TRABAJO DE INVESTIGACIÓN FINAL

Global Communication Plan for Faraday Security

Autor/es:

Victoria Garcia Weidemann - LU: 1152228
Micaela Wasserman - LU: 1145011

Carrera:
Global Communications

Tutor/es:
Mariana Simon

Año:
2025

Universidad Argentina de la Empresa
Facultad de Comunicación

UADE

Index

Authenticity Statement

By means of this statement, us Micaela Wasserman and Victoria García Weidemann students of the Bachelor's Degree in Global Communication at Argentine Business University (UADE), hereby declare that this Final Major Project titled: "A Global Communication Plan for Faraday Security" is the result of our own work and research.

All materials, sources, and references—whether from books, academic articles, institutional reports, lecture notes, interviews, websites, or personal communications—have been properly acknowledged and cited in accordance with academic standards ISO 690. We certify that this report has not previously been submitted for assessment in any other course in the program.

12/11/2025

Micaela and Victoria

Abstract

This project delivers a strategic analysis of Faraday Security's global positioning, focusing on its public relationships across Argentina, the United States, and Germany. Our in-depth assessment critically examines the company's internal structure, core capabilities, and strategic direction, alongside its intricate meso and macro-environmental forces, including intense market competition and evolving regulatory landscapes. Grounded in the Villafañe Public Mapping Model and supported by a detailed PESTEL and SWOT framework, the research identifies and segments key stakeholders—particularly within government and media spheres—according to each country's institutional logic. The analysis uncovers critical misalignments between Faraday's communication practices and the expectations of high-influence publics. The insights encountered enabled the formulation of preliminary problem statements that will guide future engagement strategies, establishing a diagnostic foundation for understanding how Faraday's communication structure and stakeholder visibility impact its operational and reputational effectiveness. This underscores the foundational need for a unified communication strategy to overcome these identified limitations and unlock Faraday's full global potential.

Key Words

Faraday; Communication Plan; Cybersecurity; Strategic Analysis; Public Mapping

Glossary

Vulnerability Management is a systematic approach to identifying, evaluating, treating, and reporting vulnerabilities in software and hardware systems. It aims to reduce the risk of cyber threats and enhance the overall security posture of an organization[1]

A bug is a flaw or vulnerability in the software or hardware design that can be potentially exploited by the attackers. These security bugs can be used to exploit various vulnerabilities by compromising – user authentication, authorization of access rights and privileges, data confidentiality, and data integrity.[2]

Penetration testing (pentesting) is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.[3]

B2B (Business to Business) is referred by the Cambridge Dictionary as involving arrangements or trade between different businesses, rather than between businesses and the general public[4]

Freemium service is a blend of "free" and "premium"—is a business strategy where companies offer basic features of a product or service at no cost, while charging for access to more advanced or premium functionalities[5].

---

[1]IBM. *What is vulnerability management?* [online]. August 24, 2022 [Accessed 3 April 2025]. Available from: https://www.ibm.com/think/topics/vulnerability-management

[2]NETENRICH. *What is a bug?* [online]. [no date] [Accessed 18 April 2025]. Available from: https://netenrich.com/glossary/bug

[3]NATIONAL CYBER SECURITY CENTRE. *Penetration testing* [online]. [no date] [Accessed 15 April 2025]. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing

[4]CAMBRIDGE DICTIONARY. *Meaning of business-to-business in English* [online]. [no date] [Accessed 18 April 2025]. Available from: https://dictionary.cambridge.org/us/dictionary/english/business-to-business

[5]KUMAR, Vineet. *Making "Freemium" work* [online]. Harvard Business Review, May 2014 [Accessed 11 May 2025]. Available from: https://hbr.org/2014/05/making-freemium-work

Global Organization Analysis

Micro-environment

- **Name and type of corporation**

Faraday Security is a private company specializing in offensive cybersecurity and vulnerability management. It initially adopted an open-source approach but later evolved into a hybrid model, offering both free version and premium enterprise platform with advanced features

- **Locations (headquarters, branches, subsidiaries, factories)**[6]

Headquarters: 3310 Mary St, Suite 501, Miami, FL 33133 Phone: +1 904 715 4284

Research Lab & Development: Bolivar 238, 2nd Floor, Buenos Aires, C1066AAF, Argentina Phone: +54 11 4331 0469

- **Number of employees**

The company currently has 55 employees. Its team is distributed as follows:

- Development and R&D team in Argentina
- Commercial and Expansion team in the U.S.
- Cybersecurity Consultants working remotely or assigned to strategic clients

- **Financial information**

The technological security market in Argentina has shown steady growth. According to the Argentine Chamber of Electronic Security[7] (2024), the sector reached annual revenues of approximately $640 million, driven by the increasing demand of security solutions. This trend represents a significant opportunity to expand its footprint in a market that is becoming increasingly aware of digital threats.

- **Core business**

Faraday's main activity is Cybersecurity. The company specializes in vulnerability analysis and management, security assessments, penetration testing, reverse engineering, and code review.

- **History (timeline, or milestones)**

Founded in 2001 in Buenos Aires, Faraday rapidly established itself as a key player in the cybersecurity landscape. Initially focused on consulting services aimed at identifying and mitigating organizational vulnerabilities, the company leveraged this expertise to develop a tool designed to simplify the daily operations of security teams (Forbes Argentina, 2021).

---

[6]FARADAY. *Official website* [online]. [no date] [Accessed 27 March 2025]. Available from: https://faradaysec.com/

[7]ARGENTINE CHAMBER OF ELECTRONIC SECURITY. *CASEL official website* [online]. [no date] [Accessed 18 April 2025]. Available from: https://casel.org.ar/

The company launched its open-source vulnerability management platform in 2015. By 2018, it had integrated with over 150 security tools, significantly expanding its enterprise capabilities. The company's international expansion accelerated in 2020 with the onboarding of clients across Europe and North America, culminating in the opening of a Miami office in 2023 to solidify its presence in the U.S. market. Evolving from a research-driven initiative into a global cybersecurity leader, Faraday continues to pioneer offensive security solutions, optimizing vulnerability management through cutting-edge technology and community-driven collaboration.

- **Founders, main characters, and/or heroes**[8]
  - ★ Federico Kirschbaum: CEO & Co-Founder
  - ★ Martin D. Tartarelli: COO
  - ★ Santiago Fernandez Boccacci: CFO
  - ★ Joshua Mador: VP of Business Development and International Sales

- **Logo**

The company's logo was created and developed by SeventhDesign™, a branding studio. According to color theory, blue often signifies trust and security, which is crucial in cybersecurity.[9] The font used called "Neometric Alt Medium" is a modern sans-serif typeface characterized by its geometric shapes and clean lines that reflect a modern, forward-thinking brand identity. The minimalistic design often suggests a focus on efficiency and straightforwardness, therefore it helps establish a brand's identity as professional and accessible.

They are now undergoing a rebranding process to better reflect its identity. The process is being held internally, seeking for the new logo to fully represent the fusion of talent and technology. For instance, one of the main changes resides in integrating the color red, based on the Red Team that represents offensive security management.

[8]See Annex 1
[9]QUILL CREATIVE STUDIO. *Brand color theory: Why color matters for your brand* [online]. May 22, 2023 [Accessed 3 April 2025]. Available from: https://www.quillcreativestudio.com/blog/brand-color-theory-why-color-matters-for-your-brand

- **Main services**

Faraday Security focuses on providing advanced cybersecurity solutions. Among the key service areas, they offer the following:

Mobile application security: Evaluates mobile architectures with the goal of finding vulnerable areas in applications	**Penetration testing:** Simulates real-world attacks to identify and exploit assets and vulnerabilities within infrastructure.	**Vulnerability analysis:** Detects security weaknesses, providing a detailed map of vulnerable factors.	**Network security assessments:** Performs an in-depth analysis to identify critical risk areas
Code review: Detects vulnerabilities directly in the source code	**Reverse engineering:** Disassembles and analyzes applications to extract and understand potential cybersecurity threats	**Physical security assessments:** Evaluates physical infrastructure to detect potential security weaknesses	**Client side attacks:** Stimulates authorized intrusions to assess workstation configurations and employee security awareness

Most services offered by Faraday essentially specialize in helping companies protect themselves from potential attackers by proactively identifying vulnerabilities. While defensive security (Blue Team) involves measures like antivirus software and access controls, the offensive security (Red Team) focuses on actively testing systems to find vulnerabilities before attackers can exploit them.

The company can either offer **"one-shot" projects,** such as audits before the launch of an application, or **monthly hourly contracts for specific tasks.** Either way, Cecilia Garmendia, Head of the Marketing Department mentions “solutions are almost entirely consulting-based and adapted to the client's specific needs”.

Faraday offers their tool in four distinct versions[10] with a 15-day free trial

- **Community** version is open-source and free, ideal for users looking to leverage and collaborate with open-source tools for vulnerability management.
- **Personal** version is a *freemium* tool designed for newcomers, that includes basic features to facilitate user adoption to the tool with available purchases.
- **Professional** version targets pentesters and security teams, offering automated vulnerability management, detailed reporting, and integration with over 150 tools. It supports up to five users and starts at $670 per month, billed annually

[10]FARADAY. *Pricing* [online]. [n.d] [Accessed 10 April 2025]. Available from: https://faradaysec.com/pricing/

- **Corporate** version is built for large enterprises and MSSPs, providing unlimited users and workspaces, advanced health scans, and integration with ticketing systems. This comprehensive solution starts at $1875 per month, billed annually.

Additionally, as previously mentioned, the company has a specialized consulting team known as **Faraday Labs**, which targets offensive security testing. This is a consulting service that helps clients proactively identify and mitigate security risks, ensuring robust protection against potential cyber threats.

- **Strategic purpose**[11]

Faraday presents a clear mission, vision, and value-driven principles that guide its work, even if they are not always presented in a traditional or centralized corporate format. Instead, these elements are installed throughout internal onboarding materials, like HR presentations, and reflected in their social media and public messaging in general. The mission, *"Cybersecurity is all about being one step ahead"*, captures the commitment to helping organizations proactively detect vulnerabilities before external threats do. This proactive mindset shapes both the company's platform and its educational approach to security.

Its vision is clearly stated; *"To help conduct security engineering by maximizing team resources"*. This is achieved by centralizing efforts, aligning with the core goals of each organization, and guiding teams to adapt strategies, prioritize actions, and ultimately reduce exposure time. The ultimate goal is to simplify cybersecurity and make it accessible to everyone, not just experts. Faraday´s values are strongly implied in its positioning and communication: The company believes in taking a proactive stance on security, encouraging teams to identify vulnerabilities before malicious actors do. Cecilia emphasizes, *"What we want to promote is the idea that vulnerabilities will be found — the key is that you find them before an attacker does."*

Simplicity is a core belief of the organization, which works to challenge the idea that cybersecurity is too complex or only meant for a select few. *"We believe in simplifying the complex,"* said Cecilia, *"to stop thinking of cybersecurity as a myth, as something only meant for a select few."* Accessibility is key as well, when recognizing that the industry struggles with a lack of talent and high acquisition costs, Faraday seeks people to understand that cybersecurity is within reach. As Cecilia puts it, *"We want to debunk that idea and help people understand that security is accessible to everyone, and that there are different ways to take that first step."* Furthermore, empowerment also plays a key role. Faraday doesn't

[11] See Annex 2: *Transcript 1st Interview*

just offer tools — it supports teams so they can act confidently and effectively.

- **Strategic capabilities**

Faraday possesses key tangible and intangible resources: Among the intangibles, it has a strong organizational culture that fosters unity and a sense of purpose among employees. There is a positive work environment that is supportive and inclusive that increases overall performance and reduces turnover rates, allowing for a high employee retention that stands out. During the interview, Cecilia mentioned that many employees begin their professional careers at the company, reflecting its ability to train and develop talents.

In terms of tangible resources, Faraday stands out with their platform that integrates technology and expert knowledge to manage vulnerabilities comprehensively. This becomes a competitive advantage for the company since they provide an **"all-in-one" solution**, which centralizes tools and services in a single platform, enabling organizations to take practical and accessible control of their cybersecurity posture.

- **Going-green stage**

The company is currently in the early stages of its going-green journey. Although Faraday has participated in projects analyzing carbon footprint, it does not yet have a specific sustainability program. The company promotes diversity by encouraging women to enter the cybersecurity field, reflecting its commitment to social responsibility beyond environmental concerns. *"The company's social responsibility goes beyond just the environment. It's about considering the service being offered and how to give back to the community in which it operates"*[12]

- **Structure**

The company is departmentalized by function, with distinct areas such as product, development, sales, marketing, HR, finance, and offensive/defensive security teams (Red Team/Blue Team respectively) whereas for example, HR reports to the CEO and Finance has a CFO. The organization adopts a horizontal structure, characterized by team leaders who report directly to C-level executives (highest-ranking executives) fostering an optimized communication flow. This structure supports upward communication from team leaders to executives, downward communication from executives to teams, and lateral communication among team leaders. According to Harrison and Handy's Typology of Culture the company would classify this as a task culture, where teams are formed to address specific problems, and power is derived from expertise rather than position. The company's organizational

[12] See Annex 3: *Transcript 2nd Interview*

chart[13] reflects this functional and horizontal structure, with clear lines of reporting and collaboration.

- **Culture[14]**

Faraday has a collaborative and purpose-driven culture founded upon principles of continuous learning and talent development. Cross-functional cooperation is operationalized through institutionalized routines, such as regular feedback sessions and team-based initiatives, which serve to sustain and reinforce this culture of constant improvement. Although roles are clearly defined in terms of function and responsibility, leadership is fluid, emerging organically through demonstrated expertise and peer influence rather than hierarchical authority. In this context, power is distributed through influence and contribution, reinforcing the meritocratic structure that empowers individuals within the decentralized environment.

Operational control mechanisms are designed to promote accountability, incorporating structured processes such as performance evaluations, compliance audits, and iterative feedback cycles. These systems ensure operational excellence, aligning the companies strategic goals with the evolving external demands of the industry landscape. Interpersonal relationships are built on a foundation of trust, shared goals, and mutual respect. These values are symbolized through inclusive rituals that actively support both individual and collective development, ensuring coherence between personal aspirations and institutional objectives. This contributes to an environment where professional growth and personal well-being are integrated, fostering a genuine sense of work-life balance, encouraging questions, transparency, and collective learning. Despite the challenges of working within the complex industry of cybersecurity marked by economic volatility and competition where mobility and turnover are typically high, the company has managed to retain talents and scaled operations from Argentina.

- **Internationalization strategy[15]**

Faraday Security's internationalization is driven by several factors. The company identifies potential markets by proactively analyzing regional client needs and pain points, regulatory developments, and digital transformation trends, to tailor its offerings in the distinct contexts. One of the main components of this strategy is performing adaptive communication that allows Faraday to engage effectively with the diverse audiences by adjusting its message with the local legal frameworks, reaching potential clients expectations. For instance, in

[13] Disclaimer: We don't have the organizational chart since it's currently being updated.
[14] See Annex 2: *Transcript 1st Interview*
[15] See Annex 4: *Transcript 3rd Interview*

response to the enactment of the new cybersecurity legislation in Chile, Faraday adjusted its communication strategy to resonate with local stakeholders, thereby enhancing its credibility and relevance in the region[16].

While English is the company's primary language, the company adapts its campaigns to the linguistic and cultural preferences of each market. For example, in Latin America, campaigns are conducted in Spanish to ensure accessibility and resonance with local audiences, whereas in the United States, communication remains in English with a more technical and results-oriented tone. This adaptability enhances the company's ability to connect with diverse client segments and address unmet cybersecurity demands.

Faraday also adapts the product offering by region. In the U.S., the company offers a self-managed cybersecurity tool designed for autonomous use, reflecting the market's preference for independence and high-performance. Clients are encouraged to download, implement, and operate the tool with minimal intervention. In contrast, the Latin American market is served through a more consultative model, emphasizing continuous client engagement and support. This differentiation underscores Faraday's capacity to align product delivery with regional business cultures and digital maturity levels.

Furthermore, the company also places significant attention on the regulatory environment of each country, prioritizing countries with favorable or evolving cybersecurity regulations that align with its services. This regulatory sensitivity positions Faraday as a proactive partner in regions undergoing digital transformation. Having said this, we identify different modes of entry depending on the context. In markets with complex or restrictive legal frameworks, the company adopts a collaborative approach, partnering with local entities, to navigate compliance requirements and accelerate market entry. This reflects a pragmatic internationalization model that balances opportunity with operational practicity. Also, Faraday has made a direct foreign investment in the United States by establishing local offices to handle operations, therefore settling in the American market. Particularly these offices do not maintain permanent staff, but they function as strategic hubs to support business development and customer service. Lastly, the company also exports their services, selling its software directly to international clients.

[16]FARADAY. *Federico Kirschbaum at the Santiago Chamber of Commerce: key insights on cybersecurity* [online]. Faraday, 21 April 2025 [Accessed 12 May 2025]. Available from: https://faradaysec.com/federico-kirschbaum-at-the-santiago-chamber-of-commerce/

Regarding the balance between standardization and adaptation, they adopt a hybrid approach. While its core software solutions remain consistent across markets, unrestricted by international patenting or hardware validation requirements, the company adapts its services and messaging to comply with local regulations and market conditions. This strategic flexibility enables Faraday to maintain operational efficiency while ensuring relevance and compliance in each target market.

- **Communication background** (See Annex 11)

The company's corporate communications are managed entirely in-house by the Marketing team, which is responsible for all strategic messaging. Although the organization does not maintain a formalized internal communication policies, it utilizes a brand book to ensure consistency in tone, messaging, and visual identity across all communication channels. Also, the company has a graphic designer who accompanies all internal communication efforts[17].

To focus on customer engagement and retention, Faraday employs a third-party support team dedicated to assisting and accompanying clients throughout the solution adoption process. This team plays a critical role in ensuring timely responses to user inquiries and resolving technical issues efficiently. In terms of external communication, the company outsources the management of ads and paid media to specialized providers. They maintain an active presence on LinkedIn, X, and Instagram, using these platforms to position the brand within the cybersecurity sector through a mix of technical and emotional content.

