 32, 100, 101, 32, 77, 243, 100, 97, 99, 111

7. Agrupar los números en ternas para formar los vectores en $\mathbb{R}^3$. En caso de que el último vector tenga solo uno o dos números, agregará el número 32, que corresponde al espacio en blanco, para completar el vector.

$$\bar{y}_1 = \begin{pmatrix} 67 \\ 105 \\ 117 \end{pmatrix}, \ \bar{y}_2 = \begin{pmatrix} 100 \\ 97 \\ 100 \end{pmatrix}, \ \bar{y}_3 = \begin{pmatrix} 32 \\ 100 \\ 101 \end{pmatrix}, \ \bar{y}_4 = \begin{pmatrix} 32 \\ 77 \\ 243 \end{pmatrix}, \ \bar{y}_5 = \begin{pmatrix} 110 \\ 97 \\ 99 \end{pmatrix},$$

$$\bar{y}_6 = \begin{pmatrix} 111 \\ 32 \\ 32 \end{pmatrix}$$

8. Utilizar el método de la inversa de una matriz para obtener la matriz de transición de la base canónica a la base B, se sugiere el método de la adjunta para encontrar la matriz inversa.

$$A_{C\to B} = (A_{B\to C})^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ -2 & 1 & 1 \\ 3 & -3 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 3 \\ 1 & 0 & 2 \end{pmatrix}$$

9. Multiplicar cada vector por la matriz de transición de la base canónica a la base B, para encriptar la respuesta.

$$\bar{y}_{1B} = A_{C\to B} \cdot \bar{y}_1 = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 3 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 67 \\ 105 \\ 117 \end{pmatrix} = \begin{pmatrix} 356 \\ 67 \\ 750 \end{pmatrix}$$

Quedando los vectores de la siguiente manera:

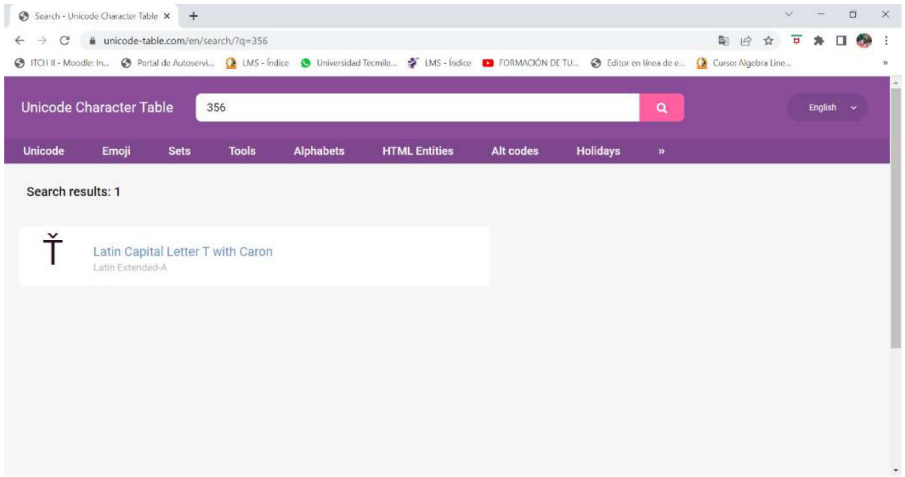
$$\bar{y}_{2B} = \begin{pmatrix} 397 \\ 100 \\ 791 \end{pmatrix}, \bar{y}_{3B} = \begin{pmatrix} 265 \\ 32 \\ 598 \end{pmatrix}, \bar{y}_{4B} = \begin{pmatrix} 384 \\ 32 \\ 813 \end{pmatrix}, \bar{y}_{5B} = \begin{pmatrix} 416 \\ 110 \\ 819 \end{pmatrix}, \bar{y}_{6B} = \begin{pmatrix} 286 \\ 111 \\ 493 \end{pmatrix}$$

10. Enlistar los componentes de los vectores.

356, 67, 750, 397, 100, 791, 256, 32, 598, 384, 32, 813, 416, 110, 819, 286, 111, 498

11. Nuevamente usando la codificación UTF-8 cambiará cada número a carácter, con la ayuda de la página web *Unicode character table*.

