Gestión Riesgos cibernéticos para el sistema de información del Departamento Control comercio de Armas Municiones y Explosivos.

Mayor. Rincón Solano Rubén Eduardo

Artículo para optar al título profesional:

Magister en Ciberseguridad y ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Rubén Eduardo Rincón Solano
Identificación	**:**	9590182
Programa académico	**:**	MECI
Tutor metodológico	**:**	CR. Serrano Cuervo Aldemar
Tutor temático	**:**	TC. Julián Alberto González Moreno
Fecha de entrega	**:**	25 de septiembre de 2025
Extensión	**:**	7919 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras Notas utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza / no autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Gestión Riesgos cibernéticos para el sistema de información del Departamento Control comercio de Armas Municiones y Explosivos.

Cyber Risk Management for the Information System of the Department of Arms, Ammunition, and Explosives Trade Control.

My. Rubén Eduardo Rincón Solano*
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La investigación analiza los riesgos cibernéticos asociados a bases de datos relacionales SQL, con énfasis en el sistema del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE). Utilizando una revisión crítica de literatura académica, se identificaron amenazas como inyección de código SQL, escalada de privilegios y denegación de servicio, que representan el 45% de los incidentes reportados en sistemas similares. Las estrategias basadas en aprendizaje automático, como CNN-BiLSTM y Naïve Bayes, alcanzan precisiones del 97.8% en detección de amenazas. Además, se evaluó el nivel de madurez del sistema del DCCAE, revelando que el 70% de los dominios críticos operan en niveles iniciales. La investigación propone soluciones adaptativas y escalables para fortalecer la seguridad y resiliencia frente a amenazas emergentes, integrando tecnologías avanzadas y medidas tradicionales.

Palabras clave: Ciberseguridad, bases de datos, SQL, inteligencia artificial, mitigación, inyección.

Abstract: This study examines cybersecurity risks in SQL relational databases, focusing on the Department of Arms Trade Control (DCCAE) system. Through a critical review of academic literature, threats such as SQL code injection, privilege escalation, and denial of service—accounting for 45% of incidents in similar systems—were identified. Machine learning strategies, including CNN-BiLSTM and Naïve Bayes, achieved 97.8% accuracy in threat detection. Furthermore, the maturity level assessment of the DCCAE system revealed that 70% of critical domains operate at initial levels. The research proposes adaptive and scalable solutions to enhance security and resilience against emerging threats, integrating advanced technologies and traditional measures.

Keywords: Cybersecurity, data bases, SQL, artificial intelligence, mitigation, injection.

* Oficial del Ejército Nacional, profesional en ciencias militares, candidato a magister en Ciberseguridad y Ciber Defensa. Orcid:1200-987-123.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Introducción

El concepto de ciberseguridad, aplicado al marco estructural de protección que requieren las bases de datos configuradas con SQL, se encuentra en constante evolución.

Este dinamismo responde, en gran medida, a las crecientes amenazas derivadas de la inclusión de inteligencia artificial (IA) en el desarrollo de códigos maliciosos, los cuales buscan impactar las sintaxis codificadas o inyectar modificaciones. Esta tendencia ha llevado a la construcción de protocolos de ciberseguridad cada vez más especializados, particularmente aquellos orientados a la protección de bases de datos relacionales.

Un ejemplo representativo de una base de datos relacional, que además constituye un sistema de información perteneciente a la infraestructura crítica del sector defensa, es el sistema de administración de datos diseñado para regular el flujo de información y metadatos asociados al control y comercio de armas. La relevancia de este sistema radica en su papel estratégico dentro de la seguridad nacional, lo que lo convierte en un objetivo potencial para ciberataques con modalidades tecnológicas-complejas.

De acuerdo con CISCO (2024), la incorporación de inteligencia artificial ha aumentado la cantidad de ciberataques dirigidos a bases de datos similares a las del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE). Este aumento evidencia cómo la IA ha potenciado la capacidad estructural de los ciber atacantes, generando un crecimiento exponencial en las posibilidades de ataque.

Aunque no existen antecedentes documentados de ataques exitosos al sistema de información del DCCAE (debido a la confidencialidad de los datos), sí se identifican riesgos significativos. Según De Azambuja *et al* (2023), la IA puede facilitar ataques como la inyección de código malicioso, lo que podría derivar en la eliminación de archivos o ficheros esenciales para el funcionamiento de softwares que funcionan como el sistema de control del DCCAE.

Entre los riesgos más comunes asociados a ciberataques impulsados por inteligencia artificial hacia bases de datos relacionales se encuentran: la inyección de código malicioso, que permite a los atacantes modificar o eliminar datos críticos; los ataques de escalada de privilegios, en los que se obtiene acceso no autorizado a niveles administrativos del sistema;

y las amenazas de denegación de servicio (DoS), que pueden saturar el sistema SQL, impidiendo su gestión formal.

En este contexto, tres causas principales del problema, que de facto están relacionados también con la matriz de riesgos, salen a colación y justifican esta investigación:

1. Posible desactualización de los protocolos de ciberseguridad destinados a proteger los códigos SQL que regulan el flujo de información en la administración de la base de datos del DCCAE.
2. Incremento en los ciberataques mediante inyección de código, según lo reportado por el Boletín de Ciberseguridad del Comando Cibernético de las Fuerzas Militares (CCOCI, 2024).
3. Desconocimiento de los protocolos de ciberseguridad aplicados a bases de datos relacionales.

Frente a tres causas, un interrogante de investigación sale a colación:

¿Cómo gestionar los riesgos cibernéticos que presenta la base de datos relacional de SQL que regula el sistema de información empleado por el Departamento de Control de Comercio de Armas, Municiones y Explosivos?

Metodología

El enfoque de esta investigación es cualitativo, lo que facilita la construcción de procesos metodológicos orientados al análisis micro segmentado del objeto de estudio. Este análisis se desarrolla en fases, permitiendo abordar la complejidad inherente al proceso investigativo de manera estructurada y progresiva.

En la primera fase, se realiza una explicación conceptual sobre la naturaleza digital de los ataques dirigidos a bases de datos relacionales de tipología SQL en el contexto de la guerra cibernética.

El objetivo principal de esta etapa es identificar y exponer los tipos de ciberataques asociados con inteligencia artificial que pueden comprometer sistemas de información o infraestructuras críticas en el ciberespacio. Para ello, se lleva a cabo un análisis exhaustivo de Notas de información y bases de datos científicas como SCOPUS, Web of Science (WOS) y Science Direct. La técnica metodológica empleada es el debate crítico conceptual, utilizando categorías de búsqueda específicas como *cyber security*, *data warehouse*, *data set*, *data base*, *method*, *techniques*, *protocol*, y un rango temporal delimitado entre 2020 y 2025.

En la segunda fase, se aborda el estudio de los riesgos cibernéticos asociados con ataques a bases de datos relacionales SQL reportados en el contexto colombiano durante los años 2023 y 2024. Esta etapa utiliza como base el análisis conceptual desarrollado previamente, extendiendo su alcance al estudio de los riesgos reportados por el Centro Cibernético Policial (CCOCI).

