Yolanda Blanco · Manuel Fernández Veiga · Ana Fernández Vilas · José M. de Fuentes (eds.)

Jornadas Nacionales de Investigación en Ciberseguridad

JNIC2023

ACTAS DE LAS VIII JORNADAS NACIONALES DE INVESTIGACIÓN EN CIBERSEGURIDAD

Vigo, 21 a 23 de junio de 2023

ISBN: 978-84-8158-970-2

gradiant

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

atlanTTic
Universidade Vigo

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Patrocinadores

Patrocinio técnico

Comités técnicos

Comité de programa científico

Manuel Fernández Veiga	atlanTTic, UVigo
José María de Fuentes	Universidad Carlos III de Madrid
Lilian Adkinson	GRADIANT
Cristina Alcaraz	Universidad de Málaga
Ana Ayerbe	TECNALIA
Marta Beltrán	Universidad Rey Juan Carlos
Carlos Blanco	Universidad de Cantabria
Jorge Blasco	Universidad Politécnica de Madrid
Pino Caballero	Universidad de La Laguna
Agustín Cañas	GRADIANT
Andrés Caro	Universidad de Extremadura
Jesús Esteban Díaz	Universidad de Granada
Josep Lluís Ferrer	Universitat de les Illes Balears
Joaquín García-Alfaro	Telecom-Sud Paris
David García	Universidad de Castilla-La Mancha
Luis Javier García	Universidad Complutense de Madrid
Manuel Gil	Universidad de Murcia
Félix Gómez	Universidad de Murcia
Lorena González	Universidad Carlos III de Madrid
Luis Hernández	CSIC
Javier López	Universidad de Málaga
Jorge López	Verisure
Agustín Martín	CSIC
Gregorio Martínez	Universidad de Murcia
David Megías	Universitat Oberta de Catalunya
Pantaleón Nespoli	Universidad de Murcia
Francisco J. Nóvoa	Universidade da Coruña
Raúl Orduña	VICOMTECH
Inés Ortega	GRADIANT
Luis Panizo	Universidad de León
Aljosa Pasic	ATOS
Luis Pérez Freire	GRADIANT
Fernando Pérez González	atlanTTic y Universidade de Vigo
Cristina Regueiro	TECNALIA
Erkuden Ríos	TECNALIA
Margarita Robles	Universidad de Granada
Ricardo J. Rodríguez	Universidad de Zaragoza
Luis E. Sánchez	Universidad de Castilla-La Mancha
Miquel Soriano	Universitat Politécnica de Catalunya
Juan Ramón Troncoso	Tuneinsight
Narseo Vallina	IMDEA
José M. Vázquez-Naya	Universidade da Coruña
Víctor Villagrá	Universidad Politécnica de Madrid
Urko Zurutuza	Mondragón Unibertsitatea

Comité del programa de transferencia

Yolanda Blanco Fernández	atlanTTic y UVigo
Juan González Martínez	GRADIANT
Ana Ayerbe	TECANALIA
Javier Sedano	ICTL
Gregorio Martínez	U. Murcia
Urko Zurutuza	U. Mondragón
Raúl Orduña	VICOMTECH
Jordi Guijarro	I2CAT
Juan Díez	INCIBE
Pino Caballero	U. de La Laguna
David Pérez	FUNDITEC
Cristina Alcaraz	U. Málaga
Felipe Gil	U. Vigo
Juan Caubet	EURECAT
Marta Fuentes	FIDESOL
Marc Barceló	IKERLAN
Aitor Urbieta	IKERLAN
Víctor Carneiro	U. da Coruña

Comité del programa de formación

Yolanda Blanco Fernández	atlanTTic y UVigo
José Carlos Sancho Núñez	Universidad de Extremadura
José Carlos Sancho Núñez	Universidad de Extremadura
Noemí De Castro García	Universidad de León
Adriana Suárez Corona	Universidad de León
Isaac Agudo Ruiz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Mar Ávila Vegas	Universidad de Extremadura
Xavier Larriva	Universidad Politécnica de Madrid
David García Rosado	Universidad de Castilla – La Mancha
Óscar Mogollón Gutiérrez	Universidad de Extremadura
Ángel Jesús Varela Vaca	Universidad de Sevilla
Roberto Magán Carrión	Universidad de Granada
Raquel Poy Castro	Universidad de León
Javier Corral García	CénitS – COMPUTAEX
Sara García Bécares	INCIBE – Responsable de Talento en Ciberseguridad
Victoria Alicia Marcos Sbarbaro	INCIBE – Técnico de Talento en Ciberseguridad
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid

Índice general

Conferencias invitadas

Mesas Redondas

Programa científico

Sesión I: Seguridad en entornos distribuidos

Sesión II: Inteligencia artificial y ciberseguridad I

Sesión III: Técnicas de ciberseguridad y ciencia forense I

Sesión IV: Transferencia I

Sesión V: Transferencia II

Sesión VI: Técnicas de ciberseguridad y ciencia forense II

Sesión VII: Inteligencia artificial y ciberseguridad II

Sesión VIII: Gestión avanzada de riesgos y seguridad

Sesión IX: Criptografía en la era cuántica

Sesión X: Innovación educativa

Programa científico: pósters

Sesión I: Investigación publicada I

Sesión II: Investigación publicada II

Sesión III: Investigación original I

Sesión IV: Investigación original II

Sesión V: Investigación original III

Call for Flags

Retos CFF

Premios RENIC a la mejor tesis doctoral y el mejor trabajo de fin de máster

Minimización del tiempo de respuesta a incidentes en entornos reales usando computación cuántica

Manuel A. Serrano
Univ. de Castilla-La Mancha
Ciudad Real, España
Manuel.Serrano@uclm.es

Luis E. Sánchez
Univ. de Castilla-La Mancha
Ciudad Real, España
LuisE.Sanchez@uclm.es

Antonio Santos-Olmo
Univ. de Castilla-La Mancha
Ciudad Real, España
Antonio.SantosOlmo@uclm.es

David G. Rosado
Univ. de Castilla-La Mancha
Ciudad Real, España
David.GRosado@uclm.es

Carlos Blanco
Universidad de Cantabria
Santander, España
Carlos.Blanco@unican.es

Vita Santa Barletta
Università di Bari
Bari, Italia
vita.barletta@uniba.it

Danilo Caivano
Università di Bari
Bari, Italia
danilo.caivano@uniba.it

Eduardo Fernández-Medina
Univ. de Castilla-La Mancha
Ciudad Real, España
Eduardo.FdezMedina@uclm.es