The most recent campaign was launched on February 2, 2023, and it was focused on an educational and awareness-driven initiative aimed at promoting cybersecurity best practices. (See Annex 11)

Meso-environment

- ### Generic strategy

In the framework of the fast-evolving market in which the company functions, Faraday has adopted firstly a **market penetration strategy**, aiming to increase its shares within its existing market. To this end, by offering the Freemium, Open-Source version of its platform, they have managed effectively to lower entry barriers for new users. This initiative not only aligns with the company's foundational values of openness and community-driven development, but also serves as a strategic mechanism to attract emerging professionals and organizations with limited resources. However, According to Kumar[18], freemium works

[17] See Annex 4: *Transcript 3rd Interview*
[18]KUMAR, Vineet. *Making freemium work* [online]. Harvard Business Review, May 2014 [Accessed 14 June 2025]. Available from: https://hbr.org/2014/05/making-freemium-work

best when either the conversion of potential users is strong or the cost to serve free users is low. In Faraday's case, maintaining non-converting users may not be profitable long-term. Furthermore, without continuous value upgrades or strategic upselling mechanisms, the freemium offering may create a perception of commoditized service rather than a gateway to premium value.

The company also adopts a **product development strategy**, by continuously designing and introducing new cybersecurity tools aimed at enhancing protection and mitigating the impact of cyber threats. This exemplifies the sustained commitment to innovation through the development of their service portfolio, for instance the newest offering Continuous Security solution with DevSecOps Tool. While this approach aligns with industry trends toward integrating security earlier in the development lifecycle, it also reflects a broader challenge in the cybersecurity sector: the risk of over-reliance on automation and tool-centric solutions[19].

Furthermore, they implement a **market development strategy**, by targeting new markets in diverse geographical regions. As previously mentioned, by leveraging the adaptability of their solutions, the company has managed to pursue internationalization, extending the reach of its existing service portfolio to new customer segments, for example in the United States[20]. They continue their market expansion in Latin America, reinforcing its commitment to broadening its global market footprint[21].

- **Market**

Within the framework of the BCG Matrix, the company's Vulnerability Management Software and Penetration Testing Tool can be best classified as **Cash Cows** since they have maintained presence in the market over time, consistently generating stable revenue and holding significant market share. Anyways, in the cybersecurity sector, even mature products like these face constant pressure to evolve due to rapidly changing threat landscapes therefore there must be ongoing innovation and investment required to maintain their relevance[22].

---

[19]DELOITTE. *Embedding security into DevOps pipelines* [online]. Deloitte Insights, 2019 [Accessed 14 June 2025]. Available from: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html

[20]See Annex 4: *Transcript 3rd Interview*

[21]FORBES BURTON. *Market development: Unlocking growth through new market opportunities* [online]. Forbes Burton, 2023 [Accessed 13 June 2025]. Available from: https://www.forbesburton.com/insights/market-development-unlocking-growth-through-new-market-opportunities

[22]REDFOX SECURITY. *The evolving penetration testing ecosystem: Global insights* [online]. LinkedIn Pulse, 2023 [Accessed 13 June 2025]. Available from: https://www.linkedin.com/pulse/evolving-penetration-testing-ecosystem-global-insights-redfoxsec-kysfc/

In addition, the Continuous Security Software represents a **Question Mark**. Although it operates within a rapidly expanding segment of the industry, its recent introduction makes the market performance uncertain, regarding long-term viability. Such tools will depend not only on market growth but also on human and structural factors like user trust and integration into existing workflow[23]. Considering that Faraday does not yet have a clear **Star**, strategic investment will be necessary to determine whether it can gain sufficient propulsion to become one.

Furthermore, the Freemium Version of the platform can be considered as a **Dog** because, despite high user engagement, it has demonstrated limited success in converting usage into revenue. While the product has not reached the end of its life cycle, it has yet to demonstrate viability or profitability when using the 15-day trial[24].

- **Industry and sector[25]**

The cybersecurity industry presents moderate **barriers to entry**. While the sector is attractive due to its sustained growth and increasing demand for digital protection, new entrants face significant challenges. These include high initial capital requirements, the need for advanced technological infrastructure, specialized human capital, and strict regulatory compliance. These barriers limit the number of viable new competitors, although the market remains open to innovation-driven startups.

The **threat of substitution** is considerably high, driven by the continuous emergence of new technologies such as artificial intelligence, machine learning, and automation. These have the potential to replace traditional cybersecurity tools and practices. Faraday must constantly invest in research and development and maintain agility in adapting their solutions to evolving threats and client expectations to maintain competitiveness. Yet, not all substitutions are direct or immediate. Many AI-driven tools still require human oversight and are often integrated into, rather than replacing, existing systems. The real threat lies in

[23]WAGLE, K., YOUSUF, S., ALSWAILEM, Y., ALMENGASH, M., and ALTURKISTANI, F. *Turning a cybersecurity strategy into reality: A holistic performance management framework* [online]. Boston Consulting Group, 8 August 2022 [Accessed 14 June 2025]. Available from: https://www.bcg.com/publications/2022/cybersecurity-performance-management-framework

[24]PUJOL, Laurence. *Making freemium work* [online]. Harvard Business Review, May 2014 [Accessed 13 June 2025]. Available from: https://hbr.org/2014/05/making-freemium-work

[25]MCKINSEY & COMPANY. *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers* [online]. 27 October 2022 [Accessed 12 April 2025]. Available from: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

companies that can combine these technologies with superior user experience and faster deployment cycles[26].

Clients in the cybersecurity market are becoming more informed and demanding, particularly as awareness of digital risks grows. This increases their **buyer bargaining power,** especially in a market where multiple vendors offer overlapping services. However, Faraday mitigates this by offering tailored solutions and maintaining a strong value proposition through its all-in-one integral solution.

The sector relies heavily on highly skilled professionals with specialized expertise. Given the global shortage of cybersecurity talent and the complexity of the required knowledge, **suppliers hold significant bargaining power**. A key aspect for Faraday is to attract and retain their human capital, also maintaining its reputation and reliability, offering continuous training to stay on a competitive edge in the talent-driven market.

While competition is intense, it is also marked by a culture of collaboration. As noted in the company's practices, when a vulnerability is discovered, it is reported and assigned a unique identifier (e.g., CVE number), and the information is shared across the sector[27]. This collaborative way of working enhances collective security but also raises the bar for innovation and responsiveness. Companies must differentiate themselves not only through proprietary technology but also through their ability to contribute to and benefit from shared knowledge.

- **Competition**

The cybersecurity industry is currently in a growth phase of its **life cycle,** characterized by rapid expansion, technological innovation, and increasing regulatory oversight. The World Economic Forum[28] warns that hypercompetition is eroding long-term strategic advantages, pushing firms to adopt continuous innovation cycles and regulatory foresight, including trends like zero trust architecture, AI-driven threat detection, and data sovereignty will likely lead the next wave of cybersecurity evolution. Faraday competes with both established global firms and agile regional specialists.

---

[26]TANG, D. *What implications do advancements in cybersecurity technologies have on the competitive dynamics within Porter's Five Forces?* [online]. Flevy, [no date] [Accessed 14 June 2025]. Available from: https://flevy.com/topic/porters-five-forces/question/impact-cybersecurity-tech-porters-five-forces-strategy

[27]See Annex 2: *Transcript 1st Interview*

[28]WORLD ECONOMIC FORUM. *Global Cybersecurity Outlook 2024* [online]. 11 January 2024 [Accessed 14 June 2025]. Available from: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

In the Latin American market, Faraday faces competition from local firms such as Strike, Fluid Attacks, Kulkan Security, SecureTIA, and Base4Sec. These companies leverage regional expertise and competitive pricing strategies to secure market share, often operating as boutique consultancies or providers of specialized cybersecurity solutions. For example, Strike provides a client-oriented pentesting through a real-time interactive platform, enabling continuous monitoring and rapid vulnerability notifications, consequently offering a more interactive and consultative experience with domain-specific experts. Similarly, Base4Sec offers advanced methodologies like adversarial emulation and social engineering, enhancing their solutions portfolio by addressing both technical and human vulnerabilities, among these, phishing, smishing, and vishing threats. These added layers of specialization make their penetration testing offerings more comprehensive and competitive within the region. Faraday must innovate and lead to stay competitive in Latin America's growing cybersecurity market, where success depends on combining advanced technology with tailored consulting.

In comparison, the U.S. market is far more mature and competitive, dominated by large well-established firms such as Rapid7, Pentera, Bishop Fox, Vulcan Cyber, and JupiterOne. These operate on similar domains such as vulnerability management, penetration testing, and cloud security posture management yet at a scale that currently exceeds Faraday's capacity. Bishop Fox stands out as a particularly significant competitor. Known for its offensive security expertise, Bishop Fox serves high-profile clients such as Google, Amazon, and Zoom. Their innovative service offerings go beyond virtual breach tests to include physical heist trials, demonstrating a comprehensive approach to security that poses a substantial threat to other companies. While Faraday offers services comparable in scope to those of larger competitors, its principal disadvantage in the U.S. market is not technological capability but pricing. The scale and promotional capacity of these firms afford them greater visibility and market penetration, prompting Faraday to pursue alternative strategies for market entry and stakeholder engagement.

Despite its smaller size, Faraday leverages its integrated platform that consolidates multiple cybersecurity tools with expert consulting to compete effectively in both regions. The high barriers to entry in the cybersecurity sector provide a protective advantage against new entrants, enabling Faraday to focus on innovation and strategic positioning. Particularly in Latin America, where the market is less saturated but rapidly growing, Faraday has ample opportunity to differentiate itself and strengthen its market presence.

Macro-environment (PESTEL)

Political

1. Government regulations

In **Argentina**, cybersecurity regulations are evolving, with the National Directorate of Cybersecurity (DNSC)[29] overseeing national strategies. The "Law on the Protection of Personal Data" (Law 25,326)[30] aligns with international data privacy standards, like GDPR[31]. Regulatory functions are fragmented across various ministries, leading to inconsistent enforcement. Also, the lack of local cybersecurity talent presents challenges for the sector. This evolving regulatory landscape is crucial for cybersecurity firms, as it impacts compliance and innovation.

Germany has a robust cybersecurity regulatory framework, including the IT Security Act (IT-Sicherheitsgesetz)[32] and compliance with the EU's NIS Directive[33]. These regulations ensure cybersecurity resilience, especially in critical sectors such as energy, water supply, healthcare, finance, transportation, and IT infrastructure, which are considered essential for national security and public welfare. Additionally, the GDPR mandates strict data protection measures[34]. This regulatory environment presents both challenges and opportunities for cybersecurity firms operating in Germany, ensuring high standards for security but creating complexity in compliance.

The **United States** has a well established cybersecurity regulatory landscape that includes the Cybersecurity Information Sharing Act (CISA)[35] and key agencies like the NIST

---

[29]ARGENTINA. *Cybersecurity. Buenos Aires: Chief of the Cabinet of Ministers, Secretariat of Innovation, Science and Technology,* [no date] [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/ciberseguridad

[30]ARGENTINA. *Law No. 25.326 on Personal Data Protection. Buenos Aires: National Congress of the Argentine Republic, 2000* [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790

[31]EUROPEAN UNION. *Data Protection under the General Data Protection Regulation (GDPR)*. Brussels: European Union, 2025. Available at: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

[32]GERMANY. *IT Security Act (IT-Sicherheitsgesetz)*. Bonn: Federal Ministry of the Interior, Building and Community, 2015 [Accessed 11 May 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig.html

[33]EUROPEAN UNION. *NIS2 Directive: New rules on cybersecurity of network and information systems*. Brussels: European Commission, 2025 [Accessed 15 May 2025]. Available from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[34]DLA PIPER. *Data protection laws in Germany* [online]. 2025 [Accessed 11 May 2025]. Available from: https://www.dlapiperdataprotection.com/?t=law&c=DE

[35]UNITED STATES. *Cybersecurity Information Sharing Act of 2015*. Washington, D.C.: U.S. Cybersecurity and Infrastructure Security Agency, 2015 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

Cybersecurity Framework[36] or CISA Cybersecurity and Infrastructure Security Agency[37]. Federal Law requires companies to meet data protection and cybersecurity standards. While the federal government focuses on critical infrastructure security, state-level regulations can create a fragmented compliance environment, offering both opportunities and challenges for cybersecurity firms.

2. Political stability

Argentina has faced significant political instability in recent years, marked by frequent changes in government, economic crises, and social unrest. The election of Javier Milei in 2023 signaled a shift towards more market-oriented policies, but the country's political environment remains volatile, with uncertainty surrounding economic reforms. This instability can impact businesses, by making it difficult to establish sustainable partnerships with public actors, furthermore creating an unpredictable regulatory environment and increasing the risk of policy changes.

Germany is known for its political stability, which is a result of its strong democratic institutions, rule of law, and solid economic policies. The country has a long history of stable coalition governments, and its political system is designed to maintain checks and balances. While political shifts, such as the rise of the Green Party, have introduced new policies, these changes are generally well-managed and predictable. This stability fosters a conducive environment for business growth, including in the cybersecurity sector.

The **United States** has generally maintained political stability, but its political environment has become increasingly polarized in recent years, particularly following the 2020 election and the January 6th Capitol riot. Despite this, the U.S. political system remains resilient, with a strong democratic framework and stable institutions in which cybersecurity remains as a concern supported across administrations, for national security, infrastructure and data protection agendasThis political stability offers a predictable business environment.

3. Cybersecurity policies

In **Argentina**, cybersecurity policies are still developing, with the National Directorate of Cybersecurity (DNSC) working to establish frameworks to safeguard critical infrastructure and improve overall security. While the country has implemented some regulations, such as

[36]UNITED STATES. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology, 2024 [Accessed 11 May 2025]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[37]CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). *Leadership.* Washington, D.C.: CISA, 2025 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/about/leadership

the "Law on the Protection of Personal Data" (Law 25,326), there is a lack of comprehensive cybersecurity legislation. The government's focus on digital transformation and e-government services is driving the need for stronger cybersecurity measures, but enforcement remains inconsistent. This leaves businesses facing challenges in navigating a fragmented policy landscape.

Germany has a strong and comprehensive cybersecurity policy framework, boosted by the IT Security Act (IT-Sicherheitsgesetz) and adherence to the EU's Network and Information Systems (NIS) Directive[38]. These laws set out clear guidelines for securing critical infrastructure, data protection, and incident response. Additionally, the country's emphasis on GDPR ensures that businesses adhere to stringent data privacy standards. The German government also promotes cybersecurity through initiatives like the German Cyber Security Strategy[39], which focuses on enhancing resilience against cyberattacks and fostering innovation in cybersecurity technologies.

United States

The U.S. leads global cybersecurity policy through the National Cybersecurity Strategy, coordinated by the Office of the National Cyber Director (ONCD)[40]. This strategy is supported by implementation tools such as federal procurement standards for example FedRAMP or NIST frameworks that give a comprehensive approach to securing cyberspace, highlighting the need for an even more robust collaboration between public and private sectors. It emphasizes two key elements; on one hand the need to redistribute responsibility in order to defend cyberspace towards the most capable actors and, on the other, the importance of realigning incentives to favor long-term investments in cybersecurity.[41] The strategy also focuses on enhancing the cybersecurity of critical infrastructure and promoting international partnerships to counter cyber threats.

---

[38]EUROPEAN UNION. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Luxembourg: Publications Office of the European Union, 2022 [Accessed 11 May 2025]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[39]GERMANY. *Cyber Security Strategy for Germany.* Bonn: Federal Office for Information Security (BSI), 2016 [Accessed 11 May 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Strategie/strategie_node.html

[40]OFFICE OF THE NATIONAL CYBER DIRECTOR (ONCD). *Office of the National Cyber Director*. Washington, D.C.: The White House, 2025 [Accessed 27 May 2025]. Available from: https://www.whitehouse.gov/oncd/

[41]WALTZMAN, Howard W.; LILLEY, Stephen; HICKEY, Adam S. *White House releases National Cybersecurity Strategy Implementation Plan, Version 2.* Chicago: Mayer Brown LLP, 14 May 2024 [Accessed 27 May 2025]. Available from: https://www.mayerbrown.com/en/insights/publications/2024/05/white-house-releases-national-cybersecurity-strategy-implementation-plan-version-2

Economic

1. Market demand for cybersecurity

In **Argentina**, the market demand for cybersecurity is growing as digital transformation accelerates across industries. However, economic instability and inflation challenges limit companies' ability to invest heavily in cybersecurity solutions. Despite this, there is an increasing awareness of the need for robust cybersecurity measures[42], especially in sectors such as finance, healthcare, and government. Companies are beginning to recognize the importance of protecting sensitive data amid a rise in cyber threats. Still, budget constraints often lead to a reliance on cost-effective, often less advanced, cybersecurity solutions.

Germany has a highly developed market for cybersecurity, driven by stringent regulations such as the IT Security Act and the EU's GDPR. As one of Europe's largest economies, Germany's demand for cybersecurity solutions is strong across all sectors, including critical infrastructure, finance, and manufacturing. The increasing threat of cyberattacks and data breaches has led to significant investment in cybersecurity technology and services. Companies are prioritizing cybersecurity due to the economic and reputational risks associated with data breaches. This trend is expected to continue as Germany continues to enhance its digital economy.

In the **United States,** the market demand for cybersecurity is the largest and most mature, fueled by the country's advanced digital infrastructure and increasing frequency of cyberattacks. Both private and public sectors are investing heavily in cybersecurity to protect sensitive data, intellectual property, and critical infrastructure[43]. The growing adoption of cloud computing, IoT, and remote work further amplifies the need for robust cybersecurity solutions. Moreover, regulations like the CCPA[44] and CISA[45] are pushing businesses to improve their cybersecurity measures. As cyber threats evolve, U.S. companies are committed to continuously upgrading their cybersecurity defenses.