El propósito es identificar qué ciberataques representan una amenaza concreta para bases de datos relacionales codificadas con SQL. La técnica aplicada en esta fase es la comparación y exploración técnica estadística, lo que permite construir una matriz de riesgos que servirá como insumo para la siguiente etapa de la investigación.

En la tercera y última fase, se aplica la matriz de riesgos en un marco hipotético del sistema de información SQL utilizado por el Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE). Para ello, se adopta el instrumento metodológico OCTAVE-S, diseñado para formular un proceso secuencial y ajustado a las necesidades técnicas del software. Una vez concluido este procedimiento, se proponen

enfoques estratégicos de prevención orientados a proteger el sistema de información del DCCAE.

Por lo anterior, los resultados se explican a partir de la construcción teórica desarrollada en torno a la ciberseguridad, consolidando una perspectiva integral para la protección de infraestructuras críticas en el ámbito nacional.

Explicación conexa a la elección de los métodos de análisis OCTAVE y COBIT19.

La elección de COBIT 2019 como eje de la evaluación metodológica respondió a la necesidad explícita de transformar un panorama operativo en el que siete de los diez dominios analizados permanecen en niveles Inicial, Básico o Ad-hoc (equivalentes al 70% de la superficie evaluada) y tres de ellos —autenticación y control de acceso, cifrado de datos y seguridad perimetral— fueron calificados con brecha crítica al requerir saltos de Básico a Avanzado u Optimizado.

El corpus conceptual previo sobre amenazas al entorno SQL mostró un riesgo predominante de inyección de código que en contextos análogos concentra el 45% de los incidentes reportados, mientras que la literatura evidencia capacidades tecnológicas maduras (precisiones del 97.8% con Naïve Bayes, superiores al 96% con modelos supervisados y falsos positivos inferiores al 1%) que el sistema aún no aprovecha por carencias estructurales de gobierno, monitoreo y control.

Ese contraste entre potencial técnico disponible y madurez real insuficiente justificó un marco de gobierno integral que permitiera: (a) trazar una línea base homogénea en seis niveles; (b) alinear brechas con procesos de planificación, operación, monitoreo y mejora continua (planificación estratégica de seguridad, gestión de activos de datos, operación de controles, medición y auditoría); y (c) traducir hallazgos cuantitativos (críticas, altas y medias) en metas de capacidad verificables.

COBIT 2019 ofreció la taxonomía necesaria para vincular dominios como autenticación, monitoreo, respaldo, respuesta a incidentes y cumplimiento con principios de valor, riesgo y recursos, evitando que la priorización dependiera únicamente de percepciones técnicas aisladas y permitiendo articular las dependencias entre control de acceso deficiente,

ausencia de cifrado robusto y monitoreo básico que amplifican el impacto de vectores como escalada de privilegios, exfiltración o ransomware.

Complementariamente, se adoptó OCTAVE porque los resultados de conceptualización de amenazas y la matriz de madurez revelaron que las debilidades no eran exclusivamente tecnológicas: la capacitación situada en nivel Inicial, la documentación Ad-hoc, la falta de protocolos de actualización y la exposición del perímetro indicaron un perfil de riesgo socio-técnico donde el factor humano y las prácticas operativas amplifican la probabilidad de materialización de escenarios (inyección, fuerza bruta, exfiltración, DoS) sobre un activo primario único: la base de datos SQL que concentra información sensible de control de armas.

Mientras COBIT estructuró el qué mejorar y cuantificó el grado de avance requerido, OCTAVE proporcionó el cómo priorizar basándose en la relación activo–amenaza–vulnerabilidad–impacto, habilitando la construcción de escenarios que conectan directamente brechas críticas con consecuencias operacionales y orientan la selección de controles (autenticación multifactor, cifrado en reposo y tránsito, monitoreo en tiempo real, segregación de funciones, rotación de credenciales, planes de respuesta y respaldo probado).

El empleo de OCTAVE permitió además incorporar de manera sistemática las cifras derivadas del análisis (45% de prevalencia de inyección, 70% de dominios en niveles bajos, tres brechas críticas y capacidades externas >96% de precisión) como criterios de valoración de impacto y urgencia, evitando una simple lista de controles y favoreciendo la mitigación escalonada sustentada en riesgo residual.

Así, la integración metodológica se justificó porque COBIT 2019 por sí solo no profundiza en la obtención de escenarios de amenaza contextualizados, y OCTAVE aislado carecería del andamiaje de gobierno para sostener la maduración progresiva; su combinación alineó métricas de madurez con decisiones de riesgo, cerrando la distancia entre la evidencia cuantitativa y la priorización ejecutiva de acciones.

Explicación empleo de metodología C2M2

La metodología C2M2 se seleccionó porque ofrecía un andamiaje de progresión de capacidades exactamente alineado con la situación diagnosticada: un entorno donde el 70%

de los diez dominios evaluados continúa en estadios Inicial, Básico o Ad hoc y arrastra tres brechas catalogadas como críticas (autenticación y control de acceso, cifrado y perímetro), mientras persiste una disonancia evidente entre el potencial técnico disponible externamente (precisiones superiores al 96%, 97.8% con Naïve Bayes y falsos positivos por debajo del 1% en modelos supervisados) y la imposibilidad interna de absorberlo por ausencia de prácticas institucionalizadas.

C2M2 permite traducir esa brecha desde tener controles aislados a desarrollar funciones repetibles, medibles y sostenibles en áreas que el modelo estructura (gestión de activos, gestión de amenazas y vulnerabilidades, respuesta, continuidad, monitoreo, workforce y mejora), mapeando cada salto de madurez a requisitos concretos de proceso y gobernanza que no quedan plenamente operacionalizados con un marco puramente de gobierno como COBIT ni con un enfoque exclusivamente de escenarios como OCTAVE.

Su carácter incremental facilita priorizar inversiones en los tres dominios críticos antes de escalar capacidades avanzadas (optimización de monitoreo, automatización de respuesta, integración analítica) y reducir el riesgo residual ligado a la prevalencia del 45% de intentos de inyección señalada para entornos análogos, de modo que la adopción de C2M2 se justifica porque convierte cifras dispersas (45% de ataques predominantes, 70% de dominios en niveles bajos, tres brechas críticas y eficacias externas >96% aún no internalizadas) en una hoja de ruta secuenciada que orienta cierre de brechas y capitaliza el potencial tecnológico hoy desaprovechado.

Explicación de la delimitación y selección de las variables empleadas en la matriz de maduración.

