De los *bits* a los *qubits*: computación cuántica

Lorena Zúñiga Segura*
lzuniga@itcr.ac.cr
lorena.zuniga@gmail.com

El concepto de computación cuántica arranca en 1981, cuando el físico Richard Feyman se pregunta si sería posible simular la física en una computadora de la época y propone un modelo básico para una computadora que pudiera simular procesos cuánticos.

Esto representó un desafío para los científicos de la computación: crear un nuevo tipo de computadora, cuya base fuera la física cuántica, a diferencia de las computadoras clásicas, cuyos circuitos siguen las leyes de la física clásica, según las cuales solo pueden estar en un estado a la vez. A partir de entonces, surgieron diferentes esfuerzos para tratar de imaginar cómo sería esa computadora, qué tipo de problemas podría resolver y cómo podría ser construida.

Alrededor de 1985, David Deutsch describe la primera computadora cuántica universal y durante muchos años los avances y conceptos que fueron surgiendo permanecieron como cuestiones teóricas. Fue en 1990 cuando se dieron las primeras experimentaciones prácticas.

Unido a lo anterior, para los científicos los límites de la computación han sido un tema de preocupación, en el sentido de que cada vez más se reduce el tamaño de la circuitería incluida en los chips de silicio, de tal forma que en algún momento estos componentes llegarían a ser del tamaño de unos cuantos átomos.

De los *bits* a los *qubits*

Las computadoras que conocemos y utilizamos en nuestra vida diaria trabajan con unidades básicas llamadas *bits*; cada una de estas puede tener el valor 0 o el valor 1 únicamente y dichos valores no pueden ser representados simultáneamente, es decir, un bit en un momento dado solo puede representar uno de los dos. Por su parte, las computadoras cuánticas trabajan con unidades llamadas *qubits* (bits cuánticos), que pueden tomar el valor 0 o el valor 1, o cualquier combinación de esos valores de manera simultánea; en otras palabras, pueden tener o representar más de un valor al mismo tiempo. Esto plantea la posibilidad de procesar muchísima más información de la que sería posible con una computadora convencional.

Los *qubits*, para retener información y así ser de utilidad, deben cumplir con dos propiedades muy importantes llamadas *superposición y entrelazado cuántico*. La primera se refiere al hecho de que el *qubit* puede tomar más de un valor al mismo tiempo, lo que haría posible que con la misma cantidad de bits (o de *qubits* en este caso) se almacene más información simultáneamente. Por ejemplo, en la actualidad una computadora clásica con 3 *bits* puede representar ocho posibles estados o valores diferentes, pero solo uno a la vez; mientras que la computadora cuántica podría representar los ocho estados o valores al mismo tiempo, es decir, en lugar de tener solo uno de los posibles ocho valores, podría tener todos a la vez.

El entrelazado cuántico está relacionado con la propiedad cuántica según la cual una molécula (en este caso un *qubit*) está íntimamente entrelazada con otra, de tal forma que aún cuando estén separadas se pueden afectar entre sí, sin importar la distancia que las separe. De esta manera es posible formar grupos de *qubits* y manipularlos a la vez, como si fueran uno. Estas propiedades son precisamente las que le permiten a una computadora cuántica manejar inmensas cantidades de información al mismo tiempo, haciéndolas muy poderosas en lo que a procesamiento de información se refiere.

Según lo anterior, es claro que al incrementarse la cantidad de qubits aumentará casi exponencialmente la cantidad de estados o valores que la computadora puede representar.

Además de la cantidad de información que se puede representar y procesar, un aspecto de gran importancia es la velocidad de ejecución. Según datos de *The Economist*, para un algoritmo de búsqueda simple en un conjunto de datos no ordenados, una computadora común podría requerir hasta un máximo de N intentos para encontrar el dato requerido (siendo N la cantidad total de elementos o datos), mientras que una computadora cuántica podría hacerlo en una cantidad de intentos igual a la raíz cuadrada de N (The Economist, 2016). De acuerdo con lo anterior, si el conjunto de datos tiene 70 elementos, la computadora común haría un máximo de 70 intentos hasta encontrar el dato deseado, frente a unos ocho intentos aproximadamente de la computadora cuántica.

Es importante aclarar que las computadoras cuánticas generan respuestas probabilísticas, es decir, que dado un resultado, este tiene asociada cierta probabilidad de ser correcto.