---

[42]CASTILLO, Gonzalo; JAMELE, Agustín. *Cybersecurity in Argentina: Current Situation, Laws, and Crimes*. Buenos Aires: InnovaciónDigital360, 19 February 2025 [Accessed 11 May 2025]. Available from: https://www.innovaciondigital360.com/cyber-security/ciberseguridad-en-argentina-actualidad-leyes-y-delitos/

[43]GONZÁLEZ, Paloma. *USA: Increased Investments in Cybersecurity Amid Rising Data Breaches*. Buenos Aires: Asociación Argentina de Compañías de Seguros (AACS), 5 September 2024 [Accessed 11 May 2025]. Available from: https://novedades.aacs.org.ar/eeuu-intensifican-inversiones-en-ciberseguridad-ante-el-aumento-de-las-filtraciones-de-datos/

[44]CALIFORNIA. *California Consumer Privacy Act of 2018*. Sacramento: California State Legislature, 2018 [Accessed 11 May 2025]. Available from: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[45]UNITED STATES. *About CISA*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/about

2. **Economic downturns**

Argentina has experienced recurring economic downturns characterized by high inflation, currency devaluation, and fiscal deficits[46]. These conditions reduce purchasing power and corporate budgets, directly impacting investment in technology, or more precisely, in cybersecurity. Many businesses struggle to prioritize it financially during economic crises, limiting the growth potential for cybersecurity firms operating in the country. In addition, government procurement is slow and highly regulated, reducing opportunities for local cybersecurity providers like Faraday to scale through the public sector.

Germany's economy, while generally stable, has faced recent slowdowns due to global supply chain disruptions, high energy prices, and inflation pressures, particularly after the war in Ukraine[47]. Although it remains one of Europe's strongest economies, these downturns have led some companies to tighten IT budgets. However, cybersecurity is often considered essential, so investment typically remains resilient even during recessions. The German government continues to support digital security initiatives to maintain economic and infrastructure stability.

The **United States** has weathered several economic downturns, including the COVID-19 recession and recent inflation-driven slowdowns. Despite temporary contractions, cybersecurity spending has shown strong resilience, as organizations increasingly see it as a non-discretionary expense. During downturns, companies may reduce other IT investments but continue to fund cybersecurity to protect digital assets and maintain compliance with regulations. This dynamic makes the U.S. cybersecurity market more resistant to economic fluctuations than other tech sectors[48].

3. **Cost of technology and talent**

In **Argentina**, the cost of technology remains high due to import restrictions, taxes, and currency volatility, making it expensive for companies to access cutting-edge cybersecurity tools. However, the country offers access to a highly skilled and technically proficient workforce, particularly in urban centers like Buenos Aires. This combination creates an opportunity for international firms to outsource services in the country, but inflation and economic instability often affect salary expectations and talent retention.

---

[46]WORLD BANK. *Argentina – World Bank Open Data*. Washington, D.C.: World Bank, 2025 [Accessed 11 May 2025]. Available from: https://data.worldbank.org/country/argentina

[47]FRANCE 24. *Germany's Economy Ahead of the Elections: Europe's Locomotive Running at Half Speed*. Paris: France 24, 22 February 2025 [Accessed 11 May 2025]. Available from: https://www.france24.com/es/programas/econom%C3%ADa/20250222-la-econom%C3%ADa-alemana-ante-las-elecciones-la-locomotora-europea-opera-a-media-marcha

[48]STATISTA. *Cybersecurity – United States*. Hamburg: Statista, 2025 [Accessed 11 May 2025]. Available from: https://www.statista.com/outlook/tmo/cybersecurity/united-states

Germany has high labor costs and strong worker protections, making cybersecurity talent relatively expensive. The country faces a growing shortage of skilled cybersecurity professionals, which drives up wages and intensifies competition among companies. At the same time, Germany maintains good access to advanced technologies at competitive prices thanks to its strong industrial base and integration within the EU market. These factors make cybersecurity operations costly but high-quality.

The **United States** has one of the highest cost globally for both technology and cybersecurity talent[49]. Demand for skilled professionals outpaces supply, driving salaries up significantly. In major tech hubs like Silicon Valley and New York, cybersecurity experts command premium wages. While access to advanced tools and innovation is unparalleled, the high cost of labor and software licenses can be a barrier for smaller firms. Nevertheless, the U.S. remains a global leader in cybersecurity innovation and investment, therefore competing with large U.S.-based firms can be challenging without formal recognition or local presence

Social

1. **Increasing cybersecurity awareness**

In **Argentina**, there is a growing awareness of cybersecurity[50], particularly among businesses that handle sensitive customer data, such as financial institutions and e-commerce companies. However, general public awareness remains limited, with many individuals unaware of the risks associated with cyber threats. The government and private sectors are gradually pushing for more cybersecurity education, especially with the rise of digital transformation. Still, significant efforts are needed to improve cybersecurity knowledge among the broader population, as the country faces challenges related to digital literacy. Government agencies acknowledge the need for cybersecurity but often lack the expertise or strategic planning capacity to act.

Germany is a leader in cybersecurity awareness, largely due to stringent regulations like the General Data Protection Regulation (GDPR) and strong public-private partnerships. Public awareness campaigns have been effective, and Germany has a robust digital literacy infrastructure. The country is also home to organizations like the Federal Office for

[49]K, Anjali. *Cybersecurity Services Cost in the USA: What to Expect in 2024*. LinkedIn, 12 September 2024 [Accessed 11 May 2025]. Available from: https://www.linkedin.com/pulse/cybersecurity-services-cost-usa-anjali-k-iriuf/

[50]ARGENTINA. *Second National Cybersecurity Strategy Approved*. Buenos Aires: Presidency of the Nation, 5 September 2023 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad

Information Security (BSI)[51], which provides cybersecurity education and resources. German companies, especially those in critical sectors, are highly proactive in adopting cybersecurity practices, and there is a strong cultural focus on data protection.

In the **United States**, cybersecurity is relatively high-priority issue, partly due to the prevalence of cyberattacks and breaches that receive extensive media coverage. National initiatives, such as National Cybersecurity Awareness Month (October)[52], aim to educate both businesses and individuals on safe online practices. Government organizations like the Cybersecurity and Infrastructure Security Agency (CISA) and private sector campaigns also contribute significantly to public knowledge. Despite this, challenges remain in terms of ensuring that all demographics are equally educated about cybersecurity.

2. Remote work trends

Remote and hybrid work in **Argentina** has significantly grown, particularly in the tech and service sectors, as a result of the COVID-19 pandemic. This trend expands the digital attack surface and requires platforms like Faraday to provide adaptable and centralized security monitoring. However, economic challenges such as inflation and unstable internet connectivity can sometimes hinder the sustainability of remote work in certain regions. The government's introduction of a Digital Nomad Visa[53] in 2022 has also encouraged international professionals to work remotely from Argentina. Despite these advancements, remote work adoption remains varied, with urban areas like Buenos Aires seeing more widespread acceptance compared to rural locations.

Germany has seen a steady rise in remote work, with approximately 23.5% of workers regularly working from home as of 2023[54]. The country boasts robust digital infrastructure, which has made the transition to remote work smoother for both employees and employers. Additionally, German companies are adapting to this shift by providing financial support for home office setups and offering flexible work arrangements, making remote work an

---

[51]EUROPEAN COMMISSION. *Federal Office for Information Security (BSI)*. Brussels: European Commission, 2025 [Accessed 11 May 2025]. Available from: https://digital-skills-jobs.europa.eu/en/organisations/federal-office-information-security-bsi

[52]UNITED STATES. *Cybersecurity Awareness Month*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2024 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/cybersecurity-awareness-month

[53]ARGENTINA. *Digital Nomad Visa*. Buenos Aires: Ministry of Foreign Affairs, International Trade and Worship, 28 January 2025 [Accessed 11 May 2025]. Available from: https://ctoro.cancilleria.gob.ar/es/visa-para-n%C3%B3madas-digitales

[54]GERMANY. *Employed Persons Working from Home*. Wiesbaden: Federal Statistical Office of Germany, 2025 [Accessed 11 May 2025]. Available from: https://www.destatis.de/EN/Themes/Labour/Labour-Market/Quality-Employment/Dimension3/3_11_homeoffice.html

attractive option for many. The trend continues to grow, driven by both cultural acceptance and government policies promoting work-life balance[55].

In the **United States,** remote and hybrid work models have become institutionalized across labor markets. As of 2023, about 35% of full-time employees work remotely at least part-time[56]. This trend has been particularly strong among white-collar workers in sectors like technology, finance, and marketing. Despite some companies attempting to bring employees back to the office, many workers continue to demand the flexibility remote work offers, making it a dominant aspect of the workforce. This trend is expected to persist, even as the overall economy adjusts to post-pandemic realities.

3. Employee training and awareness

In **Argentina**, employee cybersecurity training is gaining traction, particularly within the public sector. A study by the Inter-American Development Bank (IDB) conducted a randomized controlled trial to assess the effectiveness of cybersecurity training among public employees, focusing on reducing exposure to phishing attacks[57]. The study found that targeted training significantly improved employees' ability to identify and respond to cyber threats. Within the public sector, there are major gaps in user-level cybersecurity practices, creating a need for external tools that simplify risk visibility and auditability.

Germany places a strong emphasis on cybersecurity awareness and training, driven by stringent data protection regulations like the General Data Protection Regulation (GDPR). Companies invest in comprehensive training programs to educate employees about cyber threats and best practices.

In the **United States,** employee cybersecurity training is a critical component of organizational security strategies. The Cybersecurity and Infrastructure Security Agency (CISA) offers a Cybersecurity Awareness Program[58] that provides resources and tools to help individuals and organizations make informed decisions about cybersecurity.

---

[55]MICHAEL BAILEY ASSOCIATES. *Flexible Working in 2023 – Germany*. Düsseldorf: Michael Bailey Associates GmbH, 2025 [Accessed 11 May 2025]. Available from: https://www.michaelbaileyassociates.com/app/public/pdf/Flexible-working-in-2023-germany.pdf

[56]INVESTOPEDIA. *Remote Work Is Here to Stay, New Data Shows*. New York: Dotdash Meredith, 2024 [Accessed 11 May 2025]. Available from: https://www.investopedia.com/remote-work-is-here-to-stay-new-data-shows-8671287

[57]KEEFER, Philip; ROSETH, Benjamin; SANTAMARIA, Julieth. G*eneral Skills Training for Public Employees: Experimental Evidence on Cybersecurity Training in Argentina*. Washington, D.C.: Inter-American Development Bank, 2024. (IDB Working Paper Series; No. IDB-WP-1643) [Accessed 11 May 2025]. Available from: https://doi.org/10.18235/0013202

[58]UNITED STATES. *CISA Cybersecurity Awareness Program*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025. [Accessed 11 May 2025]. Available from: https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program

Furthermore, the Department of Health and Human Services mandates annual information security awareness training for all employees and contractors, ensuring compliance with federal regulations and enhancing the overall security posture[59].

Technological

1. **Advancements in cybersecurity technology**

Argentina's cybersecurity sector is experiencing significant growth, with the market projected to reach USD 1.04 billion in 2025 and expand at a compound annual growth rate (CAGR) of 11.12% through 2030[60]. This growth is driven by increased digitalization across various sectors, including finance, healthcare, and e-commerce. While the country's adoption of cutting-edge cybersecurity technologies typically lags two to three years behind mature markets like the UK and the US, this delay can also present an opportunity for cybersecurity companies to capitalize on technologies already tested abroad, reducing implementation risks and accelerating innovation locally. The government is exploring the integration of artificial intelligence (AI) into crime investigations, including real-time facial recognition and drone surveillance, although these initiatives have raised concerns regarding privacy and civil liberties[61].

Germany is proactively enhancing its cybersecurity infrastructure in response to a growing threat landscape. The Federal Office for Information Security (BSI) has reported a concerning increase in cyber threats, particularly targeting small and medium-sized enterprises (SMEs) and public institutions. To combat these threats, Germany is investing in advanced technologies such as cloud security and incident response systems[62]. The country's cybersecurity market is projected to grow at a CAGR of 11.25%, reaching USD 21.47 billion by 2029[63]. Furthermore, Germany is aligning with the European Union's Cyber

---

[59]UNITED STATES. *Security Awareness and Training*. Washington, D.C.: Department of Health and Human Services, Office of the Chief Information Officer, 2024. [Accessed 11 May 2025]. Available from: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

[60]MORDOR INTELLIGENCE. *Argentina Cybersecurity Market – Size, Share & Trends*. Hyderabad: Mordor Intelligence, 2025. [Accessed 11 May 2025]. Available from: https://www.mordorintelligence.com/industry-reports/argentina-cybersecurity-market

[61]BORAK, Masha. *Argentina's plan to fight crime with AI draws concerns from rights groups*. Biometric Update, 2 August 2024. [Accessed 11 May 2025]. Available from: https://www.biometricupdate.com/202408/argentinas-plan-to-fight-crime-with-ai-draws-concerns-from-rights-groups

[62]FOURRAGE, Ludo. *Germany Cybersecurity Job Market: Trends and Growth Areas for 2024*. Nucamp, Seattle, 2024. [Accessed 11 May 2025]. Available from: https://www.nucamp.co/blog/coding-bootcamp-germany-deu-germany-cybersecurity-job-market-trends-and-growth-areas-for-2024

[63]RESEARCH AND MARKETS. *Germany Cybersecurity Market Share Analysis, Industry Trends & Growth Forecasts 2024–2029*. Research and Markets, Dublin, 2024. [Accessed 11 May 2025]. Available from: https://www.globenewswire.com/news-release/2024/09/16/2946526/28124/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html

Resilience Act, aiming to bolster the overall cybersecurity posture across the EU by ensuring the integrity and availability of digital products and services.[64]

The **United States** continues to lead in cybersecurity technological advancements, focusing on integrating artificial intelligence (AI) and machine learning (ML) to enhance threat detection and response capabilities. The Department of Homeland Security's Science and Technology Directorate is exploring AI and ML applications to process large volumes of data for improved cybersecurity resilience[65].

2. Rising cyber threats

Argentina's cybercriminal activities have escalated, including ransomware attacks and data breaches, prompting the government to enhance its cybersecurity measures[66]. The National Cybersecurity Strategy emphasizes the importance of strengthening digital infrastructure and promoting cybersecurity awareness among citizens and organizations. Despite these efforts, challenges remain in addressing the rapidly evolving threat landscape and ensuring the resilience of digital systems.

Germany faces a growing array of cyber threats, with a notable rise in malware and ransomware attacks. The Federal Office for Information Security (BSI) reported a 26% increase in the discovery of new malware variants between mid-2023 and mid-2024, averaging 309,000 daily[67]. These attacks often target small and medium-sized enterprises (SMEs) and municipalities, which may have less robust cybersecurity defenses. The BSI continues to collaborate with international partners to mitigate these threats and enhance national cyber resilience.

The **United States** is confronting an escalating cyber threat landscape, with state-sponsored actors and cybercriminal groups increasingly targeting critical infrastructure sectors such as healthcare, energy, and finance. The FBI published their Annual Internet Crime Report

---

[64]LÖLFING, Nils; HEMBT, Simon; BELITZ, Oliver; KARCHER, Benjamin. *Artificial Intelligence 2024 – Germany: Trends and Developments*. Chambers and Partners, London, 2024. [Accessed 11 May 2025]. Available from: https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/germany/trends-and-developments

[65]UNITED STATES. *Leveraging AI to Enhance the Nation's Cybersecurity*. Department of Homeland Security, Science and Technology Directorate, Washington, D.C., 17 October 2024. [Accessed 11 May 2025]. Available from: https://www.dhs.gov/group/13025/news/2024/10/17/feature-article-leveraging-ai-enhance-nations-cybersecurity

[66]ARRIETA, Fernando. *Crecen los intentos de ciberataques en Argentina*. Parlamentario, 2 July 2024. [Accessed 11 May 2025]. Available from: https://www.parlamentario.com/2024/07/02/crecen-los-intentos-de-ciberataques-en-argentina/

[67]THE CYBER EXPRESS. *Germany State of Cybersecurity 2024 Report*. The Cyber Express, 9 May 2025. [Accessed 11 May 2025]. Available from: https://thecyberexpress.com/germany-state-of-cybersecurity-2024-report/

where it reported losses exceeding $16 billion, a 33% increase in losses from 2023[68]. The government is intensifying efforts to bolster cybersecurity defenses, including the development of offensive cyber capabilities and international collaborations to deter malicious cyber activities.

3. Integration with other tools

In **Argentina**, companies are increasingly adopting Security Information and Event Management (SIEM) systems[69], endpoint detection and response (EDR) solutions[70], and threat intelligence platforms to enhance their security posture. However, many small and medium-sized enterprises (SMEs) still face challenges in integrating these tools due to budget constraints and a lack of technical expertise. To address these issues, the Argentine government, with support from the Inter-American Development Bank (IDB), is implementing the Cybersecurity Program for Critical Information Infrastructures[71], aiming to improve early detection capabilities and reduce the impact of cyberattacks.

In **Germany** companies are leveraging advanced tools such as Security Operations Centers (SOCs), threat intelligence platforms, and automated incident response systems to enhance their cybersecurity frameworks. The government supports these efforts through initiatives like the Alliance for Cyber Security[72], which promotes collaboration between public and private sectors to develop and integrate effective cybersecurity solutions.

The **United States** leads in the integration of cybersecurity tools, driven by the need to protect critical infrastructure and sensitive data. Federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), have developed the National Cybersecurity Protection System (NCPS)[73], an integrated system-of-systems that delivers capabilities like intrusion detection, analytics, and information sharing. This system enables federal agencies to secure and defend their information technology infrastructure against advanced cyber threats.

