HUB TECH IA

Deliverable report 35

AI and IAGEN Application Use Case

Generative Artificial Intelligence (AI) Security Protocol Generation in Vaca Muerta

I. Introduction

The oil and gas industry is characterized by complex operations and inherent risks that demand high safety standards. In this context, generative Artificial Intelligence (AI) emerges as an innovative tool with the potential to revolutionize the development of safety protocols in Vaca Muerta, Argentina's largest shale formation.

This report analyzes the potential of generative AI to improve safety in the industry, addressing its applications, benefits, challenges, and best practices for implementation.

II. Security Protocols Powered by IAGen

Generative Artificial Intelligence (GENI) is a branch of artificial intelligence that focuses on creating new content, such as models, images, code, or text, from existing data. This technology uses advanced algorithms to analyze large amounts of information, identify patterns, and generate new, original content that is often indistinguishable from human-created content.

Generative artificial intelligence (GAI) is transforming safety management in the energy

industry, not only through risk detection but also through the automated generation of adaptive protocols, situational recommendations, proactive monitoring, and intelligent regulatory compliance.

1. **Key Applications of IAGen in Security Protocols**

a. Automatic Generation of Customized Protocols

- Based on historical operating data, environmental conditions, and local/international regulations, IAGen can draft:
    - Specific procedures in case of leaks, explosions or spills.
    - Dynamic instructions based on roles and locations (night shift, adverse weather, well type).
    - Immediate response guides based on the type of anomaly detected.
- Example: When a leak is detected in a high-pressure valve, the system instantly generates a specific protocol for the field operator with visual and voice instructions.

b. Proactive Monitoring and Smart Alerts

- The IAGen acts as an intelligent monitoring center that interprets data from sensors, thermal images, and operational signals to issue early warnings.
- Detects unusual behavior in critical areas, such as:
    - Gradual increase in pressure in pipelines.
    - Unauthorized presence in restricted areas (computer vision).
    - Abnormal noises or suspicious vibrations (acoustic analysis).

c. Simulation of Critical Scenarios

- It uses generative models to create simulations of failures, leaks, or fires, helping to prepare more realistic and robust contingency plans.
- Virtually train operators with adaptive scenarios based on seasonal changes, shifts, location, or plant configuration.

d. Automated Regulatory Compliance

- IAGen compares operational protocols and records with regulatory requirements in real time.

- Notify when the following are detected:
    - Deficiencies in the mandatory documentation.
    - Instructions not updated according to new regulations.
    - Risks of sanctions for environmental or labor non-compliance.

e. Personal Safety and Work Fatigue Management

- Analyze schedules, shift lengths, environmental conditions, and staff health reports to:
    - Recommend breaks.
    - Warn about overload or fatigue.
    - Redesign critical shifts based on accumulated risk.
- Integration with wearables: measures staff biometric variables (heart rate, body temperature, drowsiness alerts).

f. Generation of Automated Post-Incident Reports

- In the event of an incident, IAGen automatically reconstructs the events:
    - Chronology of events.
    - Sensors activated.
    - Executed responses and reaction times.
- Produces auditable reports for regulatory authorities and improves protocols on a case-by-case basis.

2. IAGen's added value in security

Advantage	Description
Adaptability	Protocols evolve in real time, adjusting to new conditions.
Conversational interface	Any operator can instantly check the protocol via voice or chat.
Preventing human errors	Automates critical decisions when severe threats are detected.

Smart audit	Detects non-compliance or lack of controls in real time.

3. Practical example

Situation : Unexpected pressure increase in a gas pipeline during a thunderstorm.
IAGen agent action:

- Detects abnormal patterns and risk of rupture.

- Compare with similar historical events.
- Generates automatic priority alert to supervisor + nearby operators.
- It deploys a visual and voice-audited protocol, with steps for remote valve closure, preventive evacuation, and notification to Civil Defense.
- Upon completion, generate a report for post-mortem analysis.

III. Application of agents driven by IAGEN in the activity

1. **IAGEN Agents Concept**

In recent years, generative artificial intelligence (GAI) has revolutionized the way we interact with technology, enabling the development of systems capable of generating content, answering complex questions, and assisting with highly demanding cognitive tasks. From this capability, a new technological architecture has emerged: GAI-powered agents. These agents are not simple conversational interfaces, but autonomous systems that can interpret instructions, make decisions, execute tasks, and learn from their interactions with the environment.