Limitantes

Una problemática que presentan los *qubits* es que son sumamente inestables; cualquier interferencia, por mínima que sea, por ejemplo vibraciones, una variación en la temperatura o una onda electromagnética, y prácticamente cualquier interacción con el exterior, hace que pierdan su información, generando así resultados incorrectos. Además, el chip debe estar en un ambiente especialmente frío.

Debido a esto, una computadora cuántica no puede ser ubicada en cualquier lugar, sino que requiere de condiciones especiales con el

fin de contar con altos niveles de aislamiento y las condiciones de enfriamiento que requiere para funcionar adecuadamente.

Esta inestabilidad de los *qubits* y las condiciones de ambiente que necesitan son las principales limitantes para la implementación a gran escala de este tipo de computadoras.

Posibles usos

Aunque en la actualidad aún no tienen un uso práctico, expertos alrededor del mundo prevén que tendrán un gran impacto prácticamente en todas las áreas del quehacer humano, e inclusive prevén que la computación cuántica podría eventualmente crear nuevas industrias. Sin embargo, mientras su desarrollo se va afianzando, dentro del conjunto de aplicaciones visualizadas como las más inmediatas se puede mencionar las siguientes:

• **Criptografía y seguridad:** en este campo se ve tanto una amenaza como una oportunidad. En cuanto a la primera, se tiene que los algoritmos criptográficos en general, por ejemplo el RSA[1] , se basan en lo difícil que resulta factorizar números grandes, aún con una computadora de alto poder. Una computadora cuántica eventualmente podría quebrar con facilidad estos algoritmos, amenazando así las técnicas de encriptación utilizadas mundialmente. Por otro lado, se piensa que la computación cuántica generará un tipo de criptografía de alta seguridad al poder aplicar técnicas como la *distribución de claves cuánticas* (QKD, por sus siglas en inglés), mediante la cual, si alguien intercepta un mensaje cifrado con una de estas claves, perturbará el sistema y no podrá obtener la información; a la vez, tanto el receptor como el emisor se darán cuenta de que ha habido un problema, por lo que el sistema continuaría emitiendo nuevas llaves hasta que estas coincidan plenamente para el receptor y el emisor. En este campo se espera la codificación de señales mediante el uso de partículas superpuestas, de tal forma que no se puedan interceptar ni duplicar. Al parecer China ya logró lanzar un satélite que es capaz de recibir y enrutar señales de ese tipo *(The Economist)*.

• **Simulación de sistemas cuánticos:** se espera poder simular las interacciones simultáneas entre átomos y moléculas inclusive en condiciones inusuales. Por ejemplo, se podrían simular las reacciones químicas, debido a que la interacción entre átomos es un proceso cuántico (Ambainis, 2014). Esto eventualmente podría llevar al desarrollo de nuevos materiales y nuevos fármacos.

• **Optimización:** esta es otra área en la cual las computadoras cuánticas podrían ser de gran utilidad, al poder evaluar de manera muy rápida múltiples soluciones y encontrar la mejor. Podría aplicarse en áreas como la logística y la gestión de la cadena de abastecimiento de las organizaciones, optimizando tiempos de entrega de materias primas, insumos y productos terminados.

• Búsquedas en grandes volúmenes de datos.

• Análisis de grandes volúmenes de información y ejecución de pruebas complejas, que son difíciles de realizar con las computadoras tradicionales; por ejemplo análisis de genomas y mapeo de proteínas; eventualmente podría llevar a comprender mejor el desarrollo de ciertas enfermedades y posibles formas de contrarrestar su avance; análisis de datos recopilados por los telescopios; análisis de datos sobre tráfico aéreo y terrestre para de reducir tiempos de viaje; así como testing de sofware para aviones, a fin de incrementar la seguridad de las aeronaves.

Tipos de computadoras cuánticas

Según IBM Research, existen tres tipos de computadoras cuánticas, las cuales varían en cuanto a la complejidad de su construcción, su poder computacional y el tipo de aplicaciones a las que están orientadas.

La de menor complejidad es la llamada computadora de *recocido cuántico (quantum annealer)*, la más fácil de construir y la que cuenta con menor poder computacional; esto implica que solo puede ejecutar un tipo de función o algoritmo, por lo general orientada a problemas de optimización. Se ha considerado que no representa realmente una gran diferencia comparada con una computadora tradicional.