Figura 3
Conversión de números de la respuesta encriptada

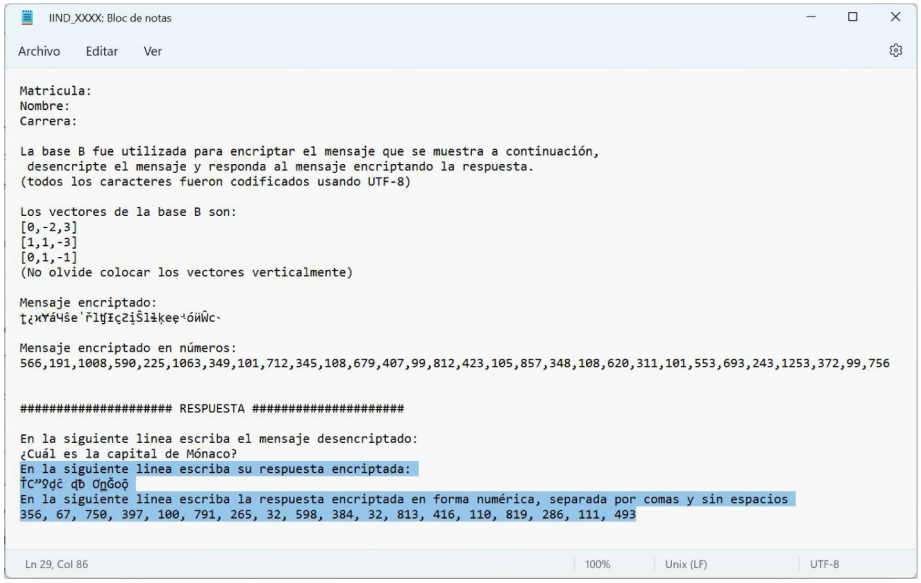


Captura de pantalla de la página.
Fuente: unicode-table.com

12. En el archivo de texto colocar los números y los caracteres de la respuesta encriptada como se muestra en la Figura 4.

Revista Electrónica Científica de Investigación Educativa
Volumen 7, enero-diciembre 2023, e1792

Figura 4
Archivo con respuestas



Captura de pantalla del archivo con respuestas.
Fuente: Construcción personal.

13. Entregar el archivo en formato electrónico incluyendo las fotografías de los procedimientos realizados en formato pdf o jpeg.

Una vez entregado el ejercicio, se formaliza la revisión utilizando el programa en lenguaje Pyhton para leer todos los archivos desencriptando las respuestas de los alumnos y creando un concentrado que permite al profesor evaluar los ejercicios de manera más directa. Se retroalimenta al alumno que no haya logrado completar correctamente el ejercicio indicando el o los pasos donde se encontraron errores y se le permite ejecutar una segunda entrega con las correcciones pertinentes; una vez entregado el ejercicio se vuelve a revisar para evaluar la comprensión y el desarrollo de este.

Resultados

Cuarenta y seis alumnos entregaron el ejercicio. Se encontraron diversos tipos de errores que se clasificaron en cinco categorías. La Tabla 1 muestra a los estudiantes que participaron por tipo de error.