***Resumen*—Los Sistemas de Gestión de la Seguridad de la Información (SGSI) son procesos globales, orientados al riesgo que permiten a las empresas desarrollar su estrategia de ciberseguridad mediante la definición de políticas de seguridad, activos de valor, controles y tecnologías para proteger sus sistemas e información de amenazas y vulnerabilidades. A pesar de la implantación de estas infraestructuras de gestión, se producen incidentes de seguridad. Cada incidente lleva asociado un nivel de gravedad y un conjunto de controles de mitigación, por lo que para restaurar el SGSI hay que seleccionar el conjunto de controles adecuado para mitigar sus daños. El tiempo en el que se restaura el SGSI es un aspecto crítico. En este sentido, las soluciones clásicas son eficientes para resolver escenarios con un número moderado de incidentes en un tiempo razonable, pero el tiempo de respuesta aumenta exponencialmente a medida que se incrementa el número de incidentes. Esto hace que las soluciones clásicas no sean adecuadas para escenarios reales en los que se gestiona un gran número de incidentes y menos aún para escenarios en los que la gestión de la seguridad se ofrece como servicio a varias empresas. Este trabajo propone una solución al problema de respuesta a incidentes que actúa en un tiempo mínimo para escenarios reales en los que se gestiona un gran número de incidentes. Se aplica la computación cuántica, como enfoque novedoso que se está aplicando con éxito a problemas reales, que permite obtener soluciones en un tiempo constante independientemente del número de incidentes gestionados. Para validar la aplicabilidad y eficiencia de nuestra propuesta, se ha aplicado a casos reales utilizando nuestro framework (MARISMA).**

***Index Terms*—Gestión de riesgos, Programación cuántica, Respuesta a incidentes**

Tipo de contribución: *Investigación original*

I. Introducción

Conceptos como ciberseguridad y ciberdefensa están cada vez más presentes en una sociedad dominada por la tecnología digital [1]. De hecho, en un mundo en constante cambio, donde la digitalización alcanza todos los ámbitos, los problemas de ciberseguridad son una de las principales amenazas para la privacidad de las personas, la sostenibilidad de las empresas y la protección de sus activos [2]. Algunos autores destacan que las organizaciones tienen que hacer frente a un mayor riesgo debido a las amenazas lo que compromete su propia supervivencia [3]. En este contexto, los datos y los sistemas de información son activos críticos que deben ser adecuadamente protegidos [4], [5], pero no deja de ser un objetivo complejo de cumplir [6], que requiere un claro compromiso y concienciación por parte de las organizaciones [7], [8] y unos recursos personales y económicos que en la mayoría de los casos no están disponibles [9].

En la actualidad, las soluciones de evaluación y gestión de riesgos presentan numerosas cuestiones pendientes que complican su aplicabilidad y eficacia. En primer lugar, la mayoría de los incidentes de seguridad se deben al desconocimiento general de los riesgos o a su evaluación inexacta [10]. Además, el estado natural de los riesgos es dinámico, ya que están relacionados con amenazas y vulnerabilidades en constante evolución, pero lamentablemente los enfoques dominantes ofrecen una imagen estática de los riesgos [11]. Además, los métodos de evaluación de riesgos existentes dependen en gran medida de la experiencia de los expertos en riesgos, por lo que se necesitan nuevos métodos que exploten la reutilización de los conocimientos para ofrecer una gestión de riesgos eficaz y objetiva y limitar los costes asumidos [12]. En este escenario, los incidentes de ciberseguridad van en aumento, tanto en intensidad como en impacto [13], por lo que la comunidad científica reclama el desarrollo de metodologías y herramientas adecuadas que permitan a las empresas abordar, conocer y gestionar su riesgo de ciberseguridad, mejorando sus actuales inconvenientes

Sin embargo, el objetivo de este trabajo es tratar de contribuir a la resolución de un problema concreto de respuesta a incidentes de seguridad, que es un aspecto fundamental del Sistema de Gestión de la Seguridad de la Información (SGSI) y en particular forma parte de la gestión de riesgos, y que se encarga de reaccionar ante los incidentes aplicando controles para reducir los daños y restaurar eficientemente los sistemas [14]. El problema que abordamos es cómo encontrar y seleccionar el conjunto mínimo de incidentes que debemos acometer para resolver todos los incidentes existentes en un periodo de tiempo determinado, teniendo en cuenta la severidad de los mismos y el conjunto de controles que se han visto afectados por ellos. Este es un problema de optimización que se resuelve fácilmente con algoritmos tradicionales cuando el número de incidencias y controles asociados es pequeño, pero a medida que el número de incidencias aumenta, el problema se hace irresoluble desde una perspectiva tradicional,

ISBN:978-84-8158-970-2

ya que la complejidad del algoritmo es exponencial y por tanto, debemos buscar otras aproximaciones. En este artículo exploramos otro paradigma para resolver este problema, los algoritmos cuánticos.

Aunque la computación cuántica se encuentra en sus fases más incipientes, ya está lista para su uso industrial, lo que la convierte en una candidata de primer orden para resolver cierto tipo de problemas de gran complejidad para los que incluso los superordenadores están fallando. Este nuevo paradigma ya se está aplicando para resolver ciertos tipos de problemas para los que dicho paradigma computacional es especialmente adecuado como la optimización [15] o los problemas de aprendizaje automático, muy utilizados en la actualidad. Además, la aparición de estos nuevos ordenadores cuánticos, tiene una gran implicación en la seguridad informática, debido a la debilidad de los sistemas criptográficos frente a la potencia computacional de los sistemas cuánticos y la necesidad de la aparición de una nueva criptografía post-cuántica. En particular, el problema propuesto en este trabajo se refiere a la optimización de la respuesta a incidentes en un sistema de análisis y gestión de riesgos, donde la respuesta a incidentes puede optimizarse seleccionando aquellos controles adecuados a realizar, siendo un problema que crece exponencialmente con el número de incidentes. Por este motivo, y dado que la optimización de la respuesta puede no converger en un ordenador clásico, se ha propuesto una solución basada en un algoritmo de recocido cuántico para encontrar la configuración óptima al problema. Esta solución ha sido programada y probada con éxito en un ordenador cuántico D'Wave.

En trabajos anteriores hemos desarrollado MARISMA [16], un marco completo y extensible que se está aplicando para llevar a cabo la evaluación y gestión de riesgos para muchas y diferentes empresas, y que aborda la mayoría de los inconvenientes de los enfoques actuales. Gracias a nuestra experiencia aplicando nuestro marco a casos reales, hemos identificado este problema en el proceso de respuesta a incidentes de seguridad. Gracias a este marco, hemos podido validar el algoritmo cuántico propuesto en casos reales.