Luego está la computadora cuántica analógica, que tendría un alto poder computacional. Se piensa que podría poseer entre 50 y 100 *qubits* y estaría en capacidad de ejecutar simulaciones de interacciones cuánticas. En consecuencia, su orientación apunta hacia aplicaciones en áreas como ciencia de materiales, química y problemas de optimización, entre otros.

Finalmente está la computadora cuántica universal, que viene a ser la más poderosa de las tres, siendo también la de mayor dificultad de construcción. Se considera que podría tener alrededor de 100 000 qubits y sus áreas de aplicación serían las de las otras computadoras antes mencionadas, más la criptografía y el aprendizaje automático *(machine learning)*.

Desarrollos e implementaciones actuales

En el año 2011 la compañía DWave dio a conocer la construcción de una computadora cuántica llamada DWave 1 y posteriormente, en el 2013, crearon la DWave2. Podría decirse que es la única computadora cuántica que se encuentra comercialmente disponible, aunque no de forma masiva, pues solo han fabricado unas pocas unidades. Cabe mencionar que como parte de los clientes y patrocinadores de esta empresa se encuentran Google, Lockheed, la NASA, la CIA y Jeff Bezos (CEO de Amazon.com), que incluso adquirieron algunas de las pocas unidades de la DWave disponibles para la venta. Sin embargo, alrededor de esta computadora se ha generado mucha polémica e incluso algunos expertos señalan que no se trata de una verdadera computadora cuántica, ya que sus qubits, aunque se demostró que están entrelazados, no se ha logrado verificar que logren la superposición al ejecutar un algoritmo. Además, en algunas mediciones de desempeño al parecer no logró superar a una computadora normal, mientras que en otras pruebas, si bien excedió a las actuales computadoras, no lo hizo en una magnitud similar a lo que se esperaría de una computadora cuántica. La empresa por su parte, superó la controversia al indicar que se trata de una computadora cuántica de *recocido cuántico*, que como se describió anteriormente, vendría a ser de las más básicas.

A la fecha, diversas universidades alrededor del mundo tales como la Delft University of Technology, la Universidad de Innsbruck (Austria), Universidad de California, Universidad de Maryland, Duke University, University of New South Wales y el Joint Quantum Institute, entre otros, han logrado crear pequeños sistemas cuánticos, entre los 14 y los 20 qubits aproximadamente. Estas insti-

1 RSA, algoritmo de encripción que lleva ese nombre por el apellido de sus creadores: R. Rivest, A. Shamir y L. Adleman.

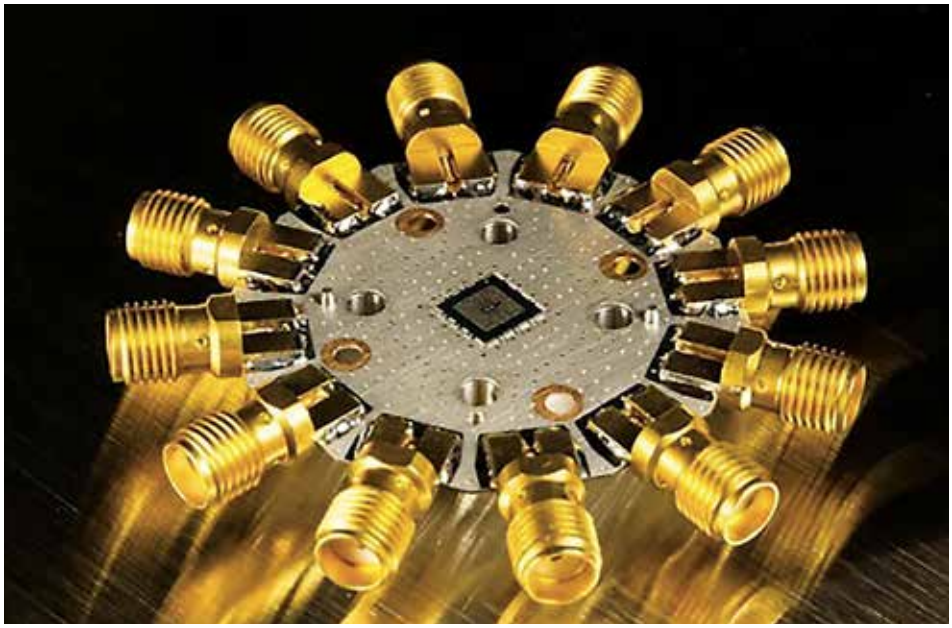


Figura 2. Computadora cuántica diseñada por la IBM.