An IAGen agent combines large language models with additional components such as external tools, memory, planning, and autonomous execution. This allows them to operate in complex environments, with the ability to break down objectives into steps, coordinate multiple actions, interact with digital systems (such as databases, APIs, or documents), and adapt to context changes in real time. These qualities distinguish them

from traditional chatbots and open up a range of more sophisticated and customizable applications.

At the organizational level, these agents are being used to automate processes, generate data analysis, assist in decision-making, and improve the user experience, both internally and externally. For example, they can take on human resources, legal, financial, or logistics tasks, and even tasks linked to the technical areas of production processes, acting as intelligent assistants that collaborate with human teams. This ability to integrate knowledge and execute tasks autonomously transforms the way organizations can scale their operations without losing quality or control.

Furthermore, agentic workflows—structures where multiple agents collaborate to solve complex problems—allow responsibilities to be distributed among different agent profiles, each with specific functions. This creates hybrid work environments where humans and agents coexist, optimizing time, costs, and results. The ability to connect agents with tools such as Google Drive, CRMs, or document management platforms further expands their capabilities.

The development of IAGen-powered agents represents a crucial step toward a new era of intelligent automation.

Among the benefits of authentic workflows powered by generative AI models is the ability to automate entire production processes, end-to-end, and even add value by leveraging the capabilities of language models based on these technologies.

However, its implementation also poses technical, ethical, and legal challenges, ranging from responsible design to human oversight. Therefore, understanding its architecture, operational logic, and potential impacts is critical for its effective and safe adoption in diverse professional contexts.

2. Proposal for the design of an Intelligent Security Agent based on IAGen

a. **General Objective**

Detect operational risks in real time, generate automatic incident protocols, simulate critical scenarios, and ensure regulatory and human compliance, all based on a continuous improvement approach.

b. **Functional Structure of the SafeGen Agent**

- **Real-Time Risk Capture Module**

Functions:

- Receives data from IoT sensors, SCADA, thermal images, security cameras, industrial audio.

- Identifies abnormal behavior (high pressure, abnormal temperature, unusual noises, intrusion).

Technologies:

- Computer vision + natural language processing (to read operator logs).
- Anomaly prediction models (Historically based ML + continuous learning).

- **Protocol Generator Module (IAGen Core)**

Functions:

- Automatically generates response protocols for:
    - Leaks, fires, electrical failures, spills, collisions.
- Adapt the protocols according to:
    - Type of facility, climatic conditions, type of resource (gas, oil, water), profile of the personnel present.

Tickets:

- Operational data + current regulations + geographic location + profile of the detected event.

Departures:

- Response document + voice alerts + visual instructions + integration with ERP or SCADA.

- **Proactive Simulation and Training Module**

Functions:

- Simulate emergency scenarios based on historical and predictive data.
- Train operators with interactive cases generated by IAGen.
- Generates automatic post-training evaluations.

a. Automated Regulatory Compliance Module

Functions:

- Check that the generated protocols are aligned with:
    - Local regulations (Energy Secretariat Resolutions)
    - International standards (API, ISO, OSHA, ASME)
- Detects operational non-compliance (e.g. lack of checklist, delay in response).

Actions:

- Alert those responsible.
- Automatic suggestion of corrections.
- Compliance and risk report.

- **Human Safety and Operational Ergonomics Module**

Functions:

- Analyze shifts, wear, thermal load, fatigue.
- Integrates data from wearables (if available).
- Suggest breaks, replacements, redistribution of tasks.
- Prevents human errors related to stress or overexertion.

- **Reports and Audit Module**

Functions:

- Create automatic post-incident reports.
- Respond to regulatory requests with traceable evidence.
- Presents dashboards of:
    - Response times
    - Root causes
    - Impact avoided
    - Level of compliance

c. Technical Characteristics of the Agent

Component	Detail
Interface	Web panel, internal chatbot, mobile app for the field
Entrance	Sensors, SCADA, audio, text, image, video
Output	Protocols, alerts, simulations, reports
Privacy	Control by role and operational area
Update	Self-coaching with each confirmed or avoided event

d. **Sample Workflow**

1. Event: Abnormal pressure increase in valve + irregular vibration.

2. Agent detects anomalous pattern → classifies event as medium level.

3. Generates specific protocol for the operator present + preventive message to supervisor.

4. Activate alarm in tower + recommend partial closure and sensor check.

5. It then records the event, generates an automatic report and suggests a scheduled inspection to avoid repetition.

IV. Additional uses of IAGEN

In the oil and gas industry, generative AI can be applied in a variety of areas. Below are some of its applications, organized by industry segment:

Upstream (Exploration and Production):

- Drilling Optimization: Generative AI analyzes geological and operational data in real time to redefine decision-making in well drilling, making it faster and more accurate. Its advanced algorithms predict potential problems and map out an optimal drilling direction, minimizing environmental risks.
- Downhole Image Analysis: During the drilling process, computer vision, a branch of AI, can be used to analyze downhole camera images. By identifying the characteristics of the rock formations encountered, AI can help optimize well placement and trajectory to maximize production from each oil well.
- Steam Leak Detection: Machine vision can be used to correctly identify and segment steam in complex environments where traditional sensors can fail. This helps

prevent potential hazards, maintain optimal operating conditions, and improve energy efficiency.

Midstream (Transportation):

- Optimizing transportation and distribution networks: AI analyzes traffic, weather, and demand data to plan more efficient routes, reduce fuel consumption, and minimize delays in the transportation of oil and natural gas.
- Pipeline Inspection: Drones equipped with cameras and computer vision can be used to autonomously scan kilometers of pipelines, detecting leaks, cracks, and corrosion in incredible detail.

Downstream (Refining and Processing):

- Refinery monitoring: Machine vision can analyze camera feeds inside refineries to identify inefficiencies or potential equipment failures.
- Recovery Process Optimization: Machine learning algorithms can optimize secondary and tertiary recovery processes, increasing reservoir production levels.

Cross-cutting applications:

- Improved reservoir simulation: Generative AI creates more accurate and detailed simulation models, giving engineers deep insight into reservoir behavior. This makes it easier to understand underlying processes and enables production optimization and cost reduction.
- Predictive equipment maintenance: By analyzing real-time sensor data, generative AI can anticipate maintenance needs, prevent unplanned failures, and reduce costs.
- Exploration of new deposits: Generative AI can analyze large amounts of geological and geophysical data to identify promising areas for exploration, accelerating the decision-making process and reducing associated risks.
- Regulatory Compliance: Generative AI can help businesses manage vast amounts of information and stay up-to-date with changing regulations and standards, ensuring regulatory compliance.

- Improved operational safety: AI can detect anomalies in systems and provide early warnings of potential problems, improving operational safety.
- Talent management: AI can be used to monitor professionals' work, analyze workload, and assign tasks more equitably, avoiding stressful situations and improving job security.
- Access to information: Generative AI enables real-time access to information from a large number of documents via chat, improving efficiency, productivity, and decision-making.

V. Specific Safety Risks in Vaca Muerta

There are specific security risks that must be considered when developing protocols. Some of these risks include:

- Air pollution: Soil blasting and the substances released into the atmosphere during operations affect air quality, with potential health consequences for people living near wells or facilities. This can cause respiratory illnesses and diseases linked to the absorption of toxic substances.
- Water Pollution: Hydraulic fracturing uses large volumes of water and chemical additives, with the risk of contaminating aquifers. The migration of these substances to the surface can affect the quality of water available for human consumption.
- Induced seismic activity: The injection of water and additives into the subsoil during hydraulic fracturing can produce seismic movements. While the industry downplays the dangers of this activity, the lack of information and scientific studies is causing concern among the public.
- Waste generation: Drilling and operating wells generate waste such as drill cuttings, drilling mud, and oil-based blankets. This waste requires proper management to prevent soil and water contamination.
- Occupational Hazards: Workers at Vaca Muerta are exposed to various occupational hazards, such as motor vehicle accidents, burns, injuries, falls, exposure to hydrogen sulfide (H2S) gas, and other hazards. Safety training and the proper use of personal

protective equipment are essential to prevent accidents.

It is important to emphasize the importance of training and raising awareness among workers about the specific risks of Vaca Muerta. Obtaining authorizations and certifications to enter a field and understanding safety procedures are crucial to ensuring safe operations.

VI. Best Practices in the Generation of Security Protocols

To generate effective security protocols with generative AI, the following best practices should be considered:

- Short-term investment in AI agent implementation teams in technology and training: Investment is required in proofs of concept and pilot testing. The focus here must be on developing the talent needed to implement these solutions, as there is a trend toward cost reduction in systems that enable "no-code" and "low-code" automation. For the first stage, it is also recommended to recruit teams with experience in AI agent design and implementation. Finally, it is key to form an in-house team to support and foster an agentic culture that redefines human-machine interaction.
- Risk identification and assessment: Conduct a comprehensive analysis of Vaca Muerta's specific risks, considering tasks, equipment, environment, and regulations. Use tools such as the Job Hazard Analysis (JHA) method to identify potential hazards.
- Correct use of Personal Protective Equipment (PPE): Identify and provide the appropriate PPE for each task, and train workers on its correct use. Conduct regular inspections of the equipment to ensure its good condition.
- Emergency Response Plan: Design a detailed protocol for responding to emergencies such as fires or chemical leaks. Conduct regular drills to ensure staff understand their responsibilities.
- Equipment Inspections and Maintenance: Perform periodic inspections of machinery, tools, and safety systems. Create a maintenance schedule and document each inspection.