El artículo continúa en la sección 2 analizando los antecedentes y algunos trabajos relacionados de incidentes de seguridad y optimización cuántica; la sección 3 muestra el enfoque que seguimos en MARISMA para gestionar la respuesta a incidentes de seguridad; la sección 4 presenta el algoritmo propuesto por programación cuántica para resolver el problema planteado, y muestra un análisis y comparación de los resultados obtenidos aplicando el algoritmo cuántico frente al algoritmo clásico; por último, la sección 5 muestra las principales conclusiones obtenidas durante la investigación y futuros trabajos a realizar.

II. Antecedentes

Esta sección incluye los antecedentes sobre los temas de investigación abordados en este documento, los fundamentos de la computación cuántica y una visión general del proceso de respuesta a incidentes de seguridad y discutimos algunos problemas de investigación abiertos.

II-A. Computación Cuántica

La computación cuántica, un paradigma que explota los aspectos cuánticos de la realidad, promete tener un enorme impacto en la informática [17]. Sin embargo, para disponer de aplicaciones reales de la computación cuántica, se necesitan lenguajes de programación que proporcionen descripciones estructuradas y de alto nivel de los algoritmos cuánticos, sin referencia al hardware subyacente [18]. El descubrimiento de algoritmos cuánticos eficientes como los de Shor [19] y Grover [20] ha despertado un gran interés en el campo de la programación cuántica. Sin embargo, sigue siendo una tarea difícil encontrar nuevos algoritmos cuánticos principalmente porque los programas cuánticos son de muy bajo nivel.

La forma en que los programadores cuánticos trabajan con los cúbits (bits cuánticos) [21] es a través de circuitos cuánticos y puertas cuánticas, que proporcionan las operaciones primitivas para manipular la magnitud y la fase de los cúbits del sistema [21]. Los circuitos cuánticos y las puertas pueden representarse gráficamente como en la Figura 1, pero también mediante notaciones basadas en sintaxis que son proporcionadas por una amplia variedad de lenguajes de programación cuántica (como por ejemplo, Q#, QASM, Cirq, pyquil, QCL, entre muchos otros) que han sido propuestos para facilitar la especificación de algoritmos cuánticos. Estos algoritmos cuánticos suelen ser una traducción del circuito cuántico a código, es decir, una secuencia de sentencias textuales de programación.

Figura 1. Ejemplo de un circuito cuántico

Desde que se introdujo el primer lenguaje práctico de programación cuántica QCL, han aparecido muchos otros lenguajes [22], algunos de ellos más orientados a los circuitos cuánticos, mientras que otros se acercan más a los lenguajes de alto nivel. El diseño de los lenguajes de programación cuánticos posteriores se vio influido por el modelo QRAM (quantum random access machine) [23] en el que el sistema cuántico está controlado por un ordenador clásico. En los últimos años se han publicado varios lenguajes de programación cuántica, como qiskit [24] o Q# [25]. Todos estos lenguajes proponen respuestas a las necesidades fundamentales de la programación cuántica y con el objetivo de abordar los retos de la computación cuántica práctica [26].

II-B. Optimización Cuántica

La tecnología de computación cuántica ofrece soluciones fundamentalmente diferentes a los problemas computacionales y permite resolver problemas de forma más eficiente que con los cálculos clásicos [27]. Un cúbit es un sistema cuántico de estado múltiple, es decir, no sólo está definido por cero o uno como un bit clásico, sino que existen varios posibles valores al mismo tiempo. Así, un cúbit puede ser cero o uno con una cierta probabilidad (esto se conoce como

superposición y es la clave de la gran potencia de cálculo). El valor real de un cúbit sólo se conoce una vez que se mide, colapsando y ya no puede utilizarse sin reiniciarse. Como resultado, la filosofía de la programación cuántica se orienta hacia la exploración y búsqueda de soluciones óptimas en un espacio probabilístico [28].

Muchos de los algoritmos de optimización cuántica se basan en algoritmos de búsqueda que utilizan el conocido algoritmo de Grover [20], realizando una búsqueda en un espacio de búsqueda desconocido a partir de la codificación de los requisitos de la solución mediante un oráculo cuántico. Estos oráculos cuánticos [29], son una especie de caja negra asimilable al concepto de función de los lenguajes de alto nivel y que ayudan en la construcción de estos algoritmos de búsqueda con complejidad lineal.

Además, otros entornos cuánticos como Quantum Leap del fabricante de ordenadores cuánticos D'Wave proporcionan entornos de optimización para problemas combinatorios NP-completos mediante optimización cuántica adiabática [30]. Este tipo de programación se basa en la especificación del sistema a optimizar como un Hamiltoniano que representa tanto el objetivo como las restricciones del sistema y el ordenador cuántico se encarga de encontrar la solución que proporcione la menor energía al sistema [15]. También existen alternativas basadas en programación basada en puertas cuánticas, como el algoritmo de optimización cuántica aproximada (QAOA) [24].

II-C. Gestión de Incidentes de Seguridad

Los incidentes de seguridad son eventos no deseados que impactan en las diferentes dimensiones de los activos que conforman los sistemas de información de una empresa [31]. Estos incidentes se producen por fallos en la implementación de los controles de seguridad que protegen estos activos, es decir, por vulnerabilidades existentes en los sistemas de información. Estas vulnerabilidades son aprovechadas por las amenazas para llegar a estos activos y causarles daños [32].

Para minimizar los daños de estos incidentes, las organizaciones tratan de aplicar los métodos de respuesta a incidentes más adecuados [33]. Muchas organizaciones se han centrado en la gestión de riesgos a través de servicios integrados en Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), ya que han demostrado ser una de las mejores soluciones para mejorar la ciberseguridad colaborando entre sí, compartiendo conocimientos y aprendiendo de experiencias cruzadas [34]. Sin embargo, la implantación de un CSIRT tiene un coste considerable, siendo necesario crear sistemas de gestión de incidentes más sencillos y eficaces para las pequeñas y medianas empresas [35].

El problema más relevante al que se enfrentan las organizaciones es la agilidad en la gestión y respuesta ante incidentes de seguridad en el menor tiempo posible [36], [37]. Pero este problema es cada vez más difícil de abordar, debido al creciente número de incidentes y a su interconexión. Cuando los sistemas reciben cientos de incidentes, nos encontramos con que los equipos de respuesta a incidentes deben tomar una decisión sobre cuáles son los principales incidentes que deben empezar a analizar. Pero esta priorización no puede hacerse manualmente, ya que retrasaría la toma de decisiones. Según algunos investigadores, la respuesta a incidentes de seguridad requiere un complejo procesamiento de eventos (para capturar, procesar, integrar y analizar datos en tiempo real), así como investigar la relación causa-efecto entre los incidentes [38].