tuciones no solo trabajan e investigan para crear sistemas cuánticos, sino también para lograr formas de estabilizarlos, de tal manera que se invierta cada vez menos tiempo en corregir los errores generados por la inestabilidad propia del sistema. Paralelo a esto, grandes empresas del mundo de la tecnología de información, entre las que encontramos a líderes como Intel, IBM, Hewlett-Packard, Google y Microsoft, han creado sus propios laboratorios y equipos de investigación dedicados a este tema. Así, experimentan con tecnologías que les permitirían en un corto plazo construir una computadora cuántica universal que pueda ser utilizada fuera de entornos de experimentación.

Según los expertos, las computadoras cuánticas se pueden construir a partir de fotones, electrones, iones o moléculas, así como materiales superconductores, entre otros. Además, requieren de temperaturas extremadamente bajas. Así, por ejemplo, el procesador de 5 *qubits* de la IBM está construido en un chip a partir de rizos de un metal superconductor, que reposa en el fondo de un refrigerador de helio. Para programar el chip se transmiten dosis de microondas al refrigerador, de tal forma que cada qubit responderá a una frecuencia distinta. En el caso de la D-Wawe2, se trata de una caja de cerca de 3 m de alto, que contiene un sistema de enfriamiento para mantener el chip a una temperatura cercana a los 20 mili-kelvins, aproximadamente unos -273º Celsius (Grossman, 2014).

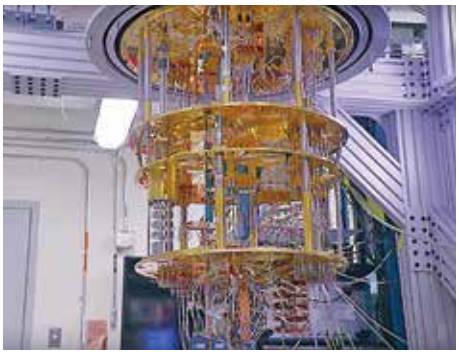


Figura 2. Computadora cuántica diseñada por la IBM.

Hoy por hoy las computadoras cuánticas no están disponibles comercialmente; de momento continúan siendo mayoritariamente prototipos de laboratorio. Sin embargo, expertos que trabajan en el área han expresado que en pocos años podrían verse las primeras computadoras a nivel comercial. Por ejemplo, la división Q de IBM, encargada de desarrollar computadoras cuánticas para su uso en negocios y ciencia, estima que en pocos años sería posible contar con este tipo de dispositivos, con una capacidad de unos 50 *qubits*. Por su parte, en Google han estimado que en cinco años ya las empresas podrían generar beneficios a partir de elementos de computación cuántica (Beall, 2017).

Software y programadores

Con el fin de difundir más estos conceptos, varias empresas han puesto a disposición del público software para la construcción de algoritmos cuánticos; por ejemplo, Google creó el *Quantum Computing Playgraoud* y DWave liberó bajo licencias de código abierto dos de sus herramientas de software para algoritmos cuánticos: Qasm y Qbsolv; estas herramientas sirven para programar las computadoras cuánticas de dicha empresa. Además, en mayo de este año IBM puso a disposición del público un servicio llamado *Quantum Experience*, mediante el cual ofrece una computadora cuántica de 5 *qubits* conectada a Internet. En este caso, se brindaría un servicio de pago por suscripción para empresas que deseen utilizar una computadora cuántica a través de la IMB Cloud. De momento, para propósitos académicos y de experimentación el servicio es gratuito.

Como ejemplo, en la siguiente figura se observa el llamado *Quantum Composer*, que es básicamente un editor o interfaz gráfica mediante la cual se pueden escribir algoritmos cuánticos usando compuertas y medidas que ya se encuentran definidas en una biblioteca; a grandes rasgos, se trata de operaciones que hacen cambiar el estado de los *qubits.* Para programar el algoritmo o circuito, basta con seleccionar y arrastrar al editor los controles que representan cada una de las compuertas y operaciones.