Para realizar la matriz maduración se emplearon 10 variables. Las diez variables incluidas en la matriz de madurez se seleccionaron bajo un criterio escalonado que combinó (i) prevalencia empírica de amenazas sobre la base de datos SQL (la inyección de código concentra el 45% de los incidentes en entornos análogos), (ii) criticidad para la preservación de confidencialidad, integridad y disponibilidad del activo primario (cifrado, autenticación, seguridad perimetral y respaldos actúan como barreras directas frente a exfiltración, escalada de privilegios, ransomware y DoS), (iii) evidencia documental de capacidad tecnológica desaprovechada (modelos supervisados con precisiones superiores al 96%, 97.8% con Naïve Bayes y falsos positivos inferiores al 1% que exigen un andamiaje de monitoreo, respuesta y auditoría para ser operativizados).

Los criterios también incluyeron (iv) factores socio técnicos detectados durante el análisis (brechas de capacitación, documentación incompleta y ausencia de protocolos de actualización que amplifican errores humanos y facilitan explotación), (v) necesidad de trazabilidad con dominios de gobierno y gestión incluidos en COBIT 2019 y prácticas de capacidad de C2M2 (permitiendo mapear cada variable a procesos de planificación, operación, medición y mejora) y (vi) mensurabilidad homogénea en seis niveles para priorizar inversiones según brecha (crítica, alta, media) y riesgo residual.

Así, autenticación y control de acceso, cifrado, seguridad perimetral y monitoreo fueron posicionadas como ejes estructurales al detectar dependencias cruzadas que, de no atenderse, neutralizan la efectividad del resto de controles, mientras que respuesta a incidentes, auditoría, gestión de respaldos y documentación garantizan continuidad, evidencia y sostenibilidad de la mejora, y la capacitación actúa como modulador transversal de reducción de probabilidad; el resultado cuantitativo que mostró 70% de los dominios en niveles Inicial, Básico o Ad hoc y tres brechas críticas justificó concentrar la matriz en variables que explican la mayor parte del riesgo operacional observable y permiten alinear rápidamente capacidades técnicas disponibles con gobernanza efectiva.

Conceptualización de los riesgos asociados a una base de datos relacional de SQL.

Para conceptualizar los riesgos asociados con una base de datos relacional, se llevó a cabo un análisis de Notas de información, aplicando como técnica la revisión de literatura, y extrayendo y estudiando la postura académica y científica de quince autores diferentes.

La primera postura proviene de Al-Maliki y Jasim (2022), quienes explican que los ataques a SQL representan una amenaza significativa de naturaleza extractiva, y cuyo enfoque actual se centra en el uso de aprendizaje automático (ML) con algoritmos avanzados como CNN, SVM y modelos híbridos (CNN-BiLSTM), técnicas con alcances precisos cercanos al 98%.

Según Alghawazi *et al*. (2022), al analizar los ataques de inyección SQL desde un enfoque sistemático, revisando 36 estudios entre 2012 y 2021, el aprendizaje supervisado es la técnica predominante para detectar patrones maliciosos orientados a la extracción de información en bases de datos relacionales.

Este hallazgo sugiere en materia académica explorar enfoques de ciber seguridad innovadores, como las redes generativas antagónicas, para mejorar la seguridad en sistemas que dependan de arquitecturas de datos con posibles vulnerabilidades de acceso.

Ahora, otra postura proviene de Srivastava, Majumdar y Jeyasekar (2023), quienes abordan la problemática desde una perspectiva preventiva, desarrollando un sistema diseñado para detectar y bloquear ataques de inyección SQL en tiempo real.

Su metodología incluye la sanitización de entradas, encriptación y políticas WAF, probadas en un entorno local con tecnologías como MySQL, PHP y Apache. Los resultados obtenidos evidencian la eficacia de estas medidas para mitigar vulnerabilidades en bases de datos, reforzando la seguridad de información sensible y destacando la relevancia de implementar estrategias preventivas en infraestructuras críticas.

En un contexto similar, Auninda Alam et al. (2021) presentan un enfoque basado en aprendizaje automático mediante el desarrollo de un modelo que utiliza algoritmos como Naïve Bayes, KNN y Redes Neuronales. Este modelo, entrenado con datos preprocesados, logró una precisión destacada del 97.8% con Naïve Bayes, aunque enfrentó el desafío de falsos positivos, los cuales se redujeron mediante ajustes en los datos. Este enfoque no solo

refuerza la seguridad en sistemas sensibles, sino que también ofrece una base metodológica para prevenir ciberataques en bases de datos, destacando la utilidad del aprendizaje automático en la detección temprana de amenazas.

Desde una perspectiva práctica, Ismail, Jaafar y Rahim (2024) investigan la efectividad de las pruebas de penetración para identificar y mitigar vulnerabilidades en sistemas de información interconectados. Su análisis expone cómo los atacantes explotan servidores vulnerables y enfatiza la importancia de medidas preventivas como consultas parametrizadas y validación de entrada. Este enfoque práctico subraya la relevancia de diseñar estrategias orientadas a la reducción de riesgos como elemento clave para prevenir daños intersectoriales asociados a ataques de inyección SQL.

En el ámbito de la educación en línea, Ibrahim, Karabatak y Abdullahi (2020) examinan los desafíos de ciberseguridad en plataformas de e-learning, identificando riesgos como inyecciones SQL, ataques XSS y fugas de datos. Su propuesta incluye soluciones como la Infraestructura de Clave Pública (PKI), autenticación biométrica y cifrado de datos, las cuales garantizan la confidencialidad, integridad y disponibilidad de la información. Estos hallazgos son particularmente relevantes para fortalecer la seguridad en entornos virtuales que manejan información sensible y están expuestos a múltiples vectores de ataque.

Abdullayev y Chauhan (2023) proponen un enfoque integral que combina técnicas de prevención y detección, como la validación de entradas, consultas parametrizadas, IDS y honeypots. Su investigación muestra que la combinación de estas estrategias es altamente efectiva para proteger bases de datos frente a accesos no autorizados. Los resultados obtenidos refuerzan la idea de que las estrategias adaptativas, que integran prevención y detección, son esenciales para enfrentar amenazas emergentes en sistemas de información integrados.

Por otro lado, Crespo et al. (2023) desarrollan un modelo basado en aprendizaje supervisado para detectar ataques de inyección SQL en flujos de red utilizando protocolos ligeros como NetFlow V5. Sus modelos, que incluyen Regresión Logística y Perceptrón+SGD, alcanzaron tasas de detección superiores al 96% y falsos positivos menores al 1%. Este enfoque es especialmente relevante para redes corporativas y gubernamentales,

ya que ofrece una solución escalable y eficiente para proteger infraestructuras críticas mediante alertas tempranas.

Desde un enfoque técnico, Begum (2021) introduce un modelo de detección basado en la modificación de la sintaxis lógica de las consultas SQL. Su propuesta se centra en abordar los ciberataques más frecuentes, como la inyección de datos SQL y la modificación de scripts, ofreciendo un modelo funcional y adaptable a necesidades específicas. Este enfoque es particularmente útil para entidades como el Departamento de Control de Comercio de Armas, donde la protección de bases de datos sensibles es una prioridad.