- Promoting a culture of safety: Foster a prevention and safety mindset throughout the organization. Recognize employees who follow good practices and conduct awareness campaigns.
- Compliance with standards and regulations: Ensure compliance with current safety laws and standards. Stay up-to-date on regulations and conduct internal audits.

VII. Benefits and Challenges of Implementing AI-Generated Security Protocols

The implementation of AI-generated security protocols in Vaca Muerta offers several benefits, but also presents challenges that must be considered.

1. Benefits

- Faster threat detection and response: AI can analyze large volumes of data in real time, enabling early risk detection and faster incident response. This can be crucial in preventing accidents and minimizing damage.
- Improved threat detection accuracy: AI can learn from historical data and use advanced algorithms to identify known threats and detect anomalous behavior. This enables better risk assessment and greater efficiency in implementing preventive measures.
- Security Task Automation: AI can automate repetitive tasks, freeing up time and resources for security professionals to focus on more strategic activities. This can include system monitoring, access management, and reporting.
- Adaptability and continuous learning: AI can adapt and learn from new threats and attack techniques as they evolve. This allows security protocols to stay up-to-date and effective against new threats.
- Reducing accidents and improving employee health: AI can help prevent accidents, detect hazards, and improve employee working conditions. This translates into a safer and healthier work environment.
- Reducing costs associated with workplace accidents: AI can mitigate the costs associated with workplace accidents by preventing their occurrence and optimizing safety management. This includes reducing medical, legal, and workers'

compensation costs.

- Improved worker productivity and morale: A safe work environment, where risks are proactively managed through AI, fosters greater worker productivity and morale. Workers feel safer and more motivated, which translates into better job performance.
- Improving project efficiency: AI enables better project schedule forecasting, reducing delays, cost overruns, and other risks by suggesting effective mitigation actions.

2. Challenges

- Data security: It is essential to ensure the security of the data used by AI systems, especially if it involves personal or sensitive data. Robust security measures must be implemented to protect data from unauthorized access and cyberattacks.
- Lack of transparency: The lack of transparency in how some AI algorithms operate can make it difficult to identify vulnerabilities and prevent attacks. It's important to understand how AI algorithms work and how decisions are made so you can trust the security protocols they generate.
- Algorithmic discrimination: It is important to ensure that AI algorithms do not exhibit biases that could lead to discriminatory decisions. It is important to ensure that the data used to train the algorithms is representative, and that the algorithms are evaluated for potential biases.
- False information: AI can be used to generate false information, which can compromise security. It's important to have mechanisms in place to verify the authenticity of AI-generated information and prevent the spread of false information.
- Data Privacy: The collection and analysis of large amounts of data by AI systems raises privacy concerns. Privacy policies must be implemented to ensure the protection of personal data and compliance with data protection regulations.
- High initial investment: Implementing AI technologies can require a significant initial investment. It's important to evaluate the return on investment and consider available financing options.
- False positives and negatives: AI systems can generate false positives or false negatives when detecting threats. It's important to have mechanisms in place to validate AI-generated alerts and minimize errors.

- Cyberattack sophistication: Cybercriminals can use AI to evade AI-based defenses. It's important to stay up-to-date on new threats and attack techniques and adapt security systems accordingly.
- Shortage of specialized talent: Effective implementation of AI in security requires AI and security experts. It's important to invest in training AI and cybersecurity professionals.
- Data quality: Data quality and accuracy are essential for the effective functioning of AI systems. Data validation and cleansing processes must be implemented to ensure the reliability of the results.
- Resistance to change: Implementing AI can generate resistance to change among staff. It's important to communicate the benefits of AI, train staff, and ensure a smooth transition.
- Continuous evaluation: It is essential to continually evaluate the impact of AI to identify areas for improvement and ensure that the expected objectives are being achieved.