---

[68]UNITED STATES. *FBI Releases Annual Internet Crime Report*. Washington, D.C.: Federal Bureau of Investigation, 23 April 2025. [Accessed 11 May 2025]. Available from: https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[69]CISCO. What Is SIEM? - *Security Information and Event Management*. San Jose: Cisco Systems, 2025. [Accessed 11 May 2025]. Available from: https://www.cisco.com/c/en/us/products/security/what-is-siem.html

[70]IBM. *What is Endpoint Detection and Response (EDR)?*. IBM, 2025. [Accessed 11 May 2025]. Available from: https://www.ibm.com/es-es/topics/edr

[71]INTER-AMERICAN DEVELOPMENT BANK. *Cybersecurity for Critical Information Infrastructure Program (AR-L1343)*. Washington, D.C.: IDB, 2023. [Accessed 11 May 2025]. Available from: https://www.iadb.org/en/project/AR-L1343

[72]FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). *The Alliance for Cyber Security. Bonn: BSI, 2025*. [Accessed 11 May 2025]. Available from: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/ACS/acs_node.html

[73]UNITED STATES. *National Cybersecurity Protection System*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025. [Accessed 11 May 2025]. Available from: https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system

Environmental

1. Sustainability of data centers

In **Argentina**, the sustainability of data centers is an emerging concern as digital infrastructure expands. While the country has not yet implemented specific regulations targeting data center sustainability, there is a growing awareness of the environmental impact of increased energy consumption and carbon emissions associated with data storage and processing. Discussions around energy self-production and the adoption of renewable energy sources are gaining traction, aiming to reduce dependence on fossil fuels and enhance the resilience of data centers[74].

Germany's enactment of the Energy Efficiency Act in 2024[75] mandates data centers to improve energy efficiency, utilize renewable energy sources, and implement energy management systems. Operators are also encouraged to reuse waste heat and reduce overall environmental impact. Companies like Hetzner are leading by example, sourcing electricity from 100% renewable energies and achieving substantial reductions in CO_2 emissions. These initiatives reflect Germany's commitment to aligning digital infrastructure growth with environmental stewardship.

In the **United States**, data centers account for over 4% of total electricity consumption, with a significant portion derived from fossil fuels, leading to substantial CO_2 emissions[76]. The rapid expansion of AI and cloud services has intensified energy demands, prompting major tech companies to seek sustainable solutions. Policy shifts, such as the suspension of clean energy initiatives, have raised concerns about the future of sustainable data center operations[77].

---

[74]ODATA. *Revolutionizing Data Infrastructure: Understand the Role of Energy Self-Production.* ODATA, 8 May 2024. [Accessed 11 May 2025]. Available from: https://odatacolocation.com/en/blog/energy-self-production/

[75]FEDERAL GOVERNMENT OF GERMANY. *The Energy Efficiency Act: the public sector is set to become a role model*. Berlin: Federal Government of Germany, 2022. [Accessed 11 May 2025]. Available from: https://www.bundesregierung.de/breg-de/service/archiv/the-energy-efficiency-act-2184958

[76]SHEHABI, A., SMITH, S. J., HUBBARD, A., NEWKIRK, A., LEI, N., SIDDIK, M. A., HOLECEK, B., KOOMEY, J. G., MASANET, E. R. & SARTOR, D. A. 2024. *United States Data Center Energy Usage Report*. Berkeley: Lawrence Berkeley National Laboratory, 19 December 2024. [Accessed 11 May 2025]. Available from: https://eta-publications.lbl.gov/sites/default/files/2024-12/lbnl-2024-united-states-data-center-energy-usage-report.pdf

[77]JOHNSON, L. 2025. *Trump pauses renewable projects leasing on federal lands, waters*. ESG Dive, 29 January. [Accessed 11 May 2025]. Available from: https://www.esgdive.com/news/trump-pauses-renewable-projects-leasing-on-federal-lands-waters-interior-executive-order/738647/.

2. Energy consumption

Argentina's energy consumption is largely dominated by natural gas, which accounts for nearly 60% of its total energy consumption[78]. The country also relies significantly on petroleum products, primarily for transport and industry. Argentina's energy infrastructure faces challenges in terms of inefficiency and reliance on fossil fuels, although the government has set ambitious goals for increasing renewable energy usage. In 2022, Argentina aimed to expand renewable energy capacity under its RenovAr program[79], which focuses on wind and solar power projects. However, despite these efforts, fossil fuels remain dominant, and the country continues to face energy security and affordability challenges.

Germany's primary energy consumption reached a new low in 2024, dropping 1.3% to 10,478 petajoules, nearly 30% less than in 1990. This decline is attributed to factors such as warmer weather, a weakened economy, and ongoing efficiency improvements. Renewable energy sources contributed 20% to primary energy consumption in 2024[80]. The share of renewables in gross electricity consumption reached a record 62.7%, with solar power generation hitting a new high of 72.2 terawatt-hours[81]. Despite these advancements, the country faces challenges in balancing renewable energy generation with demand, particularly during periods of low wind and solar availability.

In 2024, the **United States** experienced record electricity consumption, driven by increased demand from data centers, manufacturing, and the electrification of transportation and buildings[82]. Total electricity consumption is projected to reach 4,101 billion kilowatt-hours (kWh) in 2024 and 4,185 billion kWh in 2025[83]. While carbon dioxide emissions related to energy decreased by 4% in 2023[84], the country continues to depend heavily on fossil fuels,

---

[78]INTERNATIONAL ENERGY AGENCY. 2025. *Argentina – Energy Profile*. Paris: International Energy Agency. [Accessed 11 May 2025]. Available from: https://www.iea.org/countries/argentina.

[79]ARGENTINA. 2025. *RenovAr: Renewable Energy Supply Program*. Buenos Aires: Ministry of Economy. [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/economia/energia/energia-electrica/renovables/renovar.

[80]APPUNN, K. 2024. *Primary energy use in Germany drops to new low in 2024, renewables cover 20%.* Clean Energy Wire, 18 December. [Accessed 11 May 2025]. Available from: https://www.cleanenergywire.org/news/primary-energy-use-germany-drops-new-low-2024-renewables-cover-20.

[81]FRAUNHOFER INSTITUTE FOR SOLAR ENERGY SYSTEMS ISE. 2025. *Public Electricity Generation 2024: Renewable Energies Cover More Than 60 Percent of German Electricity Consumption for the First Time*. Freiburg: Fraunhofer ISE. [Accessed 11 May 2025]. Available from: https://www.ise.fraunhofer.de/en/press-media/press-releases/2025/public-electricity-generation-2024-renewable-energies-cover-more-than-60-percent-of-german-electricity-consumption-for-the-first-time.html

[82]DiSavino, S. 2024. *US power use forecast to reach record highs in 2024 and 2025, EIA says*. Reuters, 10 September. [Accessed 11 May 2025]. Available from: https://www.reuters.com/business/energy/us-power-use-forecast-reach-record-highs-2024-2025-eia-says-2024-09-10/

[83]U.S. Energy Information Administration. 2025. *Short-Term Energy Outlook*. Washington, D.C.: U.S. Department of Energy, 6 May. [Accessed 11 May 2025]. Available from: https://www.eia.gov/outlooks/steo/

[84]International Energy Agency. 2024. *CO_2 Emissions in 2023*. Paris: IEA. [Accessed 11 May 2025]. Available from: https://iea.blob.core.windows.net/assets/33e2badc-b839-4c18-84ce-f6387b3c008f/CO2Emissionsin2023.pdf

which accounted for approximately 84% of total energy production in 2023[85]. The rapid expansion of artificial intelligence and cloud services is intensifying energy demands, posing challenges to achieving sustainability goals.

Legal

1. **Cybersecurity laws and compliance**

Argentina's cybersecurity legal framework is primarily anchored by Law No. 25,326, the Personal Data Protection Law (PDPL), which aligns with international standards and has been recognized by the European Commission for providing adequate data protection[86]. To address cybercrime, Argentina enacted Law No. 26,388[87], amending the Criminal Code to criminalize unauthorized access to computer systems, data interception, and system interference. In 2025, the government introduced the Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025–2027)[88] to enhance capabilities in preventing, detecting, and investigating cybercrimes nationwide.

Germany enforces a robust cybersecurity legal framework through the Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), which complements the EU's General Data Protection Regulation (GDPR). The BDSG incorporates provisions for data processing by federal and state authorities and private entities. Additionally, the IT Security Act 2.0, effective from 2021, mandates stringent security requirements for operators of critical infrastructure, including the certification of critical components and adherence to high-level security standards.

The **United States** maintains a multifaceted cybersecurity legal landscape comprising various federal and state laws. Key federal statutes include the Federal Trade Commission Act (FTCA), which addresses deceptive practices related to data security, and sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, and the Gramm-Leach-Bliley Act (GLBA) for financial institutions[89]. Recent developments

[85]U.S. Energy Information Administration. 2024. *U.S. Energy Facts Explained – Consumption and Production*. Washington, D.C.: U.S. Department of Energy. [Accessed 11 May 2025]. Available from: https://www.eia.gov/energyexplained/us-energy-facts/

[86]DLA PIPER. *Data Protection Laws of the World – Argentina*. [s.l.]: DLA Piper, [n.d.] [Accessed 11 May 2025]. Available from: https://www.dlapiperdataprotection.com/index.html?c=AR&t=law

[87]ARGENTINA. *Law No. 26.388: Modification of the Penal Code – Incorporation of Computer Crimes*. Buenos Aires: Official Gazette, 2008 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

[88]ALLENDE & BREA. *Argentina Approves the Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025–2027)*. Buenos Aires: Allende & Brea, 21 January 2025 [Accessed 11 May 2025]. Available from: https://allende.com/en/privacy-and-cybersecurity/argentina-approves-the-federal-plan-for-the-prevention-of-cybercrime-and-strategic-management-of-cybersecurity-2025-2027-01-21-2025/

[89]CONNECTWISE. *Cybersecurity Laws & Regulations*. Tampa, FL: ConnectWise, 2024 [Accessed 11 May 2025]. Available from: https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation

include the Securities and Exchange Commission's (SEC) 2023 guidelines requiring public companies to disclose material cybersecurity incidents within four business days.[90]

2. Intellectual property protection

In **Argentina,** intellectual property (IP) protection is managed by the National Institute of Industrial Property (INPI)[91] and is governed by the country's Intellectual Property Law 24.481[92]. Argentina follows international agreements like TRIPS[93] and the Paris Convention[94]. Patents last 20 years, and trademarks are valid for 10 years with indefinite renewals. However, enforcement challenges persist, particularly with counterfeits and slow judicial processes.

Germany's IP system, overseen by the German Patent and Trade Mark Office (DPMA),[95] aligns with EU regulations and the European Patent Convention[96]. Patents last up to 20 years, and trademarks are protected for 10 years. The country also complies with international IP standards, including TRIPS.

The **United States** follows international treaties like TRIPS and the Berne Convention[97]. The U.S. enforces IP laws strongly, with both civil and criminal penalties for infringement. However, challenges include patent trolling and copyright issues in the digital space.

3. Liability in case of breach

In **Argentina**, liability for cybersecurity breaches is primarily governed by the Civil and Commercial Code and specific cybersecurity laws like the "Cybercrime Law" 26.388. Companies that fail to secure personal data or systems can be held liable for damages. While there are provisions for data protection under the Personal Data Protection Law

---

[90]EWING, Greg; JODKA, Sara H. *But really, what cybersecurity requirements and standards does my company need to follow and why?* Reuters, 31 July 2024 [Accessed 11 May 2025]. Available from: https://www.reuters.com/legal/legalindustry/really-what-cybersecurity-requirements-standards-does-my-company-need-follow-why-2024-07-31/

[91]ARGENTINA. *Instituto Nacional de la Propiedad Industrial (INPI)*. Buenos Aires: Government of Argentina, 2025 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/inpi

[92]ARGENTINA. *Law No. 24,481: Patents of Invention and Utility Models*. Buenos Aires: Official Gazette, 23 May 1995 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-24481-27289

[93]WORLD TRADE ORGANIZATION. *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)* [online]. Marrakesh: WTO, 15 April 1994 [Accessed 11 May 2025]. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

[94]WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Paris Convention for the Protection of Industrial Property* [online]. Geneva: WIPO, 20 March 1883 [Accessed 11 May 2025]. Available from: https://www.wipo.int/treaties/en/ip/paris/

[95]GERMAN PATENT AND TRADE MARK OFFICE (DPMA). *About Us* [online]. Munich: DPMA, 3 April 2025 [Accessed 11 May 2025]. Available from: https://www.dpma.de/english/our_office/about_us/index.html

[96]EUROPEAN PATENT ORGANISATION. *European Patent Convention (EPC)* [online]. Munich: European Patent Office, 2020 [Accessed 11 May 2025]. Available from: https://www.epo.org/en/legal/epc/2020/convention.html

[97]LEGAL INFORMATION INSTITUTE (LII). *Berne Convention* [online]. Ithaca, NY: Cornell Law School, 2021 [Accessed 11 May 2025]. Available from: https://www.law.cornell.edu/wex/berne_convention

25.326, enforcement is often seen as lacking in practice. Argentine law encourages companies to implement cybersecurity measures, but legal accountability can be complex and difficult to enforce in cases of breach.

In **Germany**, the General Data Protection Regulation (GDPR) plays a crucial role in liability for data breaches, imposing significant fines for non-compliance. Companies are held liable for failing to protect personal data, with penalties reaching up to 4% of global turnover. Additionally, the German Telemedia Act (TMG)[98] and the IT Security Act (IT-Sicherheitsgesetz) regulate cybersecurity breaches and establish clear liability rules for organizations.

In the **United States**, liability for cybersecurity breaches is governed by a mix of federal and state laws, such as the Federal Trade Commission (FTC) Act[99], the California Consumer Privacy Act (CCPA), and sector-specific regulations like HIPAA for healthcare. Companies can be held liable for failing to implement adequate security measures, with penalties including fines and lawsuits. The U.S. legal framework focuses heavily on consumer protection and disclosure requirements, with strong enforcement actions by agencies like the FTC.

Stakeholders and Publics

Following Villafañe's model, this section focuses on the analysis of the Government and the Media. Given Faraday's position operating in highly regulated and strategically sensitive sectors, both government bodies and media actors play essential roles in the construction of public trust, access to contracts and partnerships, and the interpretation of risk and innovation in digital infrastructure. Therefore, this chapter presents a systematic approach to mapping these publics, segmenting them through tailored criteria, and evaluating the company's relationship with each actor based on observable attributes and indicators.

Government Public

Segmentation Criteria: The government public will be segmented according to the institutional division of powers in each country, adapting terminology and structure to each national context. Within the Executive Branch, the segmentation includes ministries,

[98]GERMANY. *Telemedia Act* (TMA) [online]. Berlin: Federal Ministry of Justice, 26 February 2007 [Accessed 11 May 2025]. Available from: https://www.hunton.com/privacy-and-information-security-law/assets/htmldocuments/uploads/sites/18/2016/02/Telemedia_Act__TMA_.pdf

[99]FEDERAL TRADE COMMISSION (FTC). *FTC en Español* [online]. Washington, D.C.: FTC, 2025 [Accessed 11 May 2025]. Available from: https://www.ftc.gov/es

secretariats and undersecretaries in Argentina, federal departments in the United States, and federal ministries in Germany. These are selected for their competencies in cybersecurity and digital policy, technological innovation, science, critical infrastructure, national defense, data protection, intelligence, and digital transformation.

In the Legislative Branch, segmentation will be centered on permanent commissions or committees aligned with science and technology, cybersecurity and infrastructure, defense and intelligence oversight and communication, privacy, and public procurement, adapted to the legislative organization of each country.

Regulatory Entities will be segmented based on their institutional relevance to define cybersecurity and data protection standards, enforce technical compliance and protocols, or grant certifications and access to public-sector procurement. These include autonomous data protection authorities (for example, AAIP in Argentina, BfDI in Germany); national standards bodies (ej NIST in the U.S., IRAM in Argentina, BSI in Germany) and cybersecurity-specific agencies (ej CISA, AFC, ENISA)

1. **Argentina** (See Annex 5)

The scope will be limited geographically to the Buenos Aires Metropolitan Area (AMBA), where most national-level government entities, ministries, and congressional bodies operates

2. **United States** (See Annex 6)

Conducted according to the federal structure of the United States. The analysis will be centered on Washington, D.C., the seat of all federal executive and congressional institutions, and cybersecurity-related subcommittees in the House and Senate.

3. **Germany** (See Annex 7)

The scope is geographically limited to Berlin and Bonn, where most national ministries and agencies operate. Focus will be placed on institutions such as the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI). Germany’s approach to cybersecurity is highly structured, emphasizing certification, EU alignment through ENISA, and collaboration with private actors under the IT-Sicherheitsgesetz (IT Security Act).

Media Public

Segmentation Criteria: For this analysis, a unified segmentation criterion was established to be applied consistently across the three selected countries. It is structured in several hierarchical levels that enable the classification of media outlets based on their format, geographic reach, thematic alignment with Faraday Security's strategic interests, and, finally, the key individuals within each outlet.

First, the type of media is considered, understood as the primary channel through which content is distributed. This classification distinguishes between print press, digital media, television, radio, and multiplatform formats such as podcasts or audiovisual productions disseminated across various channels. Second, the geographic reach of each outlet is analyzed, differentiating between those with national, regional, or local coverage, and those of an international nature with a local presence or direct influence in the country being evaluated. Third, the thematic focus of the outlet or its relevant sections is assessed. Priority is given to media that cover topics aligned with Faraday Security's areas of interest, such as cybersecurity, security and defense, and technology and innovation. Generalist media that include specialized sections on these subjects are also considered. Finally, the identification of key individuals within each selected outlet is taken into account, with particular attention to those who hold strategic roles in relevant areas. This includes directors, chief editors, section editors (particularly in fields such as technology, defense, business, or innovation) and journalists specializing in cybersecurity or related topics. This comprehensive segmentation approach aims not only to identify and prioritize the most relevant media outlets for the company's strategic positioning, but also to accurately map the key actors who can enable a direct and effective engagement with each outlet.