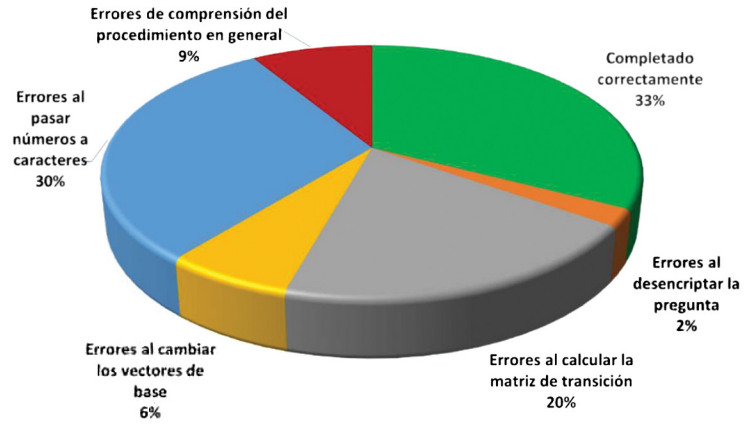
Tabla 1
Alumnos por tipo de error

Tipo de error	Número de alumnos
Desencriptar la pregunta	1
Calcular la matriz de transición	9
Cambiar los vectores de base	3
Pasar los números a carácter	14
Falta de comprensión del proceso en general	4

Fuente: Construcción personal.

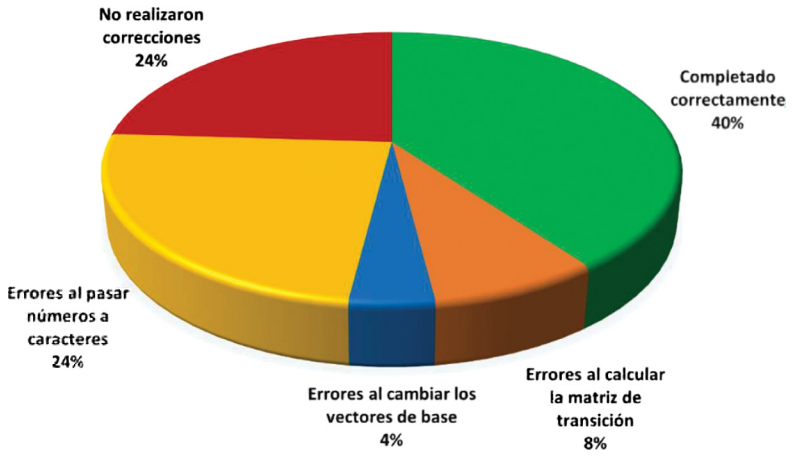
En la Figura 5 se muestra cómo se distribuyeron los ejercicios entregados por los estudiantes de acuerdo con el tipo de error.

Figura 5
Primera entrega de ejercicios clasificados por tipo de error



Fuente: Construcción personal.

Figura 6
Segunda entrega de ejercicios clasificados por tipo de error



Fuente: Construcción personal.

Una vez efectuada la primera revisión, se solicitó a los alumnos cuya actividad tenía algún error realizar las correcciones pertinentes. De estos, 25 entregaron nuevamente el ejercicio, de los cuales 6 no hicieron correcciones, 2 tuvieron errores al calcular la matriz de transición, 1 tuvo errores al cambiar los vectores de base y 6 presentaron errores al pasar los números a caracteres. En la Figura 6 se muestra la proporción de alumnos por cada tipo de error.

Durante el análisis de los datos se encontró que 25 estudiantes completaron el ejercicio correctamente, 15 en la primera entrega y 10 en la segunda, lo que representa el 54% del total. Si se agregan los 6 estudiantes que tuvieron errores al pasar de números a caracteres, dicha cifra alcanza el 67%, considerando que este tipo de error no refleja un problema en la comprensión de los temas de base y cambio de base.

De los 4 estudiantes que en la primera entrega mostraron poca o nula comprensión del procedimiento, uno de ellos no realizó la segunda entrega, 2 de ellos la entregaron sin hacer correcciones y uno la realizó terminando el ejercicio sin errores. Por lo tanto, solo tres estudiantes no lograron aplicar los conceptos de base y cambio de base en el ejercicio de encriptación, esto es el 6.5% del total.