Por tanto, podemos ver como la mayoría de las investigaciones actuales relacionadas con incidentes de seguridad han concluido que la agilidad en la respuesta a incidentes de seguridad es la base para la correcta gestión de un sistema de información [39]. Pero muy poca investigación se ha centrado en resolver los problemas derivados de la complejidad computacional de tener que analizar un gran número de eventos en cortos periodos de tiempo. Y es esta agilidad en el análisis la que permitirá tomar las decisiones correctas en plazos razonables [40].

III. MARISMA: Sistema de Gestión de Riesgos de Seguridad e Incidentes

En esta sección presentamos el marco MARISMA [16], nuestro enfoque para el análisis y gestión dinámica de riesgos, presentando el objetivo y los principales componentes de este framework, y a continuación detallamos el proceso que llevamos a cabo para la gestión de incidentes de seguridad y el posterior procesamiento de los mismos para generar conocimiento útil que ayude en la toma de decisiones de la empresa, finalizando mostrando las limitaciones computacionales que actualmente impiden su uso eficiente.

III-A. Arquitectura de MARISMA

MARISMA es nuestro marco de análisis y gestión de riesgos, que hemos ido desarrollando, mejorando, ampliando y aplicando a muchos tipos de empresas y tecnologías durante la última década. Como puede verse en la figura 2, el marco consta de tres partes, una metodología apoyada en una estructura de metadatos, un mecanismo de extensibilidad y una herramienta automática que soporta la metodología e implementa las extensiones.

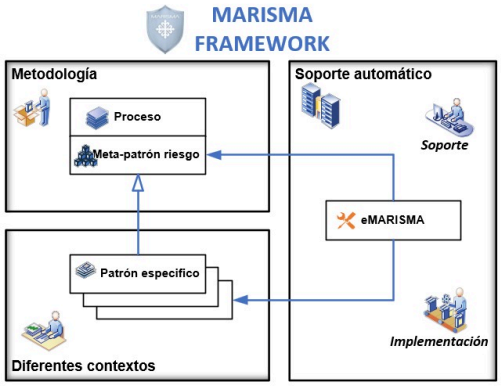

Figura 2. Arquitectura General de MARISMA

El elemento central de nuestro marco es una metodología que establece un proceso completo y detallado para llevar a cabo todo el ciclo de vida de la evaluación y gestión de riesgos para una empresa o parte de ella, incluidas las actividades necesarias para configurar las estructuras de datos reutilizables adecuadas que deben utilizarse, la generación semiautomática de datos de riesgos y, por último, la gestión

dinámica de riesgos, que incluye tareas específicas para la respuesta a incidentes de seguridad. La metodología se apoya en un conjunto de Indicadores Clave de Riesgo (KRI) y en una estructura de metadatos (el Meta-Patrón de Riesgo de la Figura 2), que define los componentes y sus relaciones que permiten la máxima personalización y automatización del proceso de evaluación y gestión de riesgos. Esta metodología se adapta a los distintos contextos mediante la creación de patrones específicos que instancian la metodología en el contexto dado.

El último componente de nuestro marco es la herramienta e-MARISMA, esta herramienta implementa todos los procesos de la metodología y es posible configurarla para soportar cualquier patrón que represente un contexto particular. Ofrece un rico conjunto de servicios, no sólo relacionados con la configuración y administración del patrón, sino también enfocados a los procesos de evaluación y gestión de riesgos llevados a cabo por nuestros clientes. El objetivo principal de esta herramienta es poder realizar una evaluación de riesgos rápida, barata, visual y precisa, así como una gestión de riesgos eficiente y eficaz, por lo que explotamos al máximo la reutilización. Además, la herramienta aprende de los conocimientos recogidos a partir de la ocurrencia de incidentes de seguridad y, en consecuencia, puede tomar decisiones automatizadas mediante la correlación de incidentes. Este marco se ha aplicado a distintos tipos de empresas (eléctricas, hidrocarburos, administraciones públicas, sanidad, construcción naval, industria química, etc.) en más de ocho países europeos y latinoamericanos.

III-B. Respuesta a Incidentes en MARISMA

La gestión y respuesta a incidentes de seguridad es una actividad crítica llevada a cabo dentro del proceso dinámico de gestión de riesgos de nuestro marco. Una vez identificado un incidente, necesitamos recopilar, categorizar y analizar la información de contexto del incidente, y algunos parámetros relevantes necesitan ser ajustados en nuestro sistema (nivel de riesgos y controles de cumplimiento, controles implicados, probabilidad de ocurrencia de la amenaza, etc.). Esta parametrización depende del conjunto de conceptos y relaciones definidos en nuestro meta-patrón de riesgos, y de su instanciación concreta a través de un patrón, que incluirá los componentes seleccionados a través del proceso mostrado en la Figura 3.

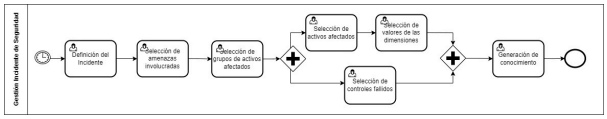

Figura 3. Proceso de gestión de incidentes de seguridad

Este proceso está totalmente implementado por eMARISMA, que proporciona un flujo de trabajo para i) introducir la información del incidente de seguridad (una descripción, la causa, la persona responsable y los plazos de resolución), ii) seleccionar a partir de la información almacenada y de acuerdo con las relaciones de datos definidas por el patrón de riesgo la jerarquía de elementos que están involucrados con el incidente de seguridad (amenazas, activos y controles), definir otra información relacionada como la gravedad del incidente, y poner en cuarentena los controles afectados bajando temporalmente su nivel de cobertura mientras se resuelve el incidente, y finalmente, una vez resuelto el incidente, iii) apoyar la gestión del conocimiento y el aprendizaje de los incidentes de seguridad ocurridos registrando la lección aprendida, los costes de resolución del incidente y algunas observaciones finales. Evidentemente, cuando se produce y registra un incidente de seguridad, se aplica automáticamente un conjunto de cambios en cadena sobre los componentes de riesgo en función de la metainformación almacenada. Esto se debe a que el nivel de cumplimiento de los controles de seguridad se ve penalizado si una amenaza ha puesto en peligro el control, lo que afecta al nivel de riesgo de muchos otros activos, y lo que implica que dichos controles deben revisarse y reforzarse.