1. **Argentina** (See Annex 8)

Given that Argentina represents Faraday Security's primary client market, the segmentation in this country will follow a more in-depth and detailed approach. Priority will be placed on identifying national and regional media outlets with strong influence in the fields of technology, business, and security, including both specialized media and generalist outlets with relevant sections.

2. **United States** (See Annex 9)

The United States segmentation will only consider the main local media outlets with influence in the city where Faraday operates and national media platforms that aim Technology and Cybersecurity.

3. **Germany** (See Annex 10)

The focus will be on media that specializes in cybersecurity and technology, with particular emphasis on those with strong reach in Munich and southern Germany, where the company's local clients are located.

Non Governmental Public[100]

Segmentation Criteria: Segmented according to the role in shaping Argentina's cybersecurity and the overall digital ecosystem outside formal government structures, focusing on forums, associations, academic-industry collaborations and non-institutional actors. While not formally part of government structures, these can facilitate interaction, reputational visibility, and potential institutional partnerships between cybersecurity-related firms and public-sector representatives, industry peers, and other strategic stakeholders. Also, may enable connections with other publics such as investors or media.

We will segment the actors in four subsegments. Initially, taking into account **International Strategic Forums**, that, although held abroad, generate strategic exposure and connections with global representatives, policy influencers, and industry leaders that may result relevant to the Argentine cybersecurity context.

We will also focus on **National Industry Conferences and Forums**, considering these are high-impact entry points where the company gains exposure and positions itself nationally, also providing indirect national governmental interaction since public officials or regulators may attend to these.

Continuing, **Professional Associations & Networks** will be taken into account since these consolidate Faraday's legitimacy, collective influence and industry standards, also

[100] Refers to a specific type of public that operates outside the formal governmental structure, but still plays a strategic role in the national cybersecurity ecosystem. They are not NGOs in the humanitarian or charity sense, but rather sectoral, professional, and academic organizations that influence policies, standards, and public discourse related to cybersecurity.

allowing the company to go beyond visibility, indicating its commitment to advocacy while also enabling potential partnerships.

Finally, **Academic-Industry Collaborations** strengthen Faraday's commitment to national talent development by connecting with future industry professionals, providing them training, and at the same time, reinforcing their image as a socially responsible actor. Having in mind the skill shortages and requirements for the sector, these seem crucial not only for reputation-building but also to contribute in the shaping of the next cybersecurity professionals generation, resulting in an effective way of positioning as a trusted player in the ecosystem.
(See Annex 14)

Community Public

Segmentation Criteria: Segmented according to non-professional audiences, prioritizing end-user cybersecurity culture and societal resilience including local and tech user communities, educational outreach programs, NGOs, and public-sector campaigns that engage directly with citizens, students, and underserved groups by promoting cybersecurity awareness, digital inclusion, community resilience and safe technology practices in Argentina. They play a critical role in shaping the public perception of cybersecurity, expanding digital safety culture, and opening pathways for corporate social responsibility (CSR) and community-based brand positioning.

The segmentation is divided into three subcategories: Firstly, in **Local Awareness & Engagement Initiatives**. These are neighborhood and city-level events or programs that bring cybersecurity knowledge directly to the community through talks, workshops, and interactive activities. These spaces facilitate face-to-face interaction, encourage trust-building, and allow Faraday to strengthen its presence within the social fabric of local areas

Secondly, we focus on **Educational Outreach Programs and Activities** aimed at students, youth, and educational institutions, such as school talks, student-led clubs, and beginner-friendly competitions. This subsegment fosters early adoption of safe digital practices and develops interest in cybersecurity careers, creating a future talent pipeline.

Finally, we include **Social Inclusion Programs**, mostly NGOs and initiatives that integrate underrepresented groups into the digital ecosystem, mainly focusing on women,

low-income youth, and senior citizens. These platforms connect cybersecurity to broader social responsibility goals and offer Faraday opportunities to position itself as a socially conscious actor. (See Annex 15)

Internal Public

Segmentation Criteria: Faraday Security's internal publics play a decisive role in sustaining organizational culture, driving innovation, and ensuring service quality across a distributed team. Their engagement and alignment directly impact not only day-to-day performance but also the company's external credibility and reputation as a trusted cybersecurity partner. By identifying and addressing the specific needs of these groups, Faraday can strengthen collaboration, enhance employee experience, and reinforce its positioning as an agile, cohesive, and future-ready organization.

We will segment the actors in four subsegments. Initially, we will take into account **Executive Leadership & Management**, since this segment drives strategic direction, organizational culture, and decision-making processes. Their alignment and clarity of communication flow throughout the company, ensuring transparency, agility, and trust both internally and externally.

We will also focus on **Sales, Marketing & Client Relations**, considering these actors are Faraday's direct link with external stakeholders. Effective internal communication with this group ensures consistent messaging, product knowledge, and client-facing professionalism, strengthening the company's reputation and facilitating business growth.

Continuing, **Technical, Development & Operations Teams** will be considered as one unified segment. This segment represents the backbone of Faraday's offering—balancing innovation, reliability, and client satisfaction. Targeted communication here must support knowledge-sharing, collaboration, and professional development, especially in a sector defined by skill shortages and rapid change.

Finally, **Support & Administrative Staff** will be taken into account. Although often less visible, these actors enable organizational efficiency and stability, ensuring that critical functions such as HR, finance, and logistics run smoothly. By reinforcing their importance and integrating them fully into Faraday's cultural narrative, internal communication can increase engagement, motivation, and long-term loyalty, contributing indirectly to external reputation. (See Annex 16)

Variables Matrix

While the analytical framework is built around three general variables—Awareness Level, Engagement Frequency, and Potential Influence—each public is also assessed using two specific variables adapted to its nature. The goal is to produce a diagnosis of the current state of the relationship between Faraday and each public, and to identify opportunities for strategic communication and stakeholder engagement in future stages of development

	Variables	Definition	Indicators + Measurement Criteria (Annual)	
GENERAL VARIABLES	**Awareness Level**	Measures the degree to which the public knows Faraday and correctly identifies its role or services within the cybersecurity sector	High (3pts)	The stakeholder has publicly mentioned Faraday **≥4 times** (e.g., in documents, events, social media, press releases) **and** associates it with cybersecurity services.
			Medium (2pts)	Faraday has been mentioned **2–3 times**, with partial understanding of its services.
			Low (1pts)	The stakeholder recognizes the **name** but does not link it clearly to its activities.
			Null (0pts)	No public evidence that the stakeholder knows of Faraday's existence.
GENERAL VARIABLES	**Engagement Frequency**	Assesses how frequently Faraday interacts or collaborates with the stakeholder through direct communication , events, shared initiatives, or media exchange	Consistent (3pts)	**≥4 interactions per year** (e.g., meetings, co-projects, content collaborations) with stakeholders promoting a substantial engagement
			Ocassional (2pts)	**1–3 interactions per year**, sporadic or limited in scope
			Absent (1pts)	**No recorded interaction** in the last 12 months

<table>
<tr>
<td>GENERAL VARIABLES</td>
<td>Potential Influence</td>
<td>Measures the extent to which the stakeholders can influence one or more specific dimensions of the company (Such as Visibility, Reputation, Decision-Making, or Strategic positioning).</td>
<td>
<table>
<tr><td>High (3pts)</td><td>The stakeholder has directly and publicly influenced at least 5 cases (companies, incidents, or regulations) related to the cybersecurity sector in the past year. (E.g. major news coverage, public denunciations, or implemented policies).</td></tr>
<tr><td>Medium (2pts)</td><td>The stakeholder has had 2-4 relevant appearances or interventions on cybersecurity-related topics. (E.g. reporting, public commentary, or participation in sectoral discussions without direct impact).</td></tr>
<tr><td>Low (1pts)</td><td>The stakeholder has only one minor or indirect intervention, such as a passing mention in general news or a brief, non-specialized statement on cybersecurity.</td></tr>
<tr><td>None
(0 pts)</td><td>No recorded interventions or relevant positioning on cybersecurity or sector-related strategic issues.</td></tr>
</table>
</td>
</tr>
<tr>
<td>GOVERNMENT VARIABLES</td>
<td>Compliance with Local Cybersecurity Laws and policies</td>
<td>Measures if Faraday publicly states adherence to national cybersecurity/data protection laws and policies (eg GDPR in Germany, CISA in the U.S., Law 25.326 in Argentina)</td>
<td>
<table>
<tr><td>Full (3pts)</td><td>Faraday explicitly states compliance with the local law on its website, legal policies, or product materials and offers compliance-supporting features (e.g. data encryption, consent logging, audit trails 2-4 times every 12 months. (May include certifications or government-related partnerships)</td></tr>
<tr><td>Partial
(2pts)</td><td>Faraday makes a singular (1), minimal explicit reference to compliance with one local cybersecurity or privacy regulation (e.g., GDPR, CISA) on its website, legal page, or product materials</td></tr>
<tr><td>Null (0pts)</td><td>No mention or evidence of local cybersecurity or privacy law compliance. No observable features or statements supporting alignment.</td></tr>
</table>
</td>
</tr>
</table>

GOVERNMENT VARIABLES	**Contribution to National Talent Development**	Evaluates the organization's involvement in publicly supported education, training, or talent-building programs within the cybersecurity sector	Full (3pts): Faraday is **formally involved** in public or university-led cybersecurity education or talent programs (e.g., internships, government-sponsored training, or mentorship initiatives) 2-4 times Partial (2pts): Faraday has **a singular occasional participation (1)** in public events or education initiatives (e.g., guest talks, roundtables, workshops), but no sustained or formal collaboration. Null (0pts): Faraday shows **no public record** (mentions, press or events listing) of involvement in talent development initiatives through education or government partnerships
MEDIA VARIABLES	**Focus on Cybersecurity Issues**	Measures how much the media focuses on topics linked to the Faraday Security universe: cybersecurity, technology, data protection, digital threats, digital regulation, etc.	High (3pts): The outlet is **strongly** focused on cybersecurity and technology. It Publishes **≥21** relevant articles per year. Medium (2pts): The outlet **occasionally** covers topics relevant to Faraday. Publishes between 10 and 20 articles per year Low (1pts): The outlet mentions these topics **sporadically or marginally**. Publishes between 3 and 9 articles per year Null (0pts): The outlet **does not** publish content relevant to Faraday. Publishes 2 or fewer articles per year.
MEDIA VARIABLES	**Amount of Mentions of Cybersecurity Companies**	States the amount of mentions the media outputs about Cybersecurity companies.	High (3pts): **≥ 10** mentions of related companies per year Medium (2pts): **3-9** mentions of related companies per year Low (1pts): **<3** mentions of related companies per year, but it publishes content about cybersecurity Null (0pts): The media **does not** mention cybersecurity companies at all

<table>
<tr>
<td>COMMUNITY VARIABLES</td>
<td>Contribution for Local Awareness</td>
<td>Measures the extent to which Faraday contributes to raising public awareness of cybersecurity within local communities (events, workshops, campaigns).</td>
<td>
<table>
<tr><td>High (3pts)</td><td>Faraday organized or actively participated in ≥5 community-facing activities (e.g., talks, workshops, awareness campaigns)</td></tr>
<tr><td>Medium (2pts)</td><td>Faraday participated in 2–4 community-facing activities with moderate visibility</td></tr>
<tr><td>Low (1pts)</td><td>Faraday participated in 1 activity, limited in scope or visibility</td></tr>
<tr><td>Null (0pts)</td><td>No recorded activity linked to community awareness</td></tr>
</table>
</td>
</tr>
<tr>
<td>COMMUNITY VARIABLES</td>
<td>Inclusivity & Social Impact</td>
<td>Evaluates Faraday’s involvement in initiatives targeting underrepresented groups (e.g., youth, women, elderly, low-income populations).</td>
<td>
<table>
<tr><td>Full (3pts)</td><td>Faraday supported or assisted to ≥3 targeted inclusion programs</td></tr>
<tr><td>Partial (2pts)</td><td>Faraday supported or assisted 1–2 targeted programs</td></tr>
<tr><td>Null (0pts)</td><td>No recorded participation in these types of initiatives</td></tr>
</table>
</td>
</tr>
<tr>
<td>INTERNAL VARIABLES</td>
<td>Visibility of Contributions</td>
<td>Assesses the degree to which internal publics are publicly or semi-publicly visible in Faraday’s initiatives (e.g., staff featured in webinars, blog posts, LinkedIn activity, events).</td>
<td>
<table>
<tr><td>High (3pts)</td><td>≥4 Public/semi-public contributions (talks, posts, content, event participation)</td></tr>
<tr><td>Medium (2pts)</td><td>2–3 contributions</td></tr>
<tr><td>Low (1pt)</td><td>1 contribution</td></tr>
<tr><td>Null (0pts)</td><td>No visible contributions.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>INTERNAL VARIABLES</td>
<td>Workforce Communication Alignment</td>
<td>Analyzes how effectively internal communication fosters employees' identification with the organization, influencing their motivation to remain engaged over time.</td>
<td>
<table>
<tr><td>High (3 pts)</td><td>No turnover, visible retention of key staff in the year.</td></tr>
<tr><td>Medium (2 pts)</td><td>1–2 departures/changes in key roles.</td></tr>
<tr><td>Low (1 pt)</td><td>Noticeable turnover, multiple departures.</td></tr>
<tr><td>Null (0 pts)</td><td>Very limited retention signals.</td></tr>
</table>
</td>
</tr>
<tr>
<td>NON GOVERNMENT VARIABLES</td>
<td>Sectoral Visibility Contribution</td>
<td>Assesses the degree to which Faraday, either as a company or through its representatives, participates in industry conferences, associations, and forums, thereby strengthening its professional visibility</td>
<td>
<table>
<tr><td>High (3pts)</td><td>Active speaker/sponsor role in ≥3 events</td></tr>
<tr><td>Medium (2pts)</td><td>Active participation in 1–2 events or passive participation (attendee) in ≥3</td></tr>
<tr><td>Low (1pts)</td><td>1 event presence without visibility (just as attendee)</td></tr>
<tr><td>Null (0pts)</td><td>No participation in any event</td></tr>
</table>
</td>
</tr>
<tr>
<td>NON GOVERNMENT VARIABLES</td>
<td>Knowledge Exchange & Networking</td>
<td>Evaluates the degree of collaboration with academic, industry, or professional networks for knowledge-sharing and partnerships.</td>
<td>
<table>
<tr><td>Full (3pts)</td><td>Collaboration with ≥3 associations or institutions</td></tr>
<tr><td>Partial (2pts)</td><td>Collaborated with 1–2 institutions through workshops, papers, or projects</td></tr>
<tr><td>Null (0pts)</td><td>No collaborations recorded</td></tr>
</table>
</td>
</tr>
</table>

SWOT analysis

Strengths

- ★ Integrated Platform and Technical Differentiation: Faraday offers an all-in-one solution platform that integrates over 150 cybersecurity tools. This centralization reflects strong technological innovation, enhancing both usability and operational efficiency for clients while providing a clear competitive advantage differentiating Faraday from competitors who offer fragmented or tool-specific service.
- ★ Adaptive Global Communication Strategy: The company demonstrates a strong capacity to tailor its communication strategies to diverse cultural and linguistic contexts. It localizes messages not only through multilingual capabilities (e.g., Spanish for Latin America, English for the U.S.) but also through adjustments in tone and content—ranging from educational and approachable to technical and compliance-oriented, depending on the target audience. This enables Faraday to maintain a coherent yet flexible global messaging strategy.
- ★ Agile Internal Structure and Talent Development: Faraday fosters a collaborative, inclusive, and purpose-driven organizational culture, which is a key asset in the highly competitive and talent-scarce cybersecurity industry. High employee retention and a strong focus on internal talent development reflects the company's commitment to long-term growth. Additionally, its small team size and agile structure support efficient internal communication and rapid decision-making, contributing to innovation and operational responsiveness.
- ★ Strategic Digital Presence: Faraday maintains a targeted and professional digital presence, actively engaging with technically proficient audiences through platforms such as GitHub and curated newsletters. By contributing to open-source communities and consistently sharing sector-relevant content, the company enhances its visibility, credibility, and trust among key stakeholders, including developers, engineers, and IT security professionals. This digital strategy reinforces Faraday's positioning as a technically competent and community-oriented cybersecurity actor.
- ★ Proactive and Client-Centered Service Model: Faraday's consulting services are highly adaptable, offering both project-based and continuous support models tailored to client needs. This flexibility allows the company to serve a wide range of organizations, from startups to large enterprises, by providing scalable solutions. The emphasis on proactive vulnerability detection and personalized consulting enhances client trust and positions Faraday as a responsive and strategic partner in managing digital risk.

Weaknesses

- Operating Costs in Different Markets: The company faces elevated operating costs in strategic regions such as the United States, where labor, regulatory compliance, and technology costs are considerably higher than in Latin America. This limits pricing flexibility and may reduce competitiveness against larger firms.
- Cultural Adaptation Challenges: While Faraday adjusts its communication strategies for different markets, achieving deeper cultural integration, particularly in complex markets such as Germany or the U.S, remains a challenge: limited local presence and reduced proximity to institutional and business norms may affect relationship-building, stakeholder engagement, and market resonance.
- Environmental Concerns: Faraday is at an early stage in adopting sustainability measures and lacks a formal environmental strategy. In a business landscape that increasingly prioritizes CSR criteria, this gap may pose reputational risks and limit opportunities for collaboration with sustainability-focused partners.
- Employee Communication Gaps: While communication is effective within small teams, the absence of formalized internal communication protocols may impede organizational alignment and limit scalability, particularly as the company expands into international markets.
- Limited Brand Recognition Outside Core Markets: Brand awareness remains concentrated within its established markets. In emerging or international markets, the company lacks visibility and name recognition, which may hinder its ability to attract new clients, form strategic partnerships, and compete effectively against more established global players. This limitation could slow international expansion efforts and require significant investment in marketing, localization, and trust-building initiatives to establish credibility and market presence.