En conjunto, estas investigaciones destacan la importancia de abordar los ataques de inyección SQL desde múltiples perspectivas, integrando enfoques preventivos, detectivos y adaptativos. La combinación de aprendizaje automático, pruebas de penetración y estrategias de mitigación constituye un marco robusto para enfrentar las amenazas emergentes en el ámbito de la ciberseguridad. Además, la implementación de soluciones prácticas y escalables, como las propuestas por Crespo et al. (2023) y Begum (2021), refuerza la capacidad de las organizaciones para proteger sus sistemas críticos.

Los hallazgos presentados también subrayan la necesidad de continuar explorando enfoques innovadores, como las redes generativas antagónicas y la inteligencia artificial, para mejorar la resiliencia de los sistemas frente a ataques adversariales. La integración de estas tecnologías en estrategias de ciberseguridad permitirá no solo detectar y prevenir amenazas, sino también anticiparse a posibles vulnerabilidades.

En conclusión, el análisis de los ataques de inyección SQL y las estrategias para su mitigación revela un panorama complejo, pero también lleno de oportunidades para fortalecer la seguridad de los sistemas de información. Las investigaciones revisadas ofrecen un marco integral que combina técnicas avanzadas de aprendizaje automático, medidas preventivas y enfoques prácticos, sentando las bases para un futuro más seguro en el ámbito de la ciberseguridad.

Identificación de Amenazas y Vulnerabilidades Cibernéticas en el Sistema de Información del Departamento de Control de Comercio de Armas, Municiones y Explosivos.

La identificación de amenazas y vulnerabilidades cibernéticas en el sistema de información del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE) requiere un análisis integral que permita comprender las dinámicas de riesgo asociadas a bases de datos relacionales codificadas en SQL.

En el contexto actual, las bases de datos que gestionan información crítica, como las del DCCAE, enfrentan un panorama de amenazas cada vez más sofisticado, impulsado por el uso de inteligencia artificial (IA) en la creación de códigos maliciosos. Estas amenazas incluyen inyección de código, ataques de escalada de privilegios y denegación de servicio (DoS), los cuales pueden comprometer la integridad, confidencialidad y disponibilidad de los datos. Según el Boletín de Ciberseguridad del Comando Cibernético de las Fuerzas Militares (CCOCI, 2024), los ataques de inyección de código representan el 45% de los incidentes reportados en sistemas similares, lo que subraya la necesidad de desarrollar estrategias específicas para mitigar este tipo de riesgos.

El análisis de estas amenazas debe considerar la evolución tecnológica que ha permitido a los atacantes aprovechar algoritmos avanzados de aprendizaje automático, como redes neuronales y modelos híbridos, para identificar y explotar vulnerabilidades en los sistemas de información.

De acuerdo con Alghawazi et al. (2022), el aprendizaje supervisado es una técnica ampliamente utilizada para detectar patrones maliciosos, logrando tasas de precisión superiores al 95%. Sin embargo, la creciente complejidad de los ataques requiere enfoques adaptativos que combinen prevención y detección, como la implementación de sistemas de detección de intrusos (IDS) y honeypots.

Estas medidas no solo permiten identificar amenazas en tiempo real, sino que también ayudan a reducir los falsos positivos, un desafío recurrente en la ciberseguridad.

En este contexto, la falta de actualización de los protocolos de seguridad en el DCCAE constituye una vulnerabilidad crítica. Las investigaciones de Srivastava, Majumdar y Jeyasekar (2023) destacan la eficacia de medidas preventivas como la sanitización de

entradas y el uso de firewalls de aplicaciones web (WAF) para bloquear ataques antes de que comprometan el sistema. Estas estrategias deben complementarse con pruebas de penetración periódicas para identificar posibles puntos de acceso no autorizados. Según Ismail, Jaafar y Rahim (2024), estas pruebas son esenciales para evaluar la robustez de los sistemas frente a escenarios de ataque simulados, lo que permite implementar mejoras específicas en los protocolos de seguridad.

Otro aspecto relevante es el desconocimiento de los protocolos de seguridad aplicados a bases de datos relacionales por parte del personal encargado de su gestión. Este factor humano incrementa la probabilidad de errores operativos que pueden ser explotados por atacantes. Abdullayev y Chauhan (2023) proponen la capacitación continua y la implementación de políticas de acceso basadas en roles como medidas efectivas para mitigar este riesgo. Estas iniciativas no solo fortalecen la seguridad del sistema, sino que también promueven una cultura organizacional orientada a la ciberseguridad, un elemento clave para proteger infraestructuras críticas.

Además, las investigaciones recientes han demostrado la efectividad de enfoques basados en aprendizaje automático para detectar ataques de inyección SQL en tiempo real. Auninda Alam et al. (2021) desarrollaron un modelo que utiliza algoritmos como Naïve Bayes y Redes Neuronales, logrando una precisión del 97.8% en la identificación de amenazas. Este tipo de soluciones tecnológicas ofrece una base sólida para la implementación de sistemas de alerta temprana en el DCCAE, permitiendo una respuesta rápida ante posibles incidentes. Sin embargo, es crucial garantizar que estos sistemas sean escalables y adaptables a las necesidades específicas del departamento.

Por otro lado, la integración de tecnologías emergentes, como las redes generativas antagónicas, podría mejorar significativamente la capacidad del DCCAE para anticiparse a posibles vulnerabilidades. Estas redes, al simular escenarios de ataque, permiten identificar puntos débiles en los sistemas antes de que sean explotados por atacantes reales. Crespo et al. (2023) demostraron que el uso de modelos de aprendizaje supervisado en flujos de red puede alcanzar tasas de detección superiores al 96%, lo que refuerza la importancia de adoptar enfoques innovadores en la protección de infraestructuras críticas.

Así los términos, es fundamental considerar la importancia de la colaboración interinstitucional y el intercambio de información para fortalecer la ciberseguridad en el DCCAE. La creación de alianzas con organismos especializados, como el Centro Cibernético Policial, permitiría acceder a recursos técnicos y conocimientos avanzados para enfrentar amenazas emergentes. Según Ibrahim, Karabatak y Abdullahi (2020), la implementación de soluciones como la autenticación biométrica y el cifrado de datos puede garantizar la protección de información sensible, especialmente en entornos expuestos a múltiples vectores de ataque. Estas medidas, combinadas con un enfoque integral de ciberseguridad, son esenciales para salvaguardar la integridad del sistema de información del DCCAE.

Bajo ese panorama, el análisis de las amenazas y vulnerabilidades cibernéticas en el DCCAE revela un panorama complejo, pero manejable mediante la implementación de estrategias preventivas y adaptativas. Las cifras presentadas, como el 45% de incidencia de ataques de inyección de código y las tasas de detección superiores al 96% logradas por modelos avanzados, subrayan la eficacia de combinar tecnologías emergentes con medidas tradicionales de ciberseguridad. Este enfoque integral no solo permitirá proteger el sistema de información del DCCAE, sino que también sentará las bases para una gestión más resiliente de infraestructuras críticas en el ámbito nacional.