XIII. Conclusions

Generative AI has the potential to transform the development of safety protocols at Vaca Muerta, improving worker safety, optimizing operations, and reducing costs. AI's ability to analyze large volumes of data, predict risks, simulate scenarios, and adapt to new threats makes it an invaluable tool for accident prevention and safety management.

A key aspect that AI can contribute is a paradigm shift in security, moving from a reactive to a proactive approach. Instead of reacting to incidents after they occur, AI allows us to anticipate and prevent risks, proactively improving security.

In addition to safety benefits, AI can generate significant cost savings and efficiency improvements. Reducing accidents, optimizing operations, and automating tasks can generate significant savings for companies.

However, it is crucial to address the challenges posed by its implementation, ensuring

data security, transparency, privacy, and regulatory compliance. Collaboration between AI experts, security professionals, businesses, and regulatory authorities will be critical to fully realize the potential of generative AI in the oil and gas industry.

It's important to consider the ethical implications of using AI in security. It's important to ensure that AI algorithms are fair, transparent, and free from biases that could discriminate against certain groups of people.

In the future, AI is expected to continue to evolve, and its applications in security are expected to expand even further. AI could be integrated with other technologies, such as the Internet of Things (IoT) and robotics, to create even more sophisticated and efficient security systems.

To fully leverage the potential of generative AI in Vaca Muerta security, companies are encouraged to:

- Invest in the implementation of AI technologies.
- Train staff in the use of AI.
- Develop robust security and privacy policies.
- Collaborate with experts in AI and industrial security.
- Continuously monitor and evaluate the impact of AI.

The adoption of generative AI in Vaca Muerta's security is a strategic investment that can generate significant benefits for businesses, workers, and the environment.

Sources cited

1. Benefits of AI in Occupational Risk Prevention - Alba Formación, access date: March 5, 2025, https://www.alba-consult.com/beneficios-de-la-ia-en-la-prevencion-de-riesgos-laborales/
2. Generative AI in Oil & Gas: 5 High-Complexity Use Cases - Nubiral, access date: March 5, 2025, https://nubiral.com/generative-ia-oil-gas/
3. AI in Oil and Gas: Refining Innovation - Ultralytics, accessed March 5, 2025,

https://www.ultralytics.com/blog/ai-in-oil-and-gas-refining-innovation
4. Artificial Intelligence applied to the Oil Industry - EADIC, access date: March 5, 2025, https://eadic.com/blog/entrada/inteligencia-artificial-aplicada-en-la-industria-petrolera/
5. Artificial Intelligence for Occupational Health and Safety - Nalanda, access date: March 5, 2025, https://www.nalandaglobal.com/blog/inteligencia-artificial-para-la-seguridad-y-la-salud-laboral-tecnologia-a-favor-de-la-prevencion/
6. What are the three key opportunities of Generative AI for the energy industry?, access date: March 5, 2025, https://econojournal.com.ar/2024/09/oportunidades-ia-generativa-para-la-industria-energetica/
7. YPF uses Artificial Intelligence and Starlink to improve the efficiency and productivity of Vaca Muerta, access date: March 5, 2025, https://www.ambito.com/energia/ypf-utiliza-inteligencia-artificial-y-starlink-mejorar-la-eficiencia-y-productividad-vaca-muerta-n6092997
8. Artificial intelligence in Vaca Muerta: YPF seeks the best well to beat US shale gas - Clarin.com, access date: March 5, 2025, https://www.clarin.com/economia/inteligencia-artificial-vaca-muerta-ypf-busca-mejor-pozo-ganarle-shale-gas-eeuu_0_sqUQt9jtH3.html
9. In Vaca Muerta, artificial intelligence is making its way into more and more processes, access date: March 5, 2025, https://www.mejorenergia.com.ar/noticias/2024/04/30/2721-en-vaca-muerta-la-inteligencia-artificial-se-abre-paso-en-cada-vez-mas-procesos
10. How artificial intelligence is revolutionizing factory safety, access date: March 5, 2025, https://www.ambientum.com/ambientum/tecnologia/como-la-inteligencia-artificial-esta-revolucionando-la-seguridad-en-fabricas.asp
11. How AI is Transforming Industrial Safety - Fracttal, accessed March 5, 2025, https://www.fracttal.com/blog/transforming-industrial-safety-with-ai
12. 7 Examples of How AI Is Improving Data Security, accessed March 5, 2025, https://www.forcepoint.com/blog/insights/ai-data-security-examples
13. Top 10 Artificial Intelligence Tools for Cybersecurity (February 2025), accessed March 5, 2025, https://www.unite.ai/artificial-intelligence-tools/
14. The Role of AI in Security Management - AMCS Group, accessed March 5, 2025,