Opportunities

- ❖ Strategic Expansion into Emerging Markets: Faraday has already considered expansion in regions such as Latin America, where rising awareness of cybersecurity and less saturated market conditions present significant growth opportunities. The company's regional expertise and service adaptability offer a competitive advantage in addressing local needs.
- ❖ Sustainability-Driven Competitive Advantage: Developing a formal sustainability strategy would allow Faraday to enhance its brand reputation, align with global Environmental, Social, and Governance (ESG) expectations, and gain a competitive edge—particularly in partnerships with organizations that prioritize responsible practices.

- ❖ Strategic Partnerships and Local Alliances for International Growth: Continuing forming partnerships with local firms or institutions in highly regulated markets—such as Germany or Chile—can support smoother market entry, enhance credibility with stakeholders, and provide access to regulatory knowledge and local networks.
- ❖ Cross-Platform Digital Strategy Expansion: Leveraging more dynamic and participatory content formats—such as webinars, live Q&A sessions, or explainer videos—across platforms like YouTube, LinkedIn, or TikTok could significantly enhance audience engagement and brand visibility, particularly among younger or tech-oriented segments.
- ❖ Regulatory Alignment and Standards Collaboration: Strengthening ties with government bodies and standard-setting institutions (e.g., NIST, ENISA, IRAM) can enhance Faraday's credibility, offer early insights into regulatory trends, and position the company as a trusted partner in cybersecurity governance.

Threats

- ➢ Regulatory Changes: Within the rapidly evolving industry, cybersecurity laws differ across countries, requiring constant adaptation. This increases compliance and operational complexity, particularly in markets like the U.S. and EU with strict data and security standards.
- ➢ Data Privacy and Compliance Issues: Operating across jurisdictions with strict data laws requires rigorous compliance to avoid legal and reputational risks. Faraday must ensure its solutions remain compliant to avoid fines and reputational damage. Cross-border data handling increases the risk.
- ➢ Intense Market Competition: Faraday competes against global players as well as regional firms that may offer lower prices or niche expertise. This presents growing obstacles to both client retention and brand differentiation, making it harder to stay competitive.
- ➢ Cybersecurity Breach Risks: As a provider of cybersecurity solutions, Faraday faces reputational and operational risk in the event that its own systems are compromised by breach or failure. Such an incident could undermine stakeholder confidence, diminish client trust, and call into question the organization's credibility in delivering secure and reliable services.
- ➢ Geopolitical Instability: Operating in multiple regions exposes Faraday to geopolitical tensions, such as trade restrictions, sanctions, or diplomatic disputes. These may disrupt client access, compromise operations, or affect international partnerships—particularly in sensitive sectors like defense and government services.

Problem Statement

Despite Faraday's leading offensive security solutions and established global presence, the company lacks a unified and strategically aligned communication approach. This gap is particularly evident in its engagement with key publics, which remains inconsistent and predominantly reactive across Argentina, Germany and the United States. This prevents the company from articulating its value in an effective and proper way, ultimately limiting Faraday's awareness, growth and partnership opportunities.

Media (See Annex 12)

Diagnosis: The analysis reveals a significant disconnect between Faraday Security and its media environment. Media engagement is mostly occasional or absent, and when it happens, it's usually reactive, based on journalist-driven requests for expert input and investigations, rather than proactive outreach by the company. This limited presence contrasts with the high influence and strong thematic alignment of many outlets, especially in the U.S., where cybersecurity topics are frequently covered. Despite this favorable context, Faraday remains marginal and passive in media narratives, with few mentions as a company and no clear communication strategy in place.

- Problem statement: Faraday lacks awareness across the media of the selected countries. Despite operating in an ecosystem with high influence and strong thematic alignment, the company remains largely unrecognized and absent from the public media conversation, limiting its ability to shape perception and position itself strategically within the cybersecurity sector.

Government (See Annex 13)

Diagnosis: Faraday demonstrates strong technical alignment with national and international cybersecurity standards and regulations. However, across Argentina, the United States, and Germany, its engagement with government stakeholders, particularly executive and legislative bodies, is inconsistent and informal. While regulatory compliance is well communicated, *awareness* of Faraday's strategic capabilities remains limited among public institutions. Moreover, its contributions to national talent development are mostly informal and not institutionally recognized. This disconnect between the company's potential value and its current visibility within the public sector limits its ability to influence cybersecurity policies, secure public-sector partnerships, and position itself as a trusted actor in national cybersecurity ecosystems.

- Problem statement: Faraday lacks visibility, institutional engagement, and strategic recognition among government stakeholders. This limits its ability to influence

cybersecurity policy, secure public-sector partnerships, and position itself as a trusted actor in national cybersecurity ecosystem, *encountering a strategic opportunity to strengthen its institutional positioning*

Non - Governmental Forums and Associations (See Annex 17)

Diagnosis: Faraday has established itself as a recognized actor within Argentina's non-governmental cybersecurity ecosystem. Its ability to connect across spaces, from global stages to local institutions is seen through the participation in high-impact international and national forums, conferences, and events. This allows the company to develop reputational visibility and direct contact with both industry peers and government representatives. Also, the active connections with professional associations and academic partnerships reinforce their credibility and indicate the clear commitment to sectorial growth and industry talent development. However, its participation remains event-driven and sponsorship-heavy, without converting into broader leadership or institutionalized influence within the sector. The significantly varying engagement frequency and consistency: strong in conferences and forums, but weaker in long-term association leadership or academic collaboration, leaves the company with high awareness but low continuity.

- Problem statement: Faraday demonstrates strong visibility and credibility across non-governmental forums and associations, yet its role remains largely event-driven and overly technical, limiting its ability to transform technical credibility into sustained influence when it comes to shaping agendas, consolidating networks, and positioning itself as a long-term reference actor.

Community (See Annex 18)

Diagnosis: The analysis indicates a growing participation in community-oriented initiatives that aim to raise awareness of cybersecurity among non-professional audiences. Through collaborations and partnerships they have shown contribution to digital inclusion, youth education, and local resilience. Yet, Faraday's presence remains sporadic and concentrated around isolated campaigns or specific events. Participation largely depends on third-party initiatives rather than proactive, structured programs led by the company itself. This reduces their visibility and ability to solidly build trust and establish its positioning as a community-oriented organization.

- Problem statement: The company's community-based activities are visible but inconsistent. Although being partnered with different initiatives, their event-based role restricts its potential for long-term programs that may have the potential for sustained awareness and social impact, also leaving the company as a leading advocate for

inclusive and resilient cybersecurity culture in Argentina with influence among non-professional audiences.

Internal (See Annex 19)

Diagnosis: Faraday's internal publics present uneven levels of awareness, engagement, and visibility. Executive leadership and management stand out for their high awareness, consistent participation, and strong influence, complemented by high visibility of contributions, though retention signals are only moderate. Technical and operations teams also display high awareness and influence, with consistent engagement and strong retention, yet their visibility of contributions remains limited compared to leadership. In contrast, sales, marketing, and client relations teams operate at a medium level of awareness and engagement, with moderate visibility and retention, restricting their ability to project influence both internally and externally. Support and administrative staff occupy the lowest levels across awareness, engagement, and influence, with limited visibility despite showing medium retention. This uneven distribution of participation and recognition generates imbalances across internal groups, preventing Faraday from consolidating a cohesive and equally valued internal structure.

- Problem statement: Faraday's internal communication is marked by uneven engagement and recognition. While leadership and technical areas concentrate influence and visibility, sales, marketing, and support teams remain less visible and inconsistently engaged. This imbalance risks reducing cohesion and limits the company's capacity to fully leverage the potential capabilities of all its internal publics.

The Plan

- **Description of the campaign concept:** *"Cybersecurity Starts With Us"*

The core idea of the plan is that cybersecurity is not the just responsibility of governments, corporations, or experts. It is a collective and shared duty that begins with each individual, team, and institution. Faraday acts as the orchestrator, bringing different publics together around the belief that everyone has a role in creating a safer digital world. The plan addresses the challenge of fragmented visibility in the cybersecurity landscape and positions Faraday as the top-of-mind platform for connection and collaboration.

We offer a Global Adaptable Plan, meaning that within it, campaigns may be separated between countries: For instance, the idea is to propose a starting campaign in Argentina, it being the founding country, that may focus on community & education; whereas in the U.S, it

amay highlight innovation & compliance; and in Germany, standardization & institutional trust.

Faraday's mission is to always stay one step ahead. With *Cybersecurity Starts With Us*, we extend that mission to everyone — because being one step ahead in security begins with each of us

Global Visual Universe: The core symbol of the campaign is a digital fingerprint formed by interconnected nodes, with each node representing one public. The fingerprint symbolizes both individual responsibility and collective identity. Aligned to the company's recent rebranding, the integration of the red color is applied in all campaign materials.

Tone: Authoritative yet approachable. The communication combines technical credibility with accessible, human-centered storytelling that makes cybersecurity understandable and relevant for all publics.

- **General goal, objective and strategy**

Campaign Goal: To position Faraday as a trusted, visible, and socially responsible cybersecurity leader in Argentina by engaging all key publics under a unified message of shared responsibility for digital security.[101]

General Objective: Increase Faraday Security's overall brand recognition and stakeholder engagement by 30% in 12 months across five key publics—media, government, non-governmental entities[102], internal staff, and community—through measurable growth in visibility, participation, and sentiment indicators.

[101]The publics referred to in this section are the government, media, community, and non-governmental publics.
[102]"Non-governmental entities" refers to professional, academic, and industry actors outside the formal government structure that influence Argentina's cybersecurity ecosystem.

- *Justification: The 30% growth target is grounded in the previous global organization analysis, where results exhibit that the current brand visibility baseline portrays strong technical credibility but limited public recognition and irregular engagement across key publics. There is an evident low-to-medium awareness and participation levels, indicating significant room for improvement through coordinated communication actions. Therefore a 30% increase represents a realistic yet ambitious goal ensuring a measurable progress in positioning Faraday as a visible and trusted cybersecurity actor in Argentina.*

General strategy:

The strategy positions Faraday as the orchestrator of a collaborative cybersecurity ecosystem, built on the belief that digital security is a shared responsibility. It aims to unify diverse publics under the message "Cybersecurity Starts With Us," emphasizing inclusion, co-responsibility, and the collective impact of individual actions. The approach unfolds from the inside out: first by empowering Faraday's employees as ambassadors of its cybersecurity culture, then by strengthening alliances with governmental and non-governmental institutions, and finally by bringing cybersecurity closer to citizens through education and accessible communication. Through consistent messaging and adaptable storytelling, Faraday combines technical credibility with human-centered narratives, making cybersecurity relevant for all.

- **Specific objectives and strategies per public**

Specific objectives

Government: Increase Faraday's recognition as a trusted institutional ally in Argentina's public cybersecurity ecosystem by 25% by December 2026[103]

Media: Improve media visibility and perceived credibility within Argentina's national media by 40% by December 2026[104]

Community: Expand Faraday's public recognition as a socially responsible cybersecurity actor in Argentina by 35% by November 2026[105]

[103] The 25% growth represents an achievable shift from sporadic to consistent institutional recognition within one year, having in mind the current low governmental visibility but strong technical alignment.
[104] Considering the current minimal media presence, a 40% increase target represents an approachable yet ambitious improvement by aiming to transition from isolated and reactive appearances, to consistent and proactive media recognition
[105] Given the company's current limited involvement in community outreach, a 35% increase represents an achievable advancement in social initiatives.

Non-Governmental Actors: Strengthen Faraday's sectoral influence and visibility within Argentina's professional and academic cybersecurity ecosystem by 30% by December 2026[106]

Internal: Enhance internal engagement and employee advocacy by achieving 80% participation in internal initiatives by Q3 2026[107]

Specific Strategies

Government: *Demonstrate* alignment and co-create initiatives with governmental national cybersecurity working entities through policy engagement and technical contributions.

Media: *Produce* clear, relevant, and accessible cybersecurity contents to strengthen relationships and enhance public understanding.

Community: *Educate and translate* technical expertise into accessible resources for citizens and students through inclusive and localized initiatives

Internal: *Train and empower* employees to become active communicators and brand ambassadors of Faraday's culture and expertise

Non-Governmental: *Consolidate* Faraday's presence in the digital ecosystem through strategic collaborations and participations

- **Key Messages**

We selected *"Starts With Us"* as a behavioral anchor for all publics, that moves beyond awareness and calls for action (that being the adoption of safer practices, partnerships, participation, etc). By using the term *"Us"* we achieve the unification of all publics.

- **Government:** "Cybersecurity starts with us — together with Faraday, we seek to protect Argentina's state and industry"
- **Media:** "Cybersecurity starts with us — clear, expert voices strengthen public trust"
- **Community:** "Cybersecurity starts with us — with Faraday every family, school, and neighborhood can be safer online"
- **Non-Governmental:** "Cybersecurity starts with us — associations, universities, and companies building Argentina's digital resilience"
- **Internal:** "Cybersecurity starts with us — our people are Faraday's strongest defense"

[106] The 30% target reflects the strengthening of ongoing collaborations and visibility, bearing in mind Faraday's irregular involvement across industry and sectoral entities.
[107] Based on the current uneven internal engagement, the 80% target aims to strengthen cross-departmental communication and participation in order to consolidate a unified internal culture.

- **Tactics**

Government

1. **Institutional Partnerships:** Formalize collaborations with two national government entities, specifically the National Directorate of Cybersecurity within the Secretariat of Innovation, Science and Technology and the Ministry of Defense's Directorate of Cyber Defense to co-develop cybersecurity initiatives[108].

   This tactic establishes long-term collaboration with governmental entities. By sharing expertise, reports, and technical knowledge, Faraday positions itself as a strategic ally in developing Argentina's cybersecurity agenda. These alliances will also support the creation of institutional references that validate Faraday's contribution to the national digital ecosystem.

Tools: Strategic partnership agreement	**Techniques**: Formalize and execute collaboration agreements.
Control: Partnership progress[109] will be monitored quarterly through meeting records and follow-up reports of and attendance	

   - *KPI:* Number of agreements signed and recorded attendances
   - *Expected Success Rate:* 100% execution of two partnerships by 2026

   Activities:

   ★ Identify and shortlist potential agencies
   ★ Internal alignment meeting with Faraday leadership
   ★ Draft proposals
   ★ Schedule and hold first meetings
   ★ Send tailored collaboration proposals
   ★ Follow-up calls and negotiation rounds
   ★ Review and finalize MoUs
   ★ Internal approval of MoUs

[108] The selection relies on the strategic relevance and institutional role that both hold within Argentina's national cybersecurity framework. The Secretariat of Innovation, through the *National Directorate of Cybersecurity*, leads the implementation of the *National Cybersecurity Strategy* and promotes public–private cooperation in digital innovation and risk management. Establishing collaboration with this entity enables Faraday to contribute its technical expertise and research capabilities to policy development and capacity-building initiatives. Simultaneously, the Ministry of Defense's Directorate of Cyber Defense is responsible for safeguarding critical national infrastructure and coordinating cyber defense operations, aligning directly with Faraday's competencies in vulnerability assessment and threat mitigation. Partnering with these two institutions ensures a balanced approach that combines policy-level participation and technical contribution, positioning Faraday as a credible and collaborative actor within Argentina's cybersecurity ecosystem.

[109] Referring to the ongoing development and implementation of the collaboration that goes beyond just signing the agreement.

- ★ Signature ceremonies (Photo + Press Note)
- ★ Kick-off joint working groups
- ★ Monthly coordination meetings
- ★ Joint public announcement (LinkedIn + Government Site)
- ★ Monitor collaboration outcomes and update progress logs
- ★ Evaluate partnership effectiveness
- ★ Final partnership report

Contact List:

- Secretariat of Innovation, Science and Technology:
  - Federico Sebastián Pierri – National Cybersecurity Director
  - Pablo Mariano Navarro – Computer Systems and Network Security Prevention Director
  - Emiliano Villa – Director, National Information Technology Office
  - Maximiliano Costantinis – Director, Standards Development and Technological Opinions
  - Claudio Gustavo Wendler – Undersecretary of Innovation
  - Rita Eugenia Domínguez Alonso – Director, Digitalization and Administrative Innovation
- Directorate of Cyber Defense
  - Luis Alfonso Petri – Minister of Defense
    Alberto Luciano Mario Corvalán – Undersecretary of Cyber Defense
  - José Gustavo Oyadomari – Director of Cyber Defense Coordination
  - Ernesto Claudio Balloffet – Director of the Cyber Defense System

<u>Materialization</u>

2. **National Cybersecurity Forum**: Participate in the *Cybersecurity Conference Córdoba*[110] *2026*, a prominent public-sector–backed cybersecurity event in Argentina, organized by the Government of Córdoba, through its Ministry of Production, Science, and Technological Innovation, and supported by the Secretariat of Innovation, Science and Technology of the Nation and the National Directorate of Cybersecurity to discuss national cybersecurity challenges and policy frameworks.

   By participating in a forum that has direct engagement with policymakers and experts, Faraday gains institutional recognition and strengthens its reputation as a contributor to digital governance.

Tools: Participatory forum	**Techniques**: Participate in national forum ensuring Faraday's executives act as speakers or panelists
Control: Event attendance registration and post-event citations in public reports documenting Faraday's contributions.	

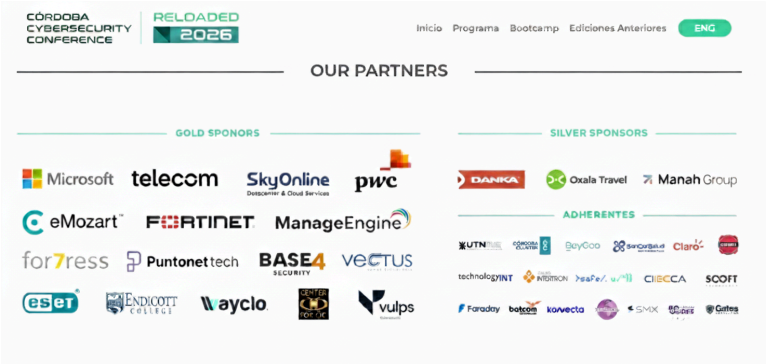
   - *KPI:* Qualitative assessment of visibility/citations in public reports
   - *Expected Success Rate:* Participation in at least two national cybersecurity forums achieving ≥ 70 % positive evaluation of Faraday's contribution.