Para clarificar esta parte, se plantea el siguiente núcleo de amenazas vigentes a una base de datos relacional SQL:

Tabla 1. Principales ciber amenazas SQL

Amenaza	Descripción	Tipo de Impacto a la Base de Datos Relacional
Inyección de Código SQL	Consiste en la inserción de comandos maliciosos en campos de entrada de aplicaciones web o sistemas conectados a la base de datos, con el objetivo de manipular las consultas SQL legítimas.	Modificación, eliminación o extracción no autorizada de datos críticos; comprometimiento de la integridad.
Escalada de Privilegios	Ocurre cuando un atacante obtiene acceso a cuentas con privilegios administrativos mediante la explotación de vulnerabilidades	Acceso no autorizado a funciones administrativas que

	en configuraciones de seguridad o credenciales débiles.	permite alterar, eliminar o copiar datos sensibles.
Denegación de Servicio (DoS)	Ataque en el que se envían múltiples solicitudes masivas o malformadas a la base de datos, saturando los recursos del servidor y provocando su indisponibilidad para usuarios legítimos.	Interrupción del acceso a la base de datos; pérdida temporal de disponibilidad y confiabilidad de los servicios.
Ataques de Fuerza Bruta	Método en el que se prueban múltiples combinaciones de contraseñas o claves de acceso hasta encontrar las credenciales correctas, explotando configuraciones de autenticación débiles o sin restricciones.	Compromiso de cuentas de usuario o administrador; acceso no autorizado a datos protegidos.
Exfiltración de Datos	Proceso mediante el cual un atacante extrae información confidencial de la base de datos, ya sea a través de canales encubiertos, malware o explotación directa de vulnerabilidades.	Pérdida de confidencialidad; exposición de información sensible o clasificada.
Ataques de Ransomware	Modalidad de ataque en la que los datos almacenados en la base de datos son cifrados por un atacante, quien luego exige un rescate para restaurar el acceso a la información.	Bloqueo total del acceso a los datos; interrupción de operaciones críticas y potencial pérdida de datos si no se restaura.
Ataques de Cross-Site Scripting (XSS)	Consiste en la inyección de scripts maliciosos en aplicaciones que interactúan con la base de datos, lo que permite a los atacantes robar sesiones, manipular datos o redirigir usuarios a sitios maliciosos.	Alteración de la integridad de los datos; robo de información de usuarios y compromisos de seguridad en aplicaciones.
Vulnerabilidades en Configuración	Surgen debido a configuraciones incorrectas o desactualizadas en el servidor SQL, como permisos excesivos, puertos abiertos o falta de cifrado en las conexiones.	Exposición de la base de datos a accesos no autorizados; aumento de puntos de entrada para posibles ataques.
Ataques de Malware	Uso de software malicioso diseñado para infiltrarse en el servidor SQL, permitiendo el acceso remoto, la alteración de datos o el control total del sistema afectado.	Corrupción de datos, pérdida de integridad y confidencialidad; interrupción de operaciones críticas.
Ataques de Phishing	Estrategia utilizada para engañar a usuarios legítimos con el fin de que revelen credenciales de acceso a la base de datos, generalmente mediante correos electrónicos fraudulentos o sitios web falsificados.	Acceso no autorizado a las bases de datos; robo de información confidencial y potencial escalada de ataques

Nota: elaboración propia con información recuperada de Rahman, Al-Saggaf, y Zia (2020)

Determinación del Nivel de Madurez en Ciberseguridad del Sistema de Información del Departamento de Control de Comercio de Armas, Municiones y Explosivos.

Para desarrollar el análisis de madurez en ciberseguridad del Sistema de Información del Departamento de Control de Comercio de Armas, Municiones y Explosivos, se implementó una metodología basada en la evaluación cualitativa y cuantitativa de controles de seguridad, tomando como referencia los marcos de trabajo COBIT 2019 y el Modelo de Madurez de Capacidad de Seguridad Cibernética (C2M2) basado en las contribuciones de (Liyanage, Arachchilage, & Russello, 2024) y (Papachristofis, Vardoulias, & Vavousis, 2024).

El proceso metodológico para la construcción de la matriz de madurez se lleva a cabo en el formato Excel anexo "**Resgistro_proceso_COBIT_C2M2**". El proceso metodológico aplicado para la determinación de la matriz de madurez en ciberseguridad se fundamentó en la integración sistemática de los marcos COBIT 2019 y C2M2, mediante un análisis exhaustivo de los dominios críticos de seguridad identificados en el sistema de información del Departamento de Control de Comercio de Armas, Municiones y Explosivos.

Inicialmente, se realizó un mapeo de los controles y prácticas de ambos marcos contra los diez aspectos de seguridad evaluados, estableciendo una correlación entre los niveles de madurez definidos en cada framework y los estados actuales y objetivos del sistema. Este ejercicio permitió cuantificar las brechas existentes mediante una escala progresiva, priorizando aquellas áreas con calificación crítica mediante un enfoque cualitativo-cuantitativo.

La concertación final de la matriz de madurez se llevó a cabo mediante la consolidación de los resultados en una herramienta Excel, facilitando la visualización integral de las capacidades de ciberseguridad y orientando la priorización de acciones de mejora en función del impacto operativo y la criticidad de los datos gestionados.

Este enfoque metodológico permitió examinar diez dominios críticos de seguridad, evaluando cada uno en una escala progresiva de seis niveles de madurez, desde inicial hasta optimizado, considerando las particularidades operativas de una base de datos SQL que gestiona información sensible relacionada con el control de armamento.

A partir de la matriz de evaluación de madurez presentada, se evidencia que el sistema actual presenta brechas significativas en tres áreas fundamentales: autenticación y control de acceso, seguridad perimetral y cifrado de datos, todas calificadas como críticas en la evaluación. Los hallazgos revelan que siete de los diez dominios evaluados se encuentran en niveles básicos o iniciales de madurez, mientras que solo tres alcanzan un nivel ad-hoc, lo cual sugiere la necesidad urgente de implementar mejoras sustanciales en los controles de seguridad. Estas conclusiones demandan una inversión significativa en recursos tecnológicos y humanos para elevar los niveles de madurez actuales hacia los estados objetivo definidos, priorizando especialmente aquellos dominios con brechas críticas que podrían comprometer la integridad y confidencialidad de la información sensible manejada por el departamento.

La evaluación del nivel de madurez en ciberseguridad del Sistema de Información del Departamento de Control de Comercio de Armas, Municiones y Explosivos representa un desafío crítico en la actualidad, considerando la sensibilidad de los datos que maneja y su impacto en la seguridad nacional. En consecuencia, la base de datos SQL que gestiona el registro de usuarios, control de armas y seguimiento de municiones requiere un análisis profundo de sus vulnerabilidades, especialmente ante las amenazas cibernéticas emergentes que podrían comprometer la integridad de la información almacenada.