El *Composer* permite a quien lo utiliza elegir si su algoritmo (o experimento) será ejecutado sobre un procesador cuántico real o simulado; en este último caso es posible especificar la cantidad de *qubits* que tendrá el procesador. En la figura previa se observa un circuito cuántico de 4 *qubits*. Una vez construido el algoritmo se puede ejecutar o simular y ver los resultados.

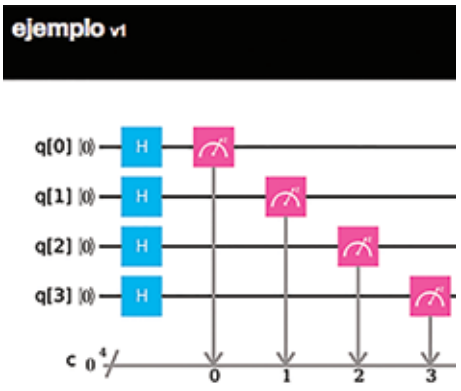
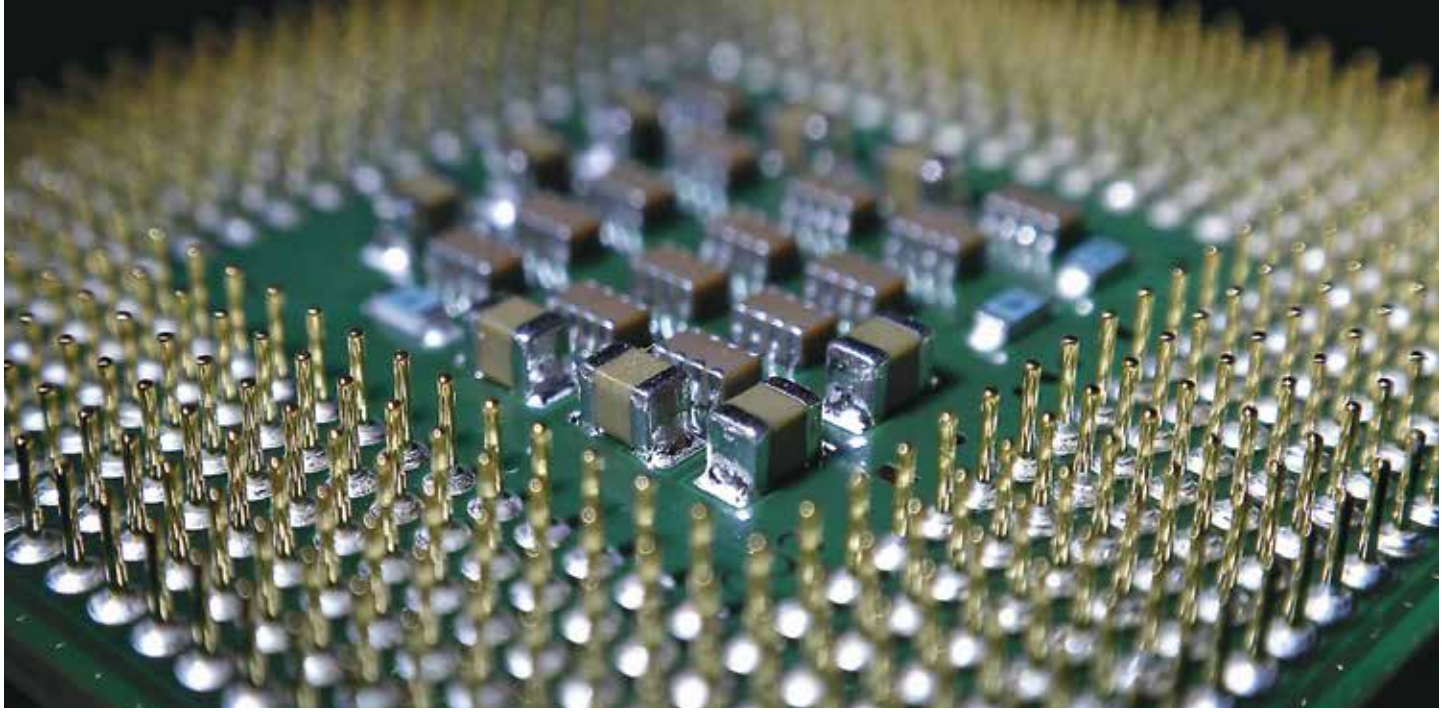


Figura 3. Ejemplo de un circuito cuántico. Elaboración propia en el Composer de IBM.