Para ilustrar este problema, consideraremos este ejemplo basado en un conjunto de datos típico de incidentes notificados que se tratarán según la estructura de gestión de incidentes utilizada por eMARISMA (véase la tabla I), que define los siguientes atributos: i) IdIncidente: Identificador único del incidente, ii) IdAmenaza: Código de la amenaza según la definición del patrón utilizado, iii) Amenaza: Descripción de la amenaza que ha causado el incidente, iv) Severidad: Valoración cualitativa de la gravedad del incidente (entre 1 y 5), v) IdControl: Código del control según la definición del patrón utilizado, vi) Control: Descripción del control que se ha visto afectado por la amenaza, y vii) Tiempo estimado: Estimación del número de horas necesarias para resolver el incidente.

Como podemos ver en la Tabla I, consideramos que cada incidente implica una única amenaza, que suele ser el escenario más frecuente. Cada incidente puede afectar a uno o varios controles cuya implementación debe ser revisada y corregida para resolver el incidente e intentar evitar que se repita. Además, es habitual que varios incidentes estén relacionados con un mismo control. Por ejemplo, el control *[12.1.3] Gestión de la capacidad* se ha visto afectado tanto por el incidente de seguridad 1 como por el 6. Del mismo modo, podemos ver cómo el control [12.3.1] Copias de seguridad de la información se ve afectado por los incidentes 1 y 9. De esta forma, priorizando la resolución del incidente 1, reforzamos los dos controles afectados, y se resolverían también los incidentes 6 y 9, con el consiguiente ahorro de tiempo y recursos.

IV. Algoritmo cuántico para optimizar la respuesta a incidentes

Para resolver el problema utilizando un enfoque de *quantum annealing*, tenemos que observar que el proceso habitual de estos algoritmos consiste en especificar el problema a resolver como cúbits en estado de superposición y colapsar los cúbits a un estado clásico que sea 0 ó 1 y represente la solución de menor energía al problema propuesto. Como se puede observar en la Figura 4 el proceso comienza con un estado energético que corresponde al estado de superposición de los cúbits, en el que sólo existe un valle (a), a medida que avanza el proceso las posibilidades energéticas se separan generando un estado potencial de doble pozo (b). Al final del proceso uno de los valles corresponde a la energía mínima que estabiliza

Tabla I
DATASET DE INCIDENTES

IdIncidente	IdAmenaza	Amenaza	Severity	IdControl	Control	Tiempo (h)
1	A.24	Denegación de Servicio	5	12.3.1	Backup de la información	6
1	A.24	Denegación de Servicio	5	12.1.3	Gestión de Capacidad	6
2	A.25	Robo	3	11.2.6	Seguridad del equipamiento Off-site	24
3	A.30	Ingeniería Social	4	11.1.2	Controles de entrada física	8
4	E.3	Errores de monitorización	3	9.4.1	Restrición de acceso a la información	40
4	E.3	Errores de monitorización	3	9.2.4	Gestión de la autenticación de la información secreta	40
5	I.5	Fallo de origen físico o lógico	4	11.2.4	Mantenimiento de los equipos	24
6	E.24	Caída del sistema por agotamiento de recursos	5	12.1.3	Gestión de la capacidad	8
7	A.6	Abuso de los privilegios de acceso	4	9.4.1	Restricción del acceso a la información	24
8	E.4	Errores de configuración	2	12.4.4	Sincronización del reloj	2
9	E.21	Errores en el mantenimiento	3	12.3.1	Backup de la información	6
10	I.7	Condiciones inadecuadas de temperatura o humedad	2	11.2.2	Servicios de suministro	72
11	A.30	Ingeniería Social	5	9.2.4	Gestión de la autenticación a información secreta	16
12	I.8	Fallo en los servicios de comunicaciones	2	13.1.1	Controles de red	8

el sistema y se genera un valle más profundo correspondiente a esa solución (c).

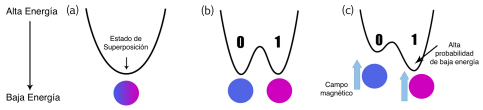

Figura 4. Quantum annealing process[1].

IV-A. Definiciones

Las variables que forman parte del algoritmo se pueden definir de la siguiente manera:

Definición 1: Sea **i** un identificador único de un incidente que se corresponde con el IdIncidente de la Tabla I.

Definición 2: Sea **k** un identificador de control que representa el código de control único IdControl.

Definición 3: Sea $\mathbf{C}_k$ el conjunto de incidentes relacionados con el IdControl k.

Definición 4: Sea $\mathbf{t}_i$ el tiempo estimado en horas necesario para resolver la incidencia cuyo IdIncidente es igual a i.

Definición 5: Sea $\mathbf{x}_i$ una variable binaria que determina, en la solución del algoritmo, si el incidente i es seleccionado para ser abordado.

Definición 6: Sea **P** un coeficiente de penalización, que sirve para modular el peso de las restricciones en la definición del algoritmo. Se puede encontrar empíricamente que es igual al mayor tiempo estimado entre todas las ocurrencias más 1, por lo que afecta a toda la solución.

A partir de estas definiciones podemos expresar algebraicamente el objetivo perseguido mediante la ejecución del algoritmo de optimización cuántica que será enviado al ordenador cuántico.

IV-B. Enfoque del algoritmo

La entrada al algoritmo es una serie de incidencias identificadas por su ID, cada uno de los incidentes tiene una gravedad y un tiempo estimado de resolución. Además, tiene una serie de controles asociados que deberán ser revisados y reforzados para considerar que la incidencia ha sido resuelta. Estos controles pueden estar asociados a la resolución de varias incidencias, de forma que si resolvemos una incidencia que comparte controles con otra, resolvemos esa para otra incidencia al mismo tiempo. Para resolver el problema, debemos seleccionar un resultado en el que se seleccione el conjunto mínimo de incidencias a resolver, de forma que cubramos todos los controles que nos permitan resolver el resto de incidencias. Esta solución debe realizarse en el menor tiempo posible.

Para resolver el problema, modelaremos este problema como un problema *Quadratic Unconstrained Binary Optimization (QUBO)*, a través de un Hamiltoniano que representará los objetivos y restricciones de nuestro problema y podrá ser enviado al solucionador del ordenador cuántico adiabático para encontrar el estado de mínima energía, que coincidirá con la combinación de incidentes, que deben ser seleccionados para resolver nuestro problema óptimamente.

Nuestro objetivo principal es minimizar el tiempo total de las cuestiones que forman parte de la solución:

$$\sum_{i=1}^{N}(x_i \times t_i) \tag{1}$$

Siendo x_i la variable binaria que determina si se selecciona o no la incidencia i, y t_i el tiempo estimado relacionado con la incidencia i. Las restricciones son algo más complicadas de modelar, ya que las incidencias pueden cumplirse bien porque han sido seleccionadas, bien porque el conjunto de controles que forman parte de ella ya han sido resueltos por una o varias incidencias previamente seleccionadas.