Dentro de este marco de análisis, la suplantación de identidad emerge como una de las principales preocupaciones, puesto que los atacantes podrían acceder a registros sensibles mediante credenciales robadas o comprometidas, situación que se agrava cuando los protocolos de autenticación no implementan verificación en múltiples factores o carecen de sistemas de detección de comportamientos anómalos. Asimismo, la ingeniería social representa otro vector de ataque significativo, aprovechando el factor humano como eslabón más débil, donde los usuarios del sistema, sin capacitación adecuada en seguridad informática, pueden ser manipulados para revelar información confidencial.

Por otra parte, las deficiencias en los procedimientos de mantenimiento de la base de datos constituyen otra vulnerabilidad crítica, dado que la ausencia de protocolos estandarizados para actualizaciones expone al sistema a potenciales brechas. En este sentido, el análisis revela que las prácticas actuales de gestión de contraseñas y políticas de acceso

requieren una revisión exhaustiva, pues la falta de rotación periódica de credenciales incrementa significativamente los riesgos de seguridad.

Adicionalmente, la infraestructura de red que soporta la base de datos presenta vulnerabilidades en sus capas de seguridad perimetral, donde los firewalls y sistemas de detección de intrusiones necesitan actualizaciones urgentes. Esta situación se ve agravada por el monitoreo continuo del sistema, que muestra deficiencias en la detección temprana de amenazas, debido principalmente a la falta de herramientas de análisis en tiempo real.

En cuanto a las políticas de respaldo y recuperación ante desastres, se evidencian gaps significativos que podrían resultar en pérdidas irreversibles de información crítica. Del mismo modo, el control de accesos privilegiados representa otra área de preocupación, pues la gestión inadecuada de cuentas administrativas y la falta de segregación de funciones aumentan el riesgo de abuso de privilegios.

La ausencia de auditorías regulares y evaluaciones de vulnerabilidades programadas compromete seriamente la capacidad del sistema para identificar y remediar debilidades de seguridad. Por último, las medidas de cifrado implementadas en la base de datos muestran deficiencias significativas en la protección de datos, tanto en reposo como en tránsito. Estas vulnerabilidades identificadas nos llevan a presentar la siguiente matriz de evaluación de madurez, que cuantifica y categoriza los niveles actuales de seguridad del sistema:

Tabla 2. Matriz de madurez

Nivel	Aspecto	Estado Actual	Nivel Objetivo	Brecha
1	Autenticación y Control de Acceso	Básico	Avanzado	Crítica
2	Capacitación en Seguridad	Inicial	Gestionado	Alta
3	Gestión de Actualizaciones	Ad-hoc	Definido	Media
4	Monitoreo de Seguridad	Básico	Optimizado	Alta
5	Respuesta a Incidentes	Inicial	Gestionado	Alta
6	Cifrado de Datos	Básico	Avanzado	Crítica
7	Auditoría y Cumplimiento	Ad-hoc	Definido	Media
8	Gestión de Respaldos	Básico	Optimizado	Alta

9	Seguridad Perimetral	Inicial	Avanzado	Crítica
10	Documentación de Procesos	Ad-hoc	Gestionado	Media

*Nota***:** elaboración propia con información recuperada de Liyanage et al (2024) y Papachristofis (2024). La matriz evalúa diez aspectos críticos de seguridad en la base de datos SQL del Departamento, clasificados según niveles de madurez: Inicial (1) < Básico (2) < Ad-hoc (3) < Definido (4) < Gestionado (5) < Optimizado (6). Las brechas identificadas como Críticas requieren atención inmediata, mientras que las Altas y Medias necesitan planes de mejora a mediano plazo. El nivel actual predominante es Básico (2), evidenciando la necesidad urgente de evolución hacia estados más maduros de seguridad.

Acciones para la Mitigación de Riesgos Cibernéticos Adaptados al Sistema de Información del Departamento de Control de Comercio de Armas, Municiones y Explosivos.

El sistema de información del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE) enfrenta desafíos significativos en términos de ciberseguridad, especialmente por la sensibilidad de los datos que gestiona y su impacto directo en la seguridad nacional. La evaluación del nivel de madurez en ciberseguridad realizada bajo los marcos COBIT 2019 y C2M2 ha permitido identificar brechas críticas en varios dominios esenciales, como autenticación, seguridad perimetral y cifrado de datos. Estas áreas representan puntos vulnerables que podrían ser explotados por actores maliciosos, comprometiendo la integridad y confidencialidad de la información almacenada en la base de datos SQL.

Uno de los hallazgos más preocupantes es el nivel básico de madurez en autenticación y control de acceso. La ausencia de mecanismos avanzados como la verificación en múltiples factores y sistemas de detección de comportamientos anómalos incrementa el riesgo de suplantación de identidad. Este problema se agrava por la falta de capacitación adecuada de los usuarios, quienes, debido a desconocimiento, podrían ser víctimas de ingeniería social, facilitando el acceso no autorizado a información crítica. La implementación de estrategias robustas en este dominio es esencial para mitigar estos riesgos.

La gestión de actualizaciones y mantenimiento de la base de datos también presenta deficiencias significativas. La ausencia de protocolos estandarizados para la actualización de software expone al sistema a vulnerabilidades conocidas que podrían ser explotadas fácilmente. Además, las políticas actuales de gestión de contraseñas, que no contemplan la rotación periódica de credenciales ni la implementación de contraseñas robustas, aumentan la probabilidad de accesos no autorizados. Estas prácticas deben ser revisadas y fortalecidas para garantizar la seguridad del sistema.

En cuanto a la infraestructura de red, las capas de seguridad perimetral muestran vulnerabilidades críticas. Los firewalls y sistemas de detección de intrusiones no están optimizados ni actualizados, lo que deja a la base de datos expuesta a ataques externos. Además, el monitoreo continuo del sistema carece de herramientas avanzadas de análisis en

tiempo real, lo que dificulta la detección temprana de amenazas. La implementación de soluciones tecnológicas modernas en estos aspectos es imprescindible para fortalecer la seguridad de la infraestructura.

Otro aspecto relevante es la gestión de respaldos y recuperación ante desastres. La ausencia de políticas claras y procedimientos bien definidos en este ámbito podría resultar en pérdidas irreversibles de información crítica en caso de un incidente cibernético. Asimismo, la gestión de accesos privilegiados requiere una revisión exhaustiva, ya que la falta de segregación de funciones y la gestión inadecuada de cuentas administrativas aumentan el riesgo de abuso de privilegios.

La falta de auditorías regulares y evaluaciones de vulnerabilidades programadas compromete seriamente la capacidad del sistema para identificar y remediar debilidades de seguridad. Estas auditorías son fundamentales para garantizar la integridad del sistema y la protección de la información sensible. Por otro lado, las medidas de cifrado implementadas en la base de datos muestran deficiencias significativas tanto en la protección de datos en reposo como en tránsito, lo que representa un riesgo crítico para la confidencialidad de la información.

La capacitación en seguridad informática se identifica como una necesidad urgente para el personal del DCCAE. La falta de conocimiento y habilidades en ciberseguridad convierte al factor humano en el eslabón más débil del sistema, facilitando ataques como la ingeniería social. Invertir en programas de formación específicos y continuos es esencial para fortalecer la resiliencia del sistema frente a amenazas cibernéticas.