   Activities:

   ★ Research and confirm the 2026 edition of the *Cybersecurity Conference Córdoba*.
   ★ Draft and send participation proposal to the Ministry of Production, Science, and Technological Innovation of Córdoba and to the National Directorate of Cybersecurity.
   ★ Negotiation rounds
   ★ Sign participation agreements
   ★ Design materials / Develop supporting presentation materials and institutional visuals.
   ★ Speaker training & rehearsal
   ★ Event execution
   ★ Final institutional summary

Materialization

[110] https://cordobaproduce.cba.gov.ar/21185/cordoba-fue-epicentro-de-la-ciberseguridad-con-la-cybersecurity-conference-2025/ The conference serves as a meeting point for public institutions, private companies, and academic experts to discuss national cybersecurity challenges, data protection, and digital policy frameworks.



---

3. **Advisory Reports for Policymakers:** Deliver two cybersecurity advisory reports focused on regulation and digital risk management.

   This tactic provides public institutions with evidence-based reports on cybersecurity trends and digital risks, making these publications reinforce Faraday's reputation as a knowledge-driven company and enhance visibility among decision-makers.

Tools: Technical policy advisory reports on cybersecurity regulation and digital risk management.	**Techniques**: Develop and distribute advisory reports
Control: Tracking report distribution, downloads, and online access metrics for consultation from government entities	

   - *KPI:* Number of reports published and downloads
   - *Expected Success Rate:* 2 reports with ≥ 150 total downloads.

   Activities:

   ★ Define report topics and objectives
   ★ Assign team of researchers
   ★ Research & data collection
   ★ Write Report #1
   ★ Approve Report #1
   ★ Launch Report #1
   ★ Write Report #2

★ Approve Report #2
★ Launch Report #2
★ Track metrics
★ Follow-up and evaluation
★ Final summary

Materialization

Media

1. **Expert Storytelling Campaign:** Feature Faraday's executives in leading national podcasts speaking about the cybersecurity industry (*La Cruda*[111] or *La Fábrica Podcast*[112])

   Featuring the company's leaders in these types of podcasts will enhance Faraday's recognition and humanize its expertise, providing content that makes cybersecurity understandable for wider audiences. It positions its executives as thought leaders in technology and security, reinforcing technical credibility.

Tools: Participation of Faraday executives in national podcast interviews and streaming platforms	**Techniques**: Produce a recorded program
Control: Track performance through media monitoring, audience analytics, and sentiment evaluation	

   - *KPI:* Total listeners/viewers reached, engagement rate, average video completion rate, and sentiment score in comments and media mentions.

[111] La Cruda: A Spanish-language interview podcast hosted by Migue Granados. Produced as a Spotify Original in Argentina, the show features candid conversations with diverse guests about personal trajectories, social issues and unexpected life stories. It gained strong listenership in Argentina and beyond.
[112] La Fábrica Podcast: A Spanish-language audio series produced in Argentina, which brings together voices from industry, business, politics and culture to explore topics shaping national identity and economic development. Available via Spotify

- *Expected Success Rate:* 40% increase in earned mentions and positive tone achieving an average 60% completion rate per episode.

Activities:

- ★ Identify key podcasts
- ★ Pitch Faraday executives as expert guests
- ★ Schedule interviews and prepare briefing materials
- ★ Record episode
- ★ Publish episode
- ★ Analyze performance

Materialization

---

2. **Expert Contributions in National Media:** Collaborate with journalists and editors from Argentina's leading national media—La Nación, Clarín, Infobae, Perfil, El Cronista, and Revista Mercado—to feature expert commentaries in technology and business coverage. These collaborations will include interviews, expert quotes, and authored opinion pieces on cybersecurity, resilience, and digital risk management

   The tactic seeks to position Faraday as a trusted, go-to source for credible cybersecurity information within the national media ecosystem, consequently increasing its visibility.

Tools: Co-created journalistic content with top-tier national outlets	**Techniques**: Publish expert columns or interviews
Control: Clipping reports, tone analysis, and article reach	

- *KPI:* Number of media appearances, article reach, and tone of coverage.

- *Expected Success Rate:* 4 expert mentions or contributions published across national outlets maintaining ≥ 70% positive or neutral tone.

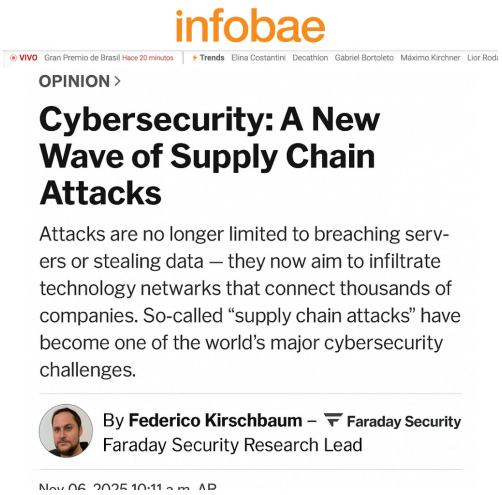
Activities:

★ Identify and contact technology and business journalists specialized in cybersecurity.
★ Propose topics to editors tied to current issues (e.g., AI threats, SME cyber-risk, data privacy).
★ Write and pitch opinion articles co-signed by Faraday experts.
★ Draft and send articles proposals
★ Approve final articles before publication
★ Publish articles
★ Monitor performance

Contact list: (Based on Annex 8)

- **Infobae**: Top online news portal in Argentina that has continuous coverage of hacking and data-privacy incidents.
    - Daniel Hadad: Director
    - Mariano Thieberger: Editor-in-Chief
    - Romina Stekar: Commercial Director
    - Gabriel Zurdo, Juan Diego Ríos, Desiree Jaimovich, and Javier Sinay: Technology & Cybersecurity Reporters
- **La Nación**: Has a wide national technology coverage with frequent cybersecurity reports and more importantly, a high public credibility.
    - Fernán Saguier: Editor-in-Chief
    - José Del Río: Executive Editor
    - Ricardo Sametband: Technology Editor
    - Ariel Torres: Tech & Digital Security Journalist
    - Débora Slotnisky: Tech & Cybersecurity
    - Victoria Menghini: AI & Cybersecurity
    - Sebastián Davidovsky: Cybersecurity & Innovation
- Revista Mercado: We will continue to prioritize this specialized newspaper in business innovation with a more suitable approach for executive-level cybersecurity insights.
    - Miguel Ángel Díaz: Director-Editor
    - Carina Martínez: Editorial Executive Secretary
    - Juan Martínez: Cybersecurity & Data Protection Reporter

Materialization


infobae

VIVO Gran Premio de Brasil Hace 20 minutos | Trends Elina Costantini Decathlon Gabriel Bortoleto Máximo Kirchner Lior Rodi

OPINION >

Cybersecurity: A New Wave of Supply Chain Attacks

Attacks are no longer limited to breaching servers or stealing data — they now aim to infiltrate technology netwarks that connect thousands of companies. So-called "supply chain attacks" have become one of the world's major cybersecurity challenges.

By **Federico Kirschbaum** – Faraday Security
Faraday Security Research Lead

Nov 06, 2025 10:11 a.m. AR

---

3. **Visual Explainer Series:** Produce and distribute short educational videos on Tik Tok addressing key cybersecurity concepts and Faraday's expertise[113]

   To make cybersecurity more relatable and expand reach beyond traditional media, this tactic simplifies complex cybersecurity-related topics, enhancing accessibility and brand recall among broader audiences.

Tools: Educational short-form videos	**Techniques**: Develop a recording program
Control: Platform analytics (views, engagement rate, video completion and retention)	

   - *KPI:* Engagement rate, impression, video completion
   - *Expected Success Rate:* 10% monthly increase in engagement across platform

   Activities:

   ★ Select cybersecurity themes for educational short videos.
   ★ Draft scripts and plan content
   ★ Record videos
   ★ Edit and design final videos
   ★ Upload
   ★ Analyze performance

[113] The specific content and video formats (e.g., excerpts from webinars, expert interviews, or case summaries) will be defined during the implementation stage according to content availability and media opportunities

Materialization:

Community

1. **“Faraday Inclusion Grants”**: Fund training initiatives promoting women and youth inclusion in tech with Chicas en Tecnología[114]. The program/s will provide financial and technical assistance to Argentine organizations already advancing digital inclusion and cybersecurity education

   By contributing to initiatives such as Chicas en Tecnología, the company enhances its social legitimacy while connecting cybersecurity with community empowerment and future employability.

Tools: Social inclusion funding program	**Techniques**: Provide annual grants for training initiatives
Control: Monitoring of progress reports from supported programs and tracking participant enrollment and completion data provided by partner organizations.	

   - *KPI:* Number of training initiatives executed and participant completion rate
   - *Expected Success Rate:* 1 program funded; average 60% course completion.

   Activities:

   ★ Identify and contact educational and social programs from Annex 15

   ★ Hold initial meetings and define grant criteria and partnership framework

   ★ Evaluate proposals and select two initiatives aligned with cybersecurity education goals.

[114] The selection relies on the recognized national trajectory of organizations working for technological inclusion. Chicas en Tecnología and its PUMM program have proven educational impact, empowering thousands of young women to join the tech sector

★ Formalize collaboration through sponsorship agreements.
★ Provide funds, mentoring sessions, and technical support to selected programs.
★ Completion and collection of progress
★ Evaluate programs effectiveness

Contact List: Chicas en Tecnología

- Vanesa Cillo: Board Member
- Lucia Mauritzen: Executive Director

Materialization:

---

2. **Digital Safety Campaign**: Launch social media storytelling and digital safety campaign using practical tips on safe digital habits

   This tactic aims to make cybersecurity part of everyday conversation and position Faraday as a responsible actor in digital safety.

Tools: Digital storytelling	**Techniques**: Social Media Campaign
Control: Monitor sentiment, impressions, and reach metrics.	

   - *KPI:* Impressions, engagement rate, positive mentions.
   - *Expected Success Rate:* Reach ≥ 200,000 users; maintain ≥ 70% positive sentiment.

   Activities:

   ★ Define campaign concept and key messages

★ Select and film 6 real testimonies
★ Create practical tip graphics + short videos
★ Build content calendar
★ Pre-campaign teaser posts
★ Official campaign launch
★ Post content
★ Monitor + final report

Materialization:

---

3. **Community Cyber-Lab:** Offer free online workshops on cybersecurity practices. The initiative will include short video modules, interactive Q&A sessions, and downloadable resources accessible through Faraday's digital platforms. Its purpose is to democratize access to cybersecurity knowledge and strengthen Faraday's role as a trusted educational voice in the community.

   By offering free online workshops on cybersecurity basics, they reinforce the educational role and contribute to building safer digital communities.

Tools: Free online workshops with interactive learning modules	**Techniques**: Offer a structured program with live Q&A and downloadable resources
Control: Monitoring online registrations, session attendance data, and participant feedback collected through post-session surveys.	

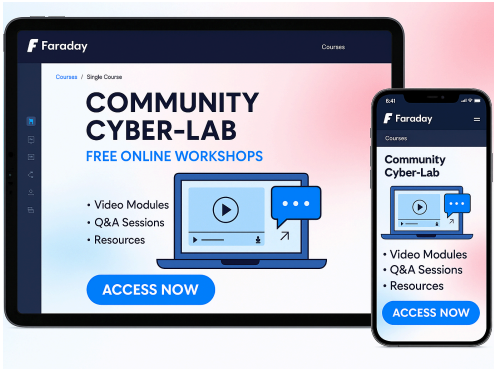
   - *KPI:* Total number of registered participants, course completion rate, and average satisfaction score.
   - *Expected Success Rate:* 1,000 participants; ≥ 70% average satisfaction.

   Activities:

   ★ Design platform page and registration form

★ Record 12 short video modules
★ Create downloadable resources
★ Build quizzes + automatic certificates
★ Run test with 50 internal users + fix bugs
★ Official public launch
★ Upload video module
★ Live Q&A sessions
★ Special October mini-hackathon
★ Monitor registrations, completion, and feedback every week + Final Report

Materialization:



Non-Governmental Actors

1. **Industry Event Sponsorship:** Sponsor[115] two major cybersecurity forums. Ekoparty 21 and 22 May 2026 in Miami, and Segurinfo)

   Through visible participation, Faraday not only showcases its expertise but also strengthens its relationships with peers, potential partners, and policy influencers, increasing institutional presence beyond the corporate sphere.

Tools: Sponsorship and active participation in national cybersecurity conferences	**Techniques**: Execute two events in where Faraday either sponsors or co-hosts panels
Control: Attendance data and brand mention analysis	

   - *KPI:* Attendance, earned media coverage, co-brand presence.
   - *Expected Success Rate:* 2 events executed, achieving 30% rise in brand mentions

   Activities:

[115] Sponsorships may provide financial or in-kind support (e.g., expert speakers, tools, content) in exchange for visibility — logo placement, mentions, and participation slots

★ Research 2026 dates, sponsorship & co-host opportunities
★ Decide role (sponsor or co-host) + get budget approval
★ Negotiate and sign contracts
★ Submit 4 speaker proposals / co-host panel requests
★ Design materials
★ Speaker training & rehearsal
★ Execute event #1
★ Execute event #2
★ Analyze metrics + Final Report

Materialization:

---

2. **Collaborative Report with Industry Partner:** Co-develop an annual cybersecurity report with a recognized professional association

   By co-authoring research reports, Faraday builds credibility and fosters alliances that expand its influence in the industry.

Tools: Joint publication of an annual report with a professional association	**Techniques**: Develop and publish report
Control: Download tracking and citation indexing	

- *KPI*: Report downloads, citations, partnership continuity.
- *Expected Success Rate*: ≥ 500 downloads and 2 industry citations

Activities:

★ Identify and shortlist 3 potential associations
★ Hold exploratory meetings + select final partner
★ Negotiate and sign collaboration agreement (MoU)

- ★ Define report topic, outline, and timeline
- ★ Joint research and data collection
- ★ Write and edit draft chapters
- ★ Design layout, cover, and infographics
- ★ Launch report
- ★ Track metrics + final report

Materialization:

---

3. **Academic Integration Program:** Create internship and research opportunities with universities

   These collaborations reinforce the company's social and educational commitment while cultivating future experts aligned with its values.

Tools: Internship and research collaboration agreements with universities.	**Techniques**: Implement partnerships with universities
Control: Enrollment and participation tracking	

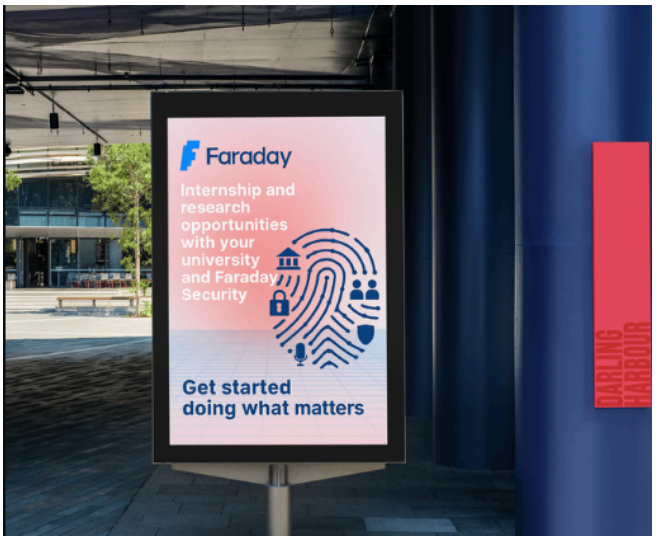
   - *KPI*: Number of institutions involved; student satisfaction rate.
   - *Expected Success Rate*: 2 universities participating; ≥ 80% positive feedback

   Activities:

   - ★ Identify and shortlist 5 target universities
   - ★ Hold exploratory meetings with deans/faculty
   - ★ Negotiate and sign collaboration agreements (2 universities)

- ★ Design internship program + research projects
- ★ Open call for applications
- ★ Selection interviews + onboarding
- ★ Internship & research period
- ★ Collect feedback surveys + final report

Materialization:



Internal

1. **Employee Advocacy Through Corporate Media**: Feature Faraday employees contributions as expert voices on the company's official digital platforms through leadership posts, short video insights, or quotes on cybersecurity trends and professional experiences[116]

   This tactic invites employees to become visible ambassadors of the company through storytelling content. By featuring internal voices on corporate channels, Faraday strengthens belonging, motivation, and pride, while projecting a unified identity aligned with its culture of collaboration and expertise.

Tools: Employee-generated content published on official digital channels	**Techniques**: Produce and publish advocacy posts authored or featuring employees
Control: Monitoring of published pieces across company-owned media, engagement analytics, and staff participation tracking.	

   - *KPI*: Number of employee-led publications and total engagement per post (likes, comments, shares)

[116] This content will follow Faraday's current communication style, emphasizing educational and approachable narratives — for example, adapting webinar extracts, employee interviews, or expert quotes as illustrated in existing corporate posts.

- *Expected Success Rate:* 10 employee advocacy posts published on Faraday's platforms

Activities:

- ★ Create advocacy guidelines + quick training video
- ★ Launch internal call for volunteers
- ★ Run 3 short training workshops
- ★ Build content calendar
- ★ Employees draft posts + short video insights
- ★ Review and approve each post/video
- ★ Publish post #1
- ★ Publish post #2
- ★ Publish post #3
- ★ Publish post #4
- ★ Publish post #5
- ★ Publish post #6
- ★ Publish post #7
- ★ Publish post #8
- ★ Publish post #9
- ★ Publish post #10
- ★ Monitor metrics + final report

Materialization:

---

2. **Internal Innovation Challenge***:* Host an annual competition for cybersecurity-related projects proposed by employees pitching innovative cybersecurity tools or outreach ideas.