En este problema, buscamos que todas las incidencias estén resueltas, y para determinar que una incidencia está resuelta miramos si sus controles han sido seleccionados o no. Queremos que todos los controles tengan al menos un incidente relacionado que haya sido seleccionado. Esta restricción se formulará de la siguiente manera:

$$\sum_{i \in C_k}(x_i) \geq 1 \tag{2}$$

Donde C_k es el conjunto de incidencias relacionadas con el

[1]https://docs.dwavesys.com/docs/latest/c_gs_2.html

control *k*. Con esta expresión controlamos que al menos una de las incidencias relacionadas con *k* haya sido seleccionada. Haciendo esto para todos los controles, obtenemos:

$$\sum_{k} \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) \tag{3}$$

Para construir la ecuación QUBO final necesitamos añadir un coeficiente de penalización (P), que sirve para modular el peso de las restricciones en la expresión hamiltoniana. El coeficiente *P* es el mayor tiempo estimado entre todas las ocurrencias más 1, de esta manera ambas partes (ecuaciones 2 y 3) contribuyen a la solución [15]. La ecuación final de QUBO es la siguiente:

$$\sum_{i=1}^{N} (x_i \times t_i) + P \times \sum_{k} \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) \tag{4}$$

Simplificando la parte de la expresión que representa las restricciones, podemos obtener la siguiente expresión:

$$\begin{aligned} P \times \sum_{k} \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) = \\ P \times \sum_{k} \Big(\sum_{i,j \in C_k} (x_i^2 + 1^2 + 2x_i x_j - 2x_j) \Big) \end{aligned} \tag{5}$$

Teniendo en cuenta que x sólo puede tomar como valores 0 y 1, podemos eliminar el cuadrado que tiene ya que es irrelevante; así como el de 1:

$$P \times \sum_{k} \Big(\sum_{i,j \in C_k} (x_i + 1 + 2x_i x_j - 2x_i) \Big) \tag{6}$$

Simplificando:

$$\begin{aligned} P \times \sum_{k} \Big(\sum_{i,j \in C_k} (-xi + 1 + 2xixj) \Big) = \\ \sum_{k} \Big(\sum_{i,j \in C_k} (-Px_i + P + 2Px_i x_j) \Big) \end{aligned} \tag{7}$$

Podemos eliminar la parte constante, ya que no modifica la solución:

$$\sum_{k} \Big(\sum_{i,j \in C_k} (-Px_i + 2Px_i x_j) \Big) \tag{8}$$

Así que nuestra expresión BQM (QUBO) del Hamiltoniano inicial es finalmente la siguiente:

$$\begin{aligned} \sum_{i=1}^{N} (x_i \times t_i) + P \times \sum_{k} \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) = \\ \sum_{i=1}^{N} (x_i \times t_i) + \sum_{k} \Big(\sum_{i,j \in C_k} (-Px_i + 2Px_i x_j) \Big) \end{aligned} \tag{9}$$

La ecuación final nos da una parte lineal $(-Px_i)$ y una parte cuadrática $(2Px_i x_j)$, que generará una matriz bidimensional equivalente a la expresión y que será enviadas al *quantum annealer*.

IV-C. Ejecución del algoritmo cuántico

Tras ejecutar el algotimo, obtenemos los resultados del muestreo como un archivo de texto en el que podemos observar los resultados del algoritmo y la energía de cada una de las soluciones encontradas. La solución con un nivel de energía mínimo es la que cumple los requisitos y objetivos de nuestro problema. A continuación se muestra la salida del algoritmo para los datos mostrados en la Tabla II:

```
Solution Found with energy: -100.0
Selected Items : [3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15]
Total Execution Time:  0:00:00.040289
Total Time for the solution: [8, 8, 6, 4, 4, 4, 8, 6, 3, 3, 6]
Total Time = 60
       1 10 11 12 13 14 15  2  3  4  5  6  7  8  9 energy oc.
21591  0  1  1  1  1  1  1  0  1  1  1  1  1  0  0 -100.0  1
21584  0  1  1  1  1  1  1  0  0  1  1  1  1  0  0  -99.0  1
11176  0  1  1  1  1  1  0  0  1  1  1  1  1  0  0  -98.0  1
21910  1  1  1  1  1  1  1  0  1  1  1  0  1  0  1  -98.0  1
11183  0  1  1  1  1  1  0  0  0  1  1  1  1  0  0  -97.0  1
...
```

Tabla II
EJEMPLO DE EJECUCIÓN DEL QUANTUM ANNEALER

IdIncidente	IdControl	Tiempo (h)
1	C12	2
2	C05	6
3	C04	11
4	C01	8
4	C05	6
5	C14	6
6	C03	4
6	C12	2
7	C09	2
8	C06	7
9	C03	4
10	C08	8
11	C02	6
12	C06	3
12	C10	3
13	C13	6
14	C07	4
15	C11	10

El resultado también puede verse gráficamente, la Figura 5 muestra la configuración de los cúbits en el procesador cuántico, en la que cada uno de los puntos muestra un cúbit que representa, respectivamente, las incidencias a gestionar. Las líneas del grafo generado que enlazan los cúbits son las restricciones y asociaciones de control que existen entre los distintos incidentes. En el mismo gráfico se muestra la configuración final de las amplitudes (0 ó 1) de cada cúbit, de forma que el sistema queda en la configuración de menor energía.

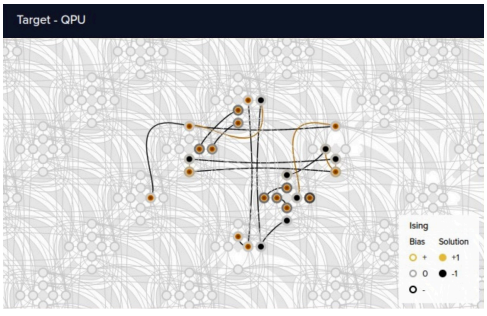

Figura 5. Cúbits cuánticos después del annealing

En la figura 6 se muestra gráficamente la salida del algoritmo en la que podemos observar que los incidentes *[3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15]* fueron seleccionados para ser procesados, ya que los controles utilizados para abordar el incidente número 6 resuelven también los incidentes 1 y 9, al igual que ocurre con los incidentes 12 y 8 y también con los incidentes 4 y 2.