De los 9 alumnos que tuvieron error en la matriz de transición en la primera entrega, en la segunda entrega 2 de ellos completaron correctamente el ejercicio, uno presentó el ejercicio sin correcciones, 5 no realizaron la segunda entrega, otro estudiante intentó hacer las correcciones sin lograr calcular la matriz de transición correctamente; por lo tanto, el 15% de los estudiantes no logró calcular correctamente la matriz de transición.

De los 3 estudiantes que tuvieron errores al cambiar los vectores de base, 2 de ellos realizaron las correcciones correspondientes en la segunda entrega, uno intentó hacer la corrección manteniendo algunos errores; por lo cual solo el 2% presentaron algunos errores al hacer el cambio de base después de realizar las correcciones.

Discusión y conclusiones

Las actividades dentro del proceso de estudio de base y cambio de base cuentan con seis momentos de estudio en el aula, es decir: cuando se aborda por primera vez la representación de un vector con respecto a una base usando la definición, *primer* y *tercer momento*; se exploran los problemas de cambio de base en diferentes espacios vectoriales, *segundo momento*; se establecen los procedimientos de resolución, *tercer momento*; se resuelven dichos problemas, *cuarto momento*; se evalúa la comprensión y se concluye o cierra el tema, *sexto* y *quinto momento*. Esta actividad retoma el *cuarto momento* de estudio, que es el trabajo de la técnica, y evalúa la comprensión del proceso de cambio de base, que es el *sexto momento*.

Al evaluar los resultados de los estudiantes se encuentra que los errores en la matriz de transición, o bien durante el cambio de base, son en su mayoría aritméticos. Se considera que los estudiantes con estos errores, así como los que completaron

correctamente el ejercicio, lograron aplicar los conceptos de base y cambio de base en un ejercicio de encriptación de datos, siendo en total el 93.5%, por lo cual se puede decir que los estudiantes sí lograron aplicar el concepto de cambio de base en la encriptación de la información.

Para dar respuesta a la pregunta de investigación "¿Cuáles son los errores más comunes durante el proceso?", los errores más comunes son aquellos relacionados con el cambio de números a caracteres y el cálculo de la matriz de transición.

Considerando los buenos resultados obtenidos en la actividad, es posible concluir que utilizar recursos fuera de la enseñanza típica de temas de naturaleza abstracta permite una mayor compresión y dominio de las técnicas, además genera interés en los estudiantes en diferentes disciplinas asociadas a la matemática.

Para futuras investigaciones se plantea llevar el programa de Python, utilizado para crear y revisar los problemas propuestos, a una plataforma web que permita la interacción directa con el estudiante, tal como lo sugiere Balacheff (1994) en la transposición informática.

Referencias

Álvarez, F., Costa, V., y Hernández-Suárez, C. (2021). Codificación de mensajes: actividad de estudio e investigación utilizando praxeologías de álgebra lineal. *Eco Matemático*, *12*(2), 37-53. https://doi.org/10.22463/17948231.3233

Balacheff, N. (1994). La transposition informatique, un nouveau problème pour la didactique. *Vingt ans de Didactique des Mathématiques en France*, *2*, 132-138. https://telearn.archives-ouvertes.fr/file/index/docid/190646/filename/Balacheff1994Transpo.pdf

Bosch, M., García, F., Gascón, J., y Ruiz, L. (2006). La modelización matemática y el problema de la articulación de la matemática escolar. Una propuesta desde la teoría antropológica de lo didáctico. *Educación Matemática*, *18*(2), 37-74.

Brousseau, G. (2007). *Iniciación al estudio de la teoría de las situaciones didácticas* (vol. 1). Libros del Zorzal. http://www.udesantiagovirtual.cl/moodle2/pluginfile.php?file=%2F204043%2Fmod_resource%2Fcontent%2F2%2F287885313-Guy-Brousseau-Iniciacion-al-estudio-de-la-teoria-de-las-situaciones-didacticas-pdf.pdf

Chevallard, Y. (1991). *La transposición didáctica. Del saber sabio al saber enseñado* (vol. 3).