Además de la construcción de una computadora cuántica universal, otro de los desafíos que se ve en el horizonte es la disponibilidad de personal calificado que pueda programar las computadoras cuánticas, algo que de entrada se considera mucho más difícil que generar programas para una computadora tradicional. Quienes diseñen estos algoritmos deben contar con un entendimiento básico de física cuántica. Además, al no existir computadoras cuánticas comerciales cuyos beneficios sean ya visibles, se vuelve dificultoso que un programador por su propio interés esté dispuesto a dedicar las horas que requeriría aprender y adquirir los conocimientos necesarios para crear algoritmos cuánticos (Gent, 2017).

Así como en los ochentas surgieron las primeras computadoras personales, con un poder computacional que ahora parece extremadamente limitado, es muy probable que a pesar de los desafíos, dentro de cinco años o más veamos las primeras computadoras cuánticas de uso comercial y con ello vendrá también la necesidad de aprender y luego enseñar a otros a programar algoritmos cuánticos.

Referencias

Ambainis, A. (2014). What Can We Do with a Quantum Computer? Institute for Advanced Study. Recuperado en https://www.ias.edu/ideas/2014/ambainis-quantum-computing

Beall, A. (2017). Inside the weird world of quantum computers. WIRED. Recuperado en http://www.wired.co.uk/article/quantum-computing-explained

Gent, E. (2017). Quantum Computing Demands a Whole New Kind of Programmer. SingularityHub. Recuperado en https://singularityhub.com/2017/05/09/quantum-computing-demands-a-whole-new-kind-of-programmer/

Google. (2017). Google's chip ready for testing. [Figura]. Recuperado en https://www.technologyreview.com/s/604242/googles-new-chip-is-a-stepping-stone-to-quantum-computing-supremacy/

Google Quantum Computing Playground http://www.quantumplayground.net/#/home

Grossman, L. (2014). The quantum quest for a Revolutionary Computer. Time. Recuperado en http://content.time.com/time/subscriber/article/0,33009,2164806,00.html

IBM Quantum Lab https://www.research.ibm.com/ibm-q/learn/

IBM Q Experience. https://quantumexperience.ng.bluemix.net/qx/editor

IBM Q Experience User Guide. https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=b03bd3750e9b05822d31f4d9ffb097ba&pageIndex=0

Institute for Quantum Computing. (s.f.). Quantum computing 101. University of Waterloo. Recuperado en https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

Narvey, J. (2017). D-Wave open sources software tool to build foundation for a quantum computing community. Betakit. Recuperado en http://betakit.com/d-wave-open-sources-software-tool-to-build-foundation-for-a-quantum-computing-community/

Satell, G. (2016). Here's How Quantum Computing will Change the World. Forbes. Recuperado en https://www.forbes.com/sites/gregsatell/2016/10/02/heres-how-quantum-computing-will-change-the-world/#7e17ba28ad6d

The Economist. (2016). Quantum Computing. Now try this. Recuperado en http://www.economist.com/news/science-and-technology/21698234-ibm-making-quantum-computer-available-anyone-play-now-try

The Economist. (2017). Subatomic opportunities Quantum leaps. Recuperado en http://www.economist.com/news/leaders/21718503-strangeness-quantum-realm-opens-up-exciting-new-technological-possibilities-quantum

Vella, M. (2014). 9 Ways Quantum Computing Will Change Everything. Time. Recuperado en http://time.com/5035/9-ways-quantum-computing-will-change-everything/

Wadler, D. (2016). IBM Gives Public Cloud Access to New 5-Qubit Quantum Computer. [Figura]. Recuperado en https://www.allaboutcircuits.com/news/quantum-composer-ibm-5-qubit-quantum-computer-cloud/

*Ingeniera en computación, profesora de la carrera de Administración de Tecnologías de Información (ATI) del TEC. Tiene un doctorado en Ciencias de la Administración y una maestría en Administración de Negocios con énfasis en Dirección Empresarial. Ha trabajado como analista de sistemas, investigadora y docente en diferentes universidades públicas y privadas.