Figura 6. Solución del Quantum Annealer

En la Figura 7, se puede observar el histograma de las energías de los ejemplos devueltos. En esta figura se puede ver la ocurrencia de cada una de las soluciones encontradas por el procesador cuántico y su energía asociada, de forma que se puede apreciar visualmente que el resultado devuelto por el algoritmo es la configuración final de los estados cúbit con menor energía y que se ha producido un mayor número de veces en el proceso de *Quantum annealing*. En este caso, la mejor solución se encontró con un valor de energía de *-100* y también fue la solución más repetida encontrada.

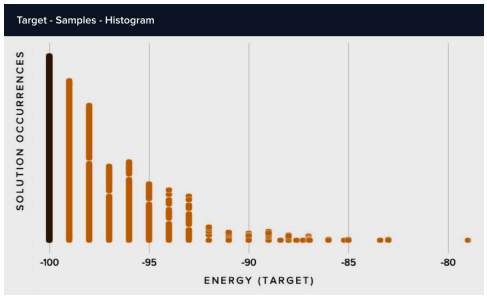

Figura 7. Lowest Energy in a Quantum Annealer

IV-D. Resultados empíricos

Los algoritmos clásicos que resuelven este tipo de problemas suelen basarse en backtracking, programación dinámica o branch and bound, que tienen una complejidad computacional exponencial. Sin embargo, los algoritmos de optimización adiabática, debido a su naturaleza cuántica y gracias al concepto de superposición, consiguen un procesamiento en tiempo constante o lineal.

Para ver la mejora computacional del algoritmo propuesto, ejecutamos el algoritmo con samplesets de diferentes tamaños utilizando un *D-Wave 2000Q lower-noise system*, con un procesador cuántico *DW_2000Q_6* que proporciona 2048 cúbits en una *[16,16,4] chimera topology*. También probamos un algoritmo de Backtracking clásico escrito en Python que se ejecuta en Mac OS System, con un Intel Core i7 a 3,2 GHz y 64 GB de RAM DDR4. Como se puede observar en la Tabla III, tenemos un tiempo constante e independiente del número de incidencias a procesar (alrededor de 3 segundos), mientras que el tiempo de un algoritmo de Backtracking para resolver el problema crece exponencialmente con el número de incidencias, no llegando a converger con más de cien incidencias.

Tabla III
TIEMPOS DE EJECUCIÓN (SEGUNDOS) DE UN COMPUTADOR CLÁSICO FRENTE UN COMPUTADOR CUÁNTICO

# de Incidentes	Tiempo Alg Q (s)	Tiempo backtracking (s)
5	3.000	0.00043
10	2.983	0.00179
12	2.999	0.00800
15	2.996	0,06300
20	2.996	1.52100
25	2.999	58.27700
30	2.990	1,824.04300
40	2.990	8,197.49900
50	2.990	104,031.91500
100	2.997	El algoritmo no converge

A la luz de estos resultados podemos considerar que el enfoque cuántico adiabático para la resolución de problemas de optimización en el contexto de la gestión de incidentes de seguridad es ampliamente eficiente y supone una mejora respecto a la gestión anterior basada en algoritmos de optimización clásicos. Esta mejora se produce tanto en tiempo de respuesta, como en precisión y también en consumo de energía.

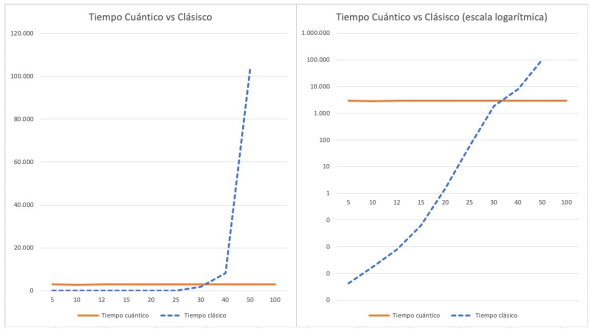

Figura 8. Tiempos de ejecución del algoritmo clásico vs cuántico (seg)

V. CONCLUSIONES

En los últimos años, la gestión de la seguridad, el análisis de riesgos y, en particular, la gestión de riesgos basada en la correcta gestión y aprendizaje de los incidentes de seguridad han adquirido una importancia creciente. En este sentido, el tiempo que se tarda en responder a los incidentes y restablecer la seguridad del sistema es un aspecto crucial. Sin embargo, el tiempo de respuesta que ofrecen las soluciones clásicas crece exponencialmente a medida que aumenta el número de incidentes, lo que las hace inadecuadas para los escenarios del mundo real.

Hemos diseñado e implementado un algoritmo basado en programación cuántica adiabática con un tiempo de ejecución

muy eficiente, con un tiempo casi constante, mientras que los algoritmos clásicos ofrecen un coste de tiempo exponencial.

AGRADECIMIENTOS

Agradecemos el apoyo de las empresas Sicaman Nuevas Tecnologías S.L. (https://www.sicaman.com) y Marisma Shield S.L. (https://www.emarisma.com) que han facilitado la validación de los casos de estudio y el uso de la herramienta eMARISMA. Este trabajo se ha desarrollado en el marco de los proyectos AETHER-UCLM (PID2020-112540RB-C42) financiado por MCIN/AEI/10.13039/501100011033, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521), ALBA-UC (TED2021-130355B-C33, id.3611130630-130630-28-521) financiado por el Ministerio de Ciencia e Innovación, y apoyado por el Proyecto Horizonte 2020 de la Unión Europea CyberSANE bajo el Acuerdo de Subvención No. 833683.

REFERENCIAS

[1] I. Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," *Computers & Security*, vol. 86, pp. 350–357, sep 2019.

[2] S. A. R. Mortazavi and F. Safi-Esfahani, "A checklist based evaluation framework to measure risk of information security management systems," *International Journal of Information Technology (Singapore)*, vol. 11, no. 3, pp. 517–534, 2019.

[3] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, "Exiting the Risk Assessment Maze," *ACM Computing Surveys*, vol. 51, no. 1, pp. 1–30, apr 2018.

[4] Z. Szabó, "The Information Security and IT Security Questions of Pension Payment," in *Key Engineering Materials*, vol. 755. Trans Tech Publ, sep 2017, Conference Proceedings, pp. 322–327.

[5] H. F. Yoseviano and A. Retnowardhani, "The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd," in *2018 International Conference on Information Management and Technology (ICIMTech)*. IEEE, sep 2018, Conference Proceedings, pp. 21–26.

[6] D. Akinwumi, G. Iwasokun, B. Alese, and S. Oluwadare, "A review of game theory approach to cyber security risk management," *Nigerian Journal of Technology*, vol. 36, no. 4, p. 1271, jan 2018.

[7] W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank," in *2018 International Conference on Information Management and Technology (ICIMTech)*. IEEE, sep 2018, Conference Proceedings, pp. 38–42.