Chevallard, Y. (1998). Analyse des pratiques enseignantes et didactique des mathématiques: l'approche anthropologique. En *Actes de l'UE de la Rochelle*, 91-118.

Chevallard, Y. (1999). L'analyse des pratiques enseignantes en théorie anthropologique du didactique. *Recherches en didactique des mathématiques (Revue)*, *19*(2), 221-265.

Dorier, J., y Sierpinska, A. (2001). Research into the teaching and learning. En *The teaching and learning of Mathematics at University level: An ICMI study* (pp. 255-273).

Fiarresga, V. (2010). Criptografia e matemática. En *Disertation*. Universidade de Lisboa Faculdade de Ciências.

García-Cuéllar, D. (2018). Enfoques teóricos en investigación con tecnología en educación matemática. *XXXI Acta Latinoamericana de Matemática Educativa*, *31*(2), 1402-1409. http://funes.uniandes.edu.co/13645/

Grossman, S., y Flores, J. (2012). *Álgebra lineal* (7a. ed.). McGraw-Hill.

Guzmán, J., y Zambrano, J. (2015). *Base de un espacio vectorial de Rn y tecnología*. XIV Conferencia Interamericana de Educación Matemática.

Hernández-Quintana, A. (2018). Evaluación del nivel de competencia en matemáticas básicas por parte de estudiantes de cálculo diferencial de nivel superior. En S. Cadena, C. Roldán, D. González, O. Rodriguez y C. Ruano (eds.), *Evaluación de aula, evaluación estandarizada y emergencia de sistemas de evaluación de aprendizajes* (pp. 31-45). Editorial Bonaventuriana/ Universidad Autónoma de Occidente.

Ibáñez, R. (2017). *Criptografía con matrices, el cifrado de Hill*. https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/

Madrid, H., Cribeiro, J., y Sánchez, M. (2016). Espacios vectoriales desde la realidad a la abstracción. *El Cálculo y su Enseñanza*, *7*(7), 1-8.

Parraguez, M., y Vera-Soria, G. (2020). Los modos de pensamiento sintético y analítico en la comprensión de base en el espacio vectorial R2: un estudio de casos en un contexto universitario. *Paradigma*, *41*, 600-365.

Stewart, S., y Thomas, M. (2010). Student learning of basis, span and linear independence in linear algebra. *International Journal of Mathematical Education in Science and Technology*, *41*(2), 173-188. https://doi.org/10.1080/00207390903399620

Symbl (2022). *Tabla de caracteres Unicode*. https://symbl.cc/es/unicode/table/

Valenzuela-González, V., Hernández-Quintana, A., y Camacho-Ríos, A. (2021). Level of competence on the concept of basis of vector space using SOLO taxonomy. *Journal Mathematical and Quantitative Methods*, *5*(8), 10-16. https://doi.org/10.35429/jmqm.2021.8.5.10.16

Vazquez, A. (2019). Una propuesta para la enseñanza del concepto abstracto de espacios vectoriales. *PädiUAQ*, *3*(6), 8-15.

Vera, M., y Miranda, E. (2014). El aprendizaje de los espacios vectoriales en ambientes computacionales. *Acta Latinoamericana de Matemática Educativa*, *27*, 2195-2203. http://funes.uniandes.edu.co/6189/1/GuadalupeELaprendizajeALME2014.pdf

Willems, W., y Gutierrez, I. (2010). *Una introducción a la criptografía de clave pública 2a* (2a ed.). Universidad del Norte.

Cómo citar este artículo:

Hernández-Quintana, A., Valenzuela González, V., y Camacho Ríos, A. (2023). Una propuesta didáctica para el cambio de base utilizando la encriptación de mensajes. *RECIE. Revista Electrónica Científica de Investigación Educativa*, *7*, e1792. https://doi.org/10.33010/recie.v7i0.1792