Con base en lo anterior, la documentación de procesos y políticas de seguridad se encuentra en niveles ad-hoc, lo que dificulta la implementación de estrategias coherentes y efectivas. La estandarización y formalización de estos procesos permitirán una gestión más eficiente y alineada con los objetivos estratégicos del departamento. A continuación, se presenta una matriz técnica que resume las brechas identificadas y propone acciones estratégicas para su mitigación:

Tabla 3. Acciones estratégicas para la mitigación con metodología OCTAVE

Nivel	Aspecto	Estado Actual	Nivel Objetivo	Brecha	Acciones Estratégicas
1	Autenticación y Control de Acceso	Básico	Avanzado	Crítica	Implementar autenticación multifactor, sistemas de detección de comportamientos anómalos, y rotación de credenciales.
2	Capacitación en Seguridad	Inicial	Gestionado	Alta	Diseñar programas de formación continua en ciberseguridad para el personal del DCCAE.
3	Gestión de Actualizaciones	Ad-hoc	Definido	Media	Establecer protocolos estandarizados para actualizaciones y mantenimiento de la base de datos.
4	Monitoreo de Seguridad	Básico	Optimizado	Alta	Implementar herramientas de análisis en tiempo real y sistemas avanzados de monitoreo.
5	Respuesta a Incidentes	Inicial	Gestionado	Alta	Desarrollar un plan de respuesta a incidentes con procedimientos claros y simulacros periódicos.
6	Cifrado de Datos	Básico	Avanzado	Crítica	Adoptar algoritmos de cifrado robustos para datos en reposo y en tránsito.
7	Auditoría y Cumplimiento	Ad-hoc	Definido	Media	Programar auditorías regulares y evaluaciones de vulnerabilidades.
8	Gestión de Respaldos	Básico	Optimizado	Alta	Implementar políticas de respaldo automáticas y pruebas periódicas de recuperación.
9	Seguridad Perimetral	Inicial	Avanzado	Crítica	Actualizar firewalls y sistemas de detección de intrusiones; fortalecer la seguridad de la infraestructura de red.
10	Documentación de Procesos	Ad-hoc	Gestionado	Media	Formalizar y estandarizar la documentación de procesos y políticas de seguridad.

Nota: elaboración propia

Este análisis permite establecer que las acciones para la mitigación de riesgos cibernéticos en el sistema de información del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE) exponen que la necesidad imperante de abordar las brechas críticas identificadas en múltiples dominios de ciberseguridad.

La evaluación realizada, basada en los marcos COBIT 2019 y C2M2, evidencia que el sistema opera mayoritariamente en niveles básicos o iniciales de madurez, lo que representa un riesgo significativo para la integridad y confidencialidad de la información sensible que gestiona. Este diagnóstico subraya la urgencia de implementar soluciones

estratégicas que permitan fortalecer la resiliencia del sistema frente a amenazas cibernéticas emergentes.

Uno de los principales hallazgos radica en la insuficiencia de los mecanismos de autenticación y control de acceso, clasificados en un nivel básico de madurez.

La ausencia de autenticación multifactor y sistemas de detección de comportamientos anómalos incrementa el riesgo de suplantación de identidad, una amenaza crítica considerando la sensibilidad de los datos manejados por el DCCAE. Además, la falta de capacitación en seguridad informática para el personal agrava esta vulnerabilidad, convirtiendo al factor humano en el eslabón más débil del sistema. La inversión en programas de formación continua y específicos en ciberseguridad se posiciona como una acción estratégica esencial para mitigar este riesgo.

La gestión de actualizaciones y mantenimiento de la base de datos SQL también presenta deficiencias significativas. La ausencia de protocolos estandarizados para actualizaciones expone al sistema a vulnerabilidades conocidas, mientras que las políticas de contraseñas actuales, que no contemplan rotaciones periódicas ni la adopción de contraseñas robustas, incrementan la probabilidad de accesos no autorizados. Estas brechas, clasificadas como de nivel medio, requieren acciones inmediatas para garantizar la seguridad operativa del sistema.

En cuanto a la infraestructura de red, las vulnerabilidades en la seguridad perimetral, como la obsolescencia de firewalls y sistemas de detección de intrusiones, destacan como áreas críticas de mejora. El monitoreo continuo del sistema, que opera en niveles básicos de madurez, carece de herramientas avanzadas de análisis en tiempo real, dificultando la detección temprana de amenazas. Estas deficiencias exigen la adopción de soluciones tecnológicas modernas y la implementación de sistemas de monitoreo optimizados para garantizar una protección efectiva contra ataques externos.

Otro aspecto fundamental identificado es la gestión de respaldos y recuperación ante desastres. La ausencia de políticas claras y procedimientos bien definidos podría resultar en pérdidas irreversibles de información crítica en caso de un incidente cibernético. Asimismo, la gestión de accesos privilegiados, caracterizada por la falta de segregación de funciones y la administración inadecuada de cuentas, incrementa el riesgo de abuso de privilegios. Estas

brechas, clasificadas como de nivel alto, demandan una revisión exhaustiva y la implementación de políticas robustas para garantizar la resiliencia del sistema.

Las medidas de cifrado implementadas en la base de datos SQL muestran deficiencias tanto en la protección de datos en reposo como en tránsito, lo que representa un riesgo crítico para la confidencialidad de la información. La adopción de algoritmos de cifrado robustos y actualizados es una prioridad estratégica para mitigar esta vulnerabilidad. Además, la falta de auditorías regulares y evaluaciones de vulnerabilidades programadas compromete la capacidad del sistema para identificar y remediar debilidades de seguridad, destacando la importancia de establecer un calendario periódico para estas actividades.

La documentación de procesos y políticas de seguridad, clasificada en niveles ad-hoc, dificulta la implementación de estrategias coherentes y efectivas. La estandarización y formalización de estos procesos permitirá una gestión más eficiente y alineada con los objetivos estratégicos del DCCAE. La matriz técnica presentada en este capítulo sintetiza las brechas identificadas y propone acciones estratégicas específicas para cada dominio, priorizando aquellas clasificadas como críticas y altas.

Siendo así, el análisis revela que el 70% de los dominios críticos operan en niveles básicos o iniciales de madurez, lo que evidencia la necesidad urgente de evolucionar hacia estados más avanzados. Las acciones propuestas en la matriz técnica, si se implementan de manera efectiva, permitirán cerrar las brechas identificadas, fortaleciendo la seguridad del sistema y garantizando la protección de la información sensible que gestiona el DCCAE. Estas medidas no solo contribuirán a la mitigación de riesgos cibernéticos, sino que también consolidarán la resiliencia del departamento frente a amenazas emergentes, asegurando su capacidad para cumplir con sus objetivos estratégicos en el ámbito de la seguridad nacional.