https://www.amcsgroup.com/blogs/the-role-of-ai-in-security-management/
15. 5 Artificial Intelligence (AI) Trends in Security 2024 - Algotive, access date: March 5, 2025, https://www.algotive.ai/es-mx/blog/5-tendencias-de-inteligencia-artificial-ia-en-seguridad-2024
16. F417-261-999 Dairy Safety: Key Hazards and Solutions - | WA.gov, accessed March 6, 2025, https://www.lni.wa.gov/forms-publications/F417-261-999.pdf
17. Golden Rules of the Oil Industry - Argentina.gob.ar, access date: March 6, 2025, https://www.argentina.gob.ar/sites/default/files/afiche_reglas_de_oro_petroleo.pdf
18. The Quadripartite Roundtable approved the poster “Golden Rules of Vaca Muerta” | Argentina.gob.ar, access date: March 6, 2025, https://www.argentina.gob.ar/noticias/la-mesa-cuatripartita-aprobo-el-afiche-reglas-de-oro-de-vaca-muerta-0
19. Only for Vaca Muerta: the Argentine Government regulated the energy chapter of the Bases Law, access date: March 6, 2025, https://www.energiaestrategica.com/solo-para-vaca-muerta-el-gobierno-argentino-reglamento-el-capitulo-energia-de-la-ley-bases/
20. The Rules of Vaca Muerta - Vacamuerta.ar | Information repository, accessed March 6, 2025, https://vacamuerta.ar/las-reglas-de-vaca-muerta/
21. Effects, impacts and socio-environmental risks of the Vaca Muerta megaproject* - Environment and Natural Resources Foundation, access date: March 6, 2025, https://farn.org.ar/wp-content/uploads/2021/02/DOC_IMPACTOS-VACA-MUERTA_links.pdf
22. Hazards and Controls: The Oil and Gas Industry | Texas Mutual, accessed March 6, 2025, https://www.texasmutual.com/employers/hazards-and-controls/oil-and-gas-span
23. Training and Safety: The Secrets of Working in an Oil Field - Vaca Muerta News, access date: March 6, 2025, https://vacamuertanews.com/actualidad/capacitacion-y-seguridad-los-secretos-de-trabajar-en-un-yacimiento.htm
24. Best Practices in Industrial Safety: What, How, When and Why, access date: March 6, 2025, https://www.safetyisab.com/mejores-practicas-en-seguridad-industrial-que-como-cuando-y-por-que
25. Network Security Best Practices - Aryaka, access date: March 6, 2025, https://www.aryaka.com/blog/network-security-best-practices/

26. Top 10 AI Tools to Strengthen Your Business Security - Wingsoft, accessed March 6, 2025, https://www.wingsoft.com/blog/mejores-herramientas-IA-seguridad-empresarial
27. Integrating AI into Security Systems - Telgian, access date: March 6, 2025, https://telgian.com/es/integrating-ai-into-security-systems/
28. How artificial intelligence is changing occupational risk assessment - Bluak, access date: March 6, 2025, https://www.bluak.com/como-la-inteligencia-artificial-esta-cambiando-la-evaluacion-de-riesgos-laborales/
29. How to Use Artificial Intelligence for Workplace Safety - DataScope, access date: March 6, 2025, https://datascope.io/es/blog/inteligencia-artificial-en-seguridad-laboral/
30. Experts warn of new risks from widespread use of AI - AP News, access date: March 6, 2025, https://apnews.com/article/artificial-intelligence-ai-security-031b96de5be10e82793386e745ff431d
31. Artificial Intelligence: Cybersecurity Benefits and Risks - Delta Protect, access date: March 7, 2025, https://www.deltaprotect.com/blog/inteligencia-artificial
32. Security challenges in the era of artificial intelligence, access date: March 7, 2025, https://www.impulsa-empresa.es/desafios-seguridad-era-inteligencia-artificial/
33. Cybersecurity and Artificial Intelligence: What are its advantages and challenges? - Ticnova, accessed March 7, 2025, https://ticnova.es/blog/ciberseguridad-e-inteligencia-artificial/
34. What Are the Challenges of Implementing Artificial Intelligence in Healthcare Systems and How to Manage Them Efficiently? - Atlantis University, accessed March 7, 2025, https://atlantisuniversity.edu/es/au_blog/retos-inteligencia-artificial-en-salud/