[8] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "How can organizations develop situation awareness for incident response: A case study of management practice," *Computers & Security*, vol. 101, p. 102122, feb 2021.

[9] S. A. R. Mortazavi and F. Safi-Esfahani, "A checklist based evaluation framework to measure risk of information security management systems," *International Journal of Information Technology*, vol. 11, no. 3, pp. 517–534, sep 2019.

[10] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach," *Informatica*, vol. 30, no. 1, pp. 187–211, jan 2019.

[11] N. Paltrinieri and G. Reniers, "Dynamic risk analysis for Seveso sites," *Journal of Loss Prevention in the Process Industries*, vol. 49, pp. 111–119, sep 2017.

[12] S. Alhawari, L. Karadsheh, A. Nehari Talet, and E. Mansour, "Knowledge-Based Risk Management framework for Information Technology project," *International Journal of Information Management*, vol. 32, no. 1, pp. 50–65, feb 2012.

[13] C. Glantz, J. Lenaeus, G. Landine, L. R. O'Neil, R. Leitch, C. Johnson, J. Lewis, and R. Rodger, *Implementing an Information Security Program*, ser. Terrorism, Security, and Computation. Cham: Springer International Publishing, 2017, book section Chapter 9, pp. 179–197.

[14] A. Bhardwaj and V. Sapra, "Security incidents & response against cyber attacks," 2021.

[15] A. Lucas, "Ising formulations of many np problems," *Frontiers in physics*, vol. 2, p. 5, 2014.

[16] D. G. Rosado, J. Moreno, L. E. Sánchez, A. Santos-Olmo, M. A. Serrano, and E. Fernández-Medina, "Marisma-bida pattern: Integrated risk analysis for big data," *Computers & Security*, vol. 102, p. 102155, 2021.

[17] IBM, *The Quantum Decade. A playbook for achieving awareness, readiness, and advantage*, 2021. [Online]. Available: https://www.ibm.com/downloads/cas/J25G35OK

[18] P. Clairambault, M. De Visme, and G. Winskel, "Game semantics for quantum programming," *Proceedings of the ACM on Programming Languages*, vol. 3, no. POPL, pp. 1–29, 2019.

[19] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Ieee. IEEE Comput. Soc. Press, 2002, pp. 124–134.

[20] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," *Physical Review Letters*, vol. 79, no. 2, pp. 325–328, jul 1997.

[21] P. Sánchez and D. Alonso, "On the Definition of Quantum Programming Modules," *Applied Sciences*, vol. 11, no. 13, p. 5843, 2021.

[22] B. Heim, M. Soeken, S. Marshall, C. Granade, M. Roetteler, A. Geller, M. Troyer, and K. Svore, "Quantum programming languages," *Nature Reviews Physics*, vol. 2, no. 12, pp. 709–722, 2020.

[23] E. Knill, "Conventions for quantum pseudocode," Los Alamos National Lab., NM (United States), Tech. Rep. LAUR-96-2724, 1996.

[24] A. Asfaw, A. Corcoles, L. Bello, Y. Ben-Haim, M. Bozzo-Rey, S. Bravyi, N. Bronn, L. Capelluto, A. C. Vazquez, J. Ceroni, R. Chen, A. Frisch, J. Gambetta, S. Garion, L. Gil, S. D. L. P. Gonzalez, F. Harkins, T. Imamichi, H. Kang, A. h. Karamlou, R. Loredo, D. McKay, A. Mezzacapo, Z. Minev, R. Movassagh, G. Nannicini, P. Nation, A. Phan, M. Pistoia, A. Rattew, J. Schaefer, J. Shabani, J. Smolin, J. Stenger, K. Temme, M. Tod, S. Wood, and J. Wootton., *Learn Quantum Computation Using Qiskit*, 2020. [Online]. Available: http://community.qiskit.org/textbook

[25] K. Svore, M. Roetteler, A. Geller, M. Troyer, J. Azariah, C. Granade, B. Heim, V. Kliuchnikov, M. Mykhailova, and A. Paz, "Q#," in *Proceedings of the Real World Domain Specific Languages Workshop 2018 on - RWDSL2018*, ser. RWDSL2018. New York, New York, USA: ACM Press, 2018, pp. 1–10.

[26] L. Gyongyosi and S. Imre, "A Survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, feb 2019.

[27] ——, "A Survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[28] M. Piattini, M. Serrano, R. Perez-Castillo, G. Petersen, and J. L. Hevia, "Toward a Quantum Software Engineering," *IT Professional*, vol. 23, no. 1, pp. 62–66, jan 2021.

[29] R. Sutor, *Dancing with Qubits*. Packt Publishing Birmingham, UK, 2019.

[30] A. Das and B. K. Chakrabarti, "Colloquium: Quantum annealing and analog quantum computation," *Reviews of Modern Physics*, vol. 80, no. 3, p. 1061, 2008.

[31] D. Mahima, "Cyber threat in public sector: Modeling an incident response framework," in *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 2021, pp. 55–60.

[32] M. Dion, "Cybersecurity policy and theory," in *Theoretical Foundations of Homeland Security*. Routledge, 2020, pp. 257–284.

[33] R. Prasad and V. Rohokale, *Secure Incident Handling*. Cham: Springer International Publishing, 2020, pp. 203–216.

[34] L. M. Tanczer, I. Brass, and M. Carr, "Csirts and global cybersecurity: How technical experts support science diplomacy," *Global Policy*, vol. 9, no. S3, pp. 60–66, 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.12625

[35] T. Plėta, M. Tvaronavičienė, and S. Della Casa, "Cyber effect and security management aspects in critical energy infrastructures," *Insights into Regional Development*, vol. 2, no. 2, pp. 538–548, Jun. 2020. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02919624

[36] R. van der Kleij, J. M. Schraagen, B. Cadet, and H. Young, "Developing decision support for cybersecurity threat and incident managers," *Computers & Security*, p. 102535, 2021.

[37] Y. He, E. D. Zamani, S. Lloyd, and C. Luo, "Agile incident response (air): Improving the incident response process in healthcare," *International Journal of Information Management*, vol. 62, p. 102435, 2022.

[38] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. Masood Siddiqui, "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis," *International Journal of Information Management*, vol. 59, p. 102334, 2021.

[39] T. Aoyama, A. Sato, G. Lisi, and K. Watanabe, "On the importance of agility, transparency, and positive reinforcement in cyber incident crisis communication," in *Critical Information Infrastructures Security*, S. Nadjm-Tehrani, Ed. Cham: Springer International Publishing, 2020, pp. 163–168.

[40] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178–188, 2019.

Índice de autores