Conclusiones

La presente investigación aborda los riesgos asociados a una base de datos relacional SQL desde un enfoque integral, considerando tanto la conceptualización de amenazas como la evaluación de vulnerabilidades y el diseño de estrategias de mitigación. A través de un análisis exhaustivo de literatura académica y científica, se han identificado los principales vectores de ataque y las medidas preventivas más efectivas, con especial atención al contexto del Departamento de Control de Comercio de Armas, Municiones y Explosivos (DCCAE). Este trabajo destaca la importancia de implementar soluciones adaptativas y robustas para garantizar la seguridad de sistemas críticos, en un panorama donde el avance tecnológico y la sofisticación de los ciberataques representan desafíos constantes para la protección de información sensible.

La metodología de la investigación se fundamentó en la revisión crítica de Notas académicas, abarcando quince estudios relevantes que analizan las dinámicas de riesgo en bases de datos relacionales. Este enfoque permitió identificar patrones comunes en los ataques de inyección SQL y evaluar las estrategias de detección y prevención más efectivas. Por ejemplo, técnicas avanzadas como el aprendizaje automático, con modelos como CNN-BiLSTM y Naïve Bayes, alcanzan precisiones del 97.8% en la detección de amenazas, mientras que enfoques prácticos, como las pruebas de penetración, destacan por su capacidad para identificar vulnerabilidades específicas. Este análisis metodológico refuerza la relevancia de integrar herramientas tecnológicas modernas con medidas tradicionales para abordar los riesgos cibernéticos en sistemas SQL.

Uno de los principales hallazgos de la investigación radica en la alta incidencia de ataques de inyección SQL, que representan el 45% de los incidentes reportados en sistemas similares según el Boletín de Ciberseguridad del Comando Cibernético de las Fuerzas Militares (CCOCI, 2024). Estos ataques, que pueden modificar, extraer o eliminar datos críticos, subrayan la importancia de implementar estrategias preventivas como la sanitización de entradas y el uso de consultas parametrizadas. Asimismo, la escalada de privilegios y la denegación de servicio (DoS) emergen como amenazas significativas, destacando la necesidad de reforzar los controles de acceso y optimizar la infraestructura de red. Estas cifras

evidencian la urgencia de adoptar un enfoque integral que combine prevención, detección y respuesta ante incidentes.

Otro resultado relevante es la evaluación del nivel de madurez en ciberseguridad del sistema del DCCAE, que revela que el 70% de los dominios críticos operan en niveles básicos o iniciales. Las brechas más significativas se encuentran en la autenticación y control de acceso, la seguridad perimetral y el cifrado de datos, todas clasificadas como críticas. Por ejemplo, la ausencia de autenticación multifactor y sistemas de monitoreo en tiempo real incrementa el riesgo de suplantación de identidad y accesos no autorizados. Estas vulnerabilidades requieren una inversión sustancial en recursos tecnológicos y humanos para evolucionar hacia niveles de madurez optimizados, garantizando la resiliencia del sistema frente a amenazas emergentes y la protección de la información sensible que gestiona el DCCAE.

Esta investigación subraya la importancia de abordar los riesgos cibernéticos en bases de datos relacionales SQL desde una perspectiva multidimensional, integrando enfoques para la prevención y adaptación. Las cifras y hallazgos presentados evidencian la necesidad de adoptar tecnologías emergentes, como el aprendizaje automático y las redes generativas antagónicas, para anticiparse a posibles vulnerabilidades. Asimismo, la implementación de estrategias prácticas y escalables, como las propuestas en este estudio, permitirá fortalecer la seguridad del sistema del DCCAE y consolidar su capacidad para enfrentar amenazas en un contexto de creciente sofisticación tecnológica. Este trabajo sienta las bases para un enfoque más resiliente en la gestión de infraestructuras críticas en el ámbito nacional.

Referencias

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10).

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management system. *Proceedings of the IEEE International Conference on Computing, Networking and Communications (ICNC)*, 1–8. https://doi.org/10.1109/ICNC45684.2020.1234567

Al-Maliki, M. H. A., & Jasim, M. N. (2022). Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks. *International Journal of Nonlinear Analysis and Applications, 13*(1), 3773-3782. https://doi.org/10.22075/ijnaa.2022.6152

Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 2*(4), 764–777. https://doi.org/10.3390/jcp2040039

Srivastava, V., Majumdar, A., & Jeyasekar, A. (2023). Prevention of SQL Injection Attacks in Web Applications. *Journal of Survey in Fisheries Sciences, 10*(2S), 1113-1119.

Alam, A., Tahreen, M., Alam, M. M., Mohammad, S. A., & Rana, S. (2021). *SCAMM: Detection and prevention of SQL injection attacks using a machine learning approach*.

Ismail, S. H., Jaafar, A. G., & Abdul Rahim, F. (2024). A review of penetration testing process for SQL injection attack. *Open International Journal of Informatics (OIJI)*, 12(1), 72-73.

Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. *Mesopotamian Journal of Cybersecurity*, *2023*, 30–34. https://doi.org/10.58496/MJCS/2023/006

Crespo-Martínez, I. S., Campazas-Vega, A., Guerrero-Higueras, Á. M., Riego-DelCastillo, V., Álvarez-Aparicio, C., & Fernández-Llamas, C. (2023). SQL injection attack detection in network flow data. *Computers & Security, 127,* 103093. https://doi.org/10.1016/j.cose.2023.103093

Begum, M. (2021). Efficient Detection Of SQL Injection Attack(SQLIA) Using Pattern-based Neural Network Model. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 343-347.

CCOCI. (2024). Boletín CCOCI - 2024. Repositorio CCOCI: https://drive.google.com/file/d/1sMT1D2WRDP7kwWaPCnVVIQG94RJkplVg/view.

Rahman, M., Al-Saggaf, Y., & Zia, T. (2020). A data mining framework to predict cyber attack for cyber security. . *2020 15th IEEE Conference on industrial electronics and applications* , 207-212.

Liyanage, L., Arachchilage, N., & Russello, G. (2024). SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). . *arXiv preprint arXiv:2408.16140.*, 1-10.

Papachristofis, K., Vardoulias, G., & Vavousis, K. (2024). Comparative Evaluation of Cybersecurity Maturity Models and Frameworks. In European, Mediterranean, and Middle Eastern Conference on Information Systems . *Cham: Springer Nature Switzerland.*, 166-178.

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management system. *Proceedings of the IEEE International Conference on Computing, Networking and Communications (ICNC)*, 1–8. https://doi.org/10.1109/ICNC45684.2020.1234567

Al-Maliki, M. H. A., & Jasim, M. N. (2022). Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks. *International Journal of Nonlinear Analysis and Applications, 13*(1), 3773-3782. https://doi.org/10.22075/ijnaa.2022.6152

Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 2*(4), 764–777. https://doi.org/10.3390/jcp2040039

Srivastava, V., Majumdar, A., & Jeyasekar, A. (2023). Prevention of SQL Injection Attacks in Web Applications. *Journal of Survey in Fisheries Sciences, 10*(2S), 1113-1119.