This tactic boosts creativity and collaboration, aligning with the company's creativity while also strengthening belonging and promoting knowledge exchange and recognition within the company.

Tools: Annual internal competition	**Techniques**: Organize one challenge per year with evaluation panels and follow-up implementation of top ideas
Control: Track submissions, participation rate, and internal engagement metrics.	

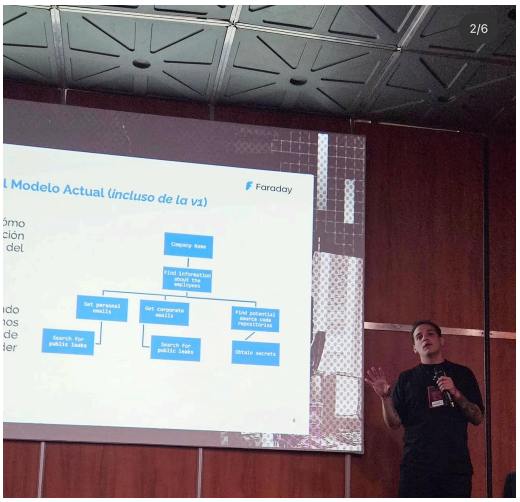
- *KPI:* Number of proposals
- *Expected Success Rate:* 10 submissions

Employee enrollment may occur on-site; however, an email invitation will be sent to remind all employees.

Activities:

- ★ Define challenge theme + rules
- ★ Design submission platform + internal materials
- ★ Official launch + Teaser campaign
- ★ Email invitation
- ★ Open call for proposals
- ★ Jury evaluation + Shortlist Top 5
- ★ Finals event – Live Pitches + Awards
- ★ Publish winner projects internally + Final Report

Materialization:



3. **“Cyber Coffee Talks” Series:** Informal monthly space for talks where employees can discuss cybersecurity topics, industry news, or internal projects in a relaxed setting. Each talk will feature a short presentation by a team member, followed by open conversation.

   This tactic promotes continuous learning and internal dialogue, aiming to strengthen cross-department communication and reinforce a culture of collaboration.

Tools: Informal discussion sessions	**Techniques**: Conduct sessions featuring brief team presentations followed by open debate
Control: Attendance and satisfaction feedback	

   - *KPI*: Number of sessions conducted, attendance rate, and satisfaction level.
   - *Expected Success Rate:* 10 sessions completed by Q3 2026, with 70% average attendance and ≥ 80% satisfaction.

   These spaces will be scheduled beforehand and added in each corporate agenda through email for employees to ensure assistance. All employees will receive the invitation.

   Activities:

   ★ Define yearly topics + create simple guidelines
   ★ Build internal sign-up form for volunteer speakers
   ★ Schedule all 10 sessions
   ★ Send monthly invitations + reminders
   ★ Session #1
   ★ Session #2
   ★ Session #3
   ★ Session #4
   ★ Session #5
   ★ Session #6
   ★ Session #7
   ★ Session #8
   ★ Session #9
   ★ Session #10
   ★ Collect quick feedback form after each talk
   ★ Final Report

Materialization:

Evaluation

The evaluation instance will determine the degree to which the general objective—*to increase Faraday's brand recognition and stakeholder engagement by 30% in 12 months*—has been achieved. In order to accomplish this, we will apply a mixed methodological approach combining quantitative and qualitative analysis.

Quantitative Analysis
To measure accomplishment of the general objective, a pre- and post-campaign Likert-scale survey will be conducted with representatives from each public (media, government, non-governmental, internal, and community)

Example:

Dimension	Statement	1	2	3	4	5
Brand Recognition	I am familiar with Faraday Security and its work in cybersecurity.	□	□	□	□	□
	I have recently seen or heard about Faraday in media or digital platforms.	□	□	□	□	□
	Faraday is visible and active in relevant industry spaces.	□	□	□	□	□
Perceived Expertise	I consider Faraday a trustworthy and professional company.	□	□	□	□	□
	Faraday demonstrates innovation and technical expertise in cybersecurity.	□	□	□	□	□
	I believe Faraday contributes valuable knowledge to the cybersecurity sector.	□	□	□	□	□
Engagement Frequency	I have interacted with Faraday's content or events during the past months.	□	□	□	□	□
	I would consider collaborating or maintaining contact with Faraday in the future.	□	□	□	□	□
	Faraday communicates in a way that encourages participation and dialogue.	□	□	□	□	□

Scale interpretation:
1 = Strongly Disagree 2 = Disagree 3 = Neut 4 = Agree 5 = Strongly Agree

- Variables: level of brand recognition, perceived expertise, and engagement frequency.
- Technique: Comparison of pre- and post-campaign averages will quantify perception growth; a minimum 30% increase will indicate fulfillment of the general objective.

To evaluate specific objectives per public, quantitative indicators will be extracted from each tactic's control system seen beforehand:

- Government: number of partnerships, reports submitted, and institutional interactions.
- Media: mentions, audience reach, and sentiment ratio.
- Non-Governmental: event participations, collaborations, and academic agreements.
- Internal: participation rate, engagement in innovation programs, and retention levels.

- Community: campaign reach, attendance at workshops, and completion of inclusion programs.

Qualitative Analysis
To complement numeric data, qualitative instruments will assess perception, message coherence, and reputation by public: - **Focus Groups**: conducted with internal and community audiences to identify attitudinal and emotional change toward Faraday's communication. - **In-depth Interviews**: applied to governmental and non-governmental partners to evaluate institutional credibility and collaborative experience. - **Media Clipping and Content Analysis**: examination of coverage tone, recurring keywords, and attributes (e.g., "trust," "expertise," "collaboration") to identify positive perception dimensions and alignment with the campaign message "Cybersecurity Starts With Us."

- **Timescale**

GANTT Chart - Faraday

- **Budget**

Budget - Faraday

Conclusion

The starting point of this project was a clear communication challenge: the company, despite its technical expertise and reputation within specialized circles, lacked a coherent communication strategy capable of translating that expertise into institutional visibility and public trust. The company's low external recognition limited its ability to influence the broader cybersecurity dialogue in Argentina and to consolidate its leadership role in a rapidly evolving sector.

The plan aims to respond to this necessity through the design of an integrated campaign, *"Cybersecurity Starts With Us,"* that positions Faraday as an orchestrator of collaboration and shared responsibility in cybersecurity. Connecting five key publics: government, non-governmental entities, media, community, and internal audiences — through

differentiated but coherent strategies that align technical authority with accessibility and inclusion.

Understanding the narratives, needs, and perceptions of each public made it possible to design actions that combine credibility with empathy — from partnerships with public institutions and media collaborations to educational and community-based programs. This process provided new insights into how organizational identity can be transformed through communication: from a provider of security services to a connector that empowers others to act securely.

Methodologically, the project integrates both strategic reasoning and measurable tools. The use of quantitative and qualitative evaluation techniques such as KPIs, Likert-scale surveys, and focus groups ensures a rigorous assessment of impact. This not only validates the proposed actions but also contributes new learning about how to operationalize brand recognition, expertise, and engagement as communication variables in the cybersecurity field.

Ultimately, this project contributes to Faraday Security's institutional growth by providing a replicable communication model that could be applied to other countries. By strengthening its reputation, deepening stakeholder relationships, and supporting the company's long-term mission: Faraday can create a Global Communication Plan to lead and connect a safer digital ecosystem. By aligning communication with organizational purpose, this plan becomes a strategic instrument that helps Faraday transform technical excellence into social relevance — ensuring that cybersecurity truly starts with all of us.

Thank you,
Micaela and Victoria

Bibliography

- ALLENDE & BREA. *Argentina Approves the Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025–2027)*. Buenos Aires: Allende & Brea, 21 January 2025 [Accessed 11 May 2025]. Available from: https://allende.com/en/privacy-and-cybersecurity/argentina-approves-the-federal-plan-for-the-prevention-of-cybercrime-and-strategic-management-of-cybersecurity-2025-2027-01-21-2025/
- ALTEA, Carlos. *Carlos Altea – iProUP*. Buenos Aires: iProUP [Accessed 30 May 2025]. Available from: https://www.iproup.com/autores/carlos-altea.
- APPUNN, K. 2024. *Primary energy use in Germany drops to new low in 2024, renewables cover 20%.* Clean Energy Wire, 18 December. [Accessed 11 May 2025]. Available from: https://www.cleanenergywire.org/news/primary-energy-use-germany-drops-new-low-2024-renewables-cover-20.
- ARD. *Speaker Marcus Bornheim. Munich: ARD, n.d.* [Accessed 31 May 2025]. Available from: https://www.ard.de/die-ard/presse-und-kontakt/speaker/Speaker-Marcus-Bornheim-100/
- ARGENTINA. 2025. *RenovAr: Renewable Energy Supply Program*. Buenos Aires: Ministry of Economy. [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/economia/energia/energia-electrica/renovables/renovar.
- ARGENTINA. *Cybersecurity. Buenos Aires: Chief of the Cabinet of Ministers, Secretariat of Innovation, Science and Technology,* [no date] [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/ciberseguridad
- ARGENTINA. *Digital Nomad Visa*. Buenos Aires: Ministry of Foreign Affairs, International Trade and Worship, 28 January 2025 [Accessed 11 May 2025]. Available from: https://ctoro.cancilleria.gob.ar/es/visa-para-n%C3%B3madas-digitales
- ARGENTINA.GOB.AR. Becas de formación en seguridad informática para agentes del Estado [online]. Buenos Aires: Secretaría de Innovación Pública, [Accessed 16 August 2025]. Available from: https://www.argentina.gob.ar/noticias/becas-de-formacion-en-seguridad-informatica-para-agentes-del-estado
- ARGENTINA. *Instituto Nacional de la Propiedad Industrial (INPI)*. Buenos Aires: Government of Argentina, 2025 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/inpi
- ARGENTINA. *Law No. 24,481: Patents of Invention and Utility Models*. Buenos Aires: Official Gazette, 23 May 1995 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-24481-27289
- ARGENTINA. *Law No. 25.326 on Personal Data Protection. Buenos Aires: National Congress of the Argentine Republic, 2000* [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
- ARGENTINA. *Law No. 26.388: Modification of the Penal Code – Incorporation of Computer Crimes*. Buenos Aires: Official Gazette, 2008 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto
- ARGENTINA. *Second National Cybersecurity Strategy Approved*. Buenos Aires: Presidency of the Nation, 5 September 2023 [Accessed 11 May 2025]. Available from: https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad
- ARGENTINA CIBERSEGURA. *Argentina Cibersegura*. [online] [Accessed 30 May 2025]. Available from: https://www.argentinacibersegura.org
- ARGENTINA CIBERSEGURA. Charlas en escuelas [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/charlas-en-escuelas. Established initiative that offers in-person and online talks for students ages 7 and up, covering topics such as: identity and digital footprint, online safety, digital violence and digital citizenship
- ARGENTINA CIBERSEGURA. *Comisión Directiva*. [online] [Accessed 27 May 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos
- ARGENTINA CIBERSEGURA. Mi Red Segura – Guillermo Brea [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/mi-red-segura/#:~:text=Guillermo%20Brea-,Guillermo%20Brea,e%20instituciones%20p%C3%BAblicas%20y%20privadas.&text=Guillermo%20Brea%20es%20uno%20de,en%20media%20docena%20de%20pa%C3%ADses.
- ARGENTINA CIBERSEGURA. Quiénes somos [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos
- Argentine Association of Informatics and Communications Users (USUARIA). *Official website of the Argentine Association of Informatics and Communications Users* [online]. [Accessed 1 June 2025]. Available from: https://www.usuaria.org.ar/.
- ARGENTINE CHAMBER OF ELECTRONIC SECURITY. *CASEL official website* [online]. [no date] [Accessed 18 April 2025]. Available from: https://casel.org.ar/

- ARRIETA, Fernando. *Crecen los intentos de ciberataques en Argentina*. Parlamentario, 2 July 2024. [Accessed 11 May 2025]. Available from: https://www.parlamentario.com/2024/07/02/crecen-los-intentos-de-ciberataques-en-argentina/
- BA-CSIRT. BA-CSIRT [online]. Buenos Aires: BA-CSIRT, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/ba-csirt/
- Black Hat. *Black Hat Official Website* [online]. [Accessed 18 April 2025]. Available from: https://www.blackhat.com/
- BORAK, Masha. *Argentina's plan to fight crime with AI draws concerns from rights groups*. Biometric Update, 2 August 2024. [Accessed 11 May 2025]. Available from: https://www.biometricupdate.com/202408/argentinas-plan-to-fight-crime-with-ai-draws-concerns-from-rights-groups
- BSides Córdoba. Official website [online]. BSides Córdoba, [Accessed 16 August 2025]. Available from: https://bsidescordoba.org/. BSides Córdoba is a community-driven cybersecurity conference held annually in Córdoba, Argentina that promotes open, inclusive, and technically rich events focused on information security.
- Bundestag. (n.d.). Friedrich Merz – Bundestag profile. Bundestag. [Accessed June 1, 2025]. Available from: https://www.bundestag.de/abgeordnete/biografien/M/merz_friedrich-1046080
- BURASTERO, Alan. Ciberseguridad awareness: concientización [online]. LinkedIn, 2025 [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/alanburastero_ciberseguridad-awareness-concientizaciaejn-activity-7334252196475072513-qtFQ
- CALIFORNIA. *California Consumer Privacy Act of 2018*. Sacramento: California State Legislature, 2018 [Accessed 11 May 2025]. Available from: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
- CAMBRIDGE DICTIONARY. *Meaning of business-to-business in English* [online]. [no date] [Accessed 18 April 2025]. Available from: https://dictionary.cambridge.org/us/dictionary/english/business-to-business
- CANAL AR. *Darío Drucaroff – Opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=3.
- CANAL AR. *Federico Tandeter – Columnas de opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=1374.
- CANAL AR. *Matías Nahón – Opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=1229.
- CASTILLO, Gonzalo; JAMELE, Agustín. *Cybersecurity in Argentina: Current Situation, Laws, and Crimes*. Buenos Aires: InnovaciónDigital360, 19 February 2025 [Accessed 11 May 2025]. Available from: https://www.innovaciondigital360.com/cyber-security/ciberseguridad-en-argentina-actualidad-leyes-y-delitos/
- CENTRAL OFFICE FOR INFORMATION TECHNOLOGY IN THE SECURITY SECTOR (ZITiS). *Leadership* [online]. Munich: ZITiS. [Accessed 1 June 2025]. Available from: https://www.zitis.bund.de/DE/WerWirSind/werwirsind_node.html#leitung
- CHICAS EN TECNOLOGÍA. Chicas en Tecnología [online]. Buenos Aires: Chicas en Tecnología, [Accessed 16 August 2025]. Available from: https://chicasentecnologia.org/. Nonprofit organization that seeks to reduce the gender gap in the technology sector. It is dedicated to motivating, training, and supporting young women to engage in technology careers and ventures, providing free programs and resources to develop their digital skills and encourage their participation in the sector.
- CHICAS EN TECNOLOGÍA. Chicas en Tecnología [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/chicasentecnologia/
- CIBERSEGURIDAD LATAM. ¡Hola a todos! Queremos invitarlos a participar... [online]. LinkedIn, 2025 [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/ciberseguridadlatam_hola-a-todos-queremos-invitarlos-a-participar-activity-7361424893252370433-3sWH
- CILLO, Vanesa. LinkedIn profile [online]. LinkedIn, [Accessed 18 August 2025]. Available from: https://www.linkedin.com/in/vanesacillo/
- CISCO. What Is SIEM? - *Security Information and Event Management*. San Jose: Cisco Systems, 2025. [Accessed 11 May 2025]. Available from: https://www.cisco.com/c/en/us/products/security/what-is-siem.html
- CLARÍN. *Ricardo Roa - Clarín*. [online] [Accessed 20 May 2025]. Available from: https://www.clarin.com/autor/ricardo-roa.html.
- CONNECTWISE. *Cybersecurity Laws & Regulations*. Tampa, FL: ConnectWise, 2024 [Accessed 11 May 2025]. Available from: https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation
- CYBERCIRUJAS CLUB. Cybercirujas [online]. Buenos Aires: Cybercirujas Club, [Accessed 16 August 2025]. Available from: https://linktr.ee/cybercirujas. A grassroots movement that refurbishes discarded tech and promotes digital inclusion in underserved communities across Argentina. They host repair workshops, donation campaigns, and digital self-defense talks, often using free software and recycled devices.
- CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). *Leadership.* Washington, D.C.: CISA, 2025 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/about/leadership

- CYBERSUMMIT. Ciberseguridad Industrial [online]. Linkedin, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/thecybersummit_ciberseguridadindustrial-thepremierconference-activity-7336394329323716608-VKsX
- CYBERSUMMIT. CyberSummit [online]. Buenos Aires: CyberSummit, [Accessed 16 August 2025]. Available from: https://cybersummit.io/
- DEF CON COMMUNICATIONS. *DEF CON Hacking Conference*. [n.d.] [Accessed 1 June 2025]. Available from: https://defcon.org/.
- DELOITTE. *Embedding security into DevOps pipelines* [online]. Deloitte Insights, 2019 [Accessed 14 June 2025]. Available from: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html
- DEUTSCHLANDRADIO. *Presseteam*. Cologne: Deutschlandradio, n.d. [Accessed 30 May 2025]. Available from: https://www.deutschlandradio.de/presseteam-100.html
- DI IORIO, Ana. *Ana Di Iorio – Info-Lab*. Buenos Aires: Info-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/prensa/novedades/181-entrevista-a-ana-di-iorio-
- DISAVINO, S. 2024. *US power use forecast to reach record highs in 2024 and 2025, EIA says*. Reuters, 10 September. [Accessed 11 May 2025]. Available from: https://www.reuters.com/business/energy/us-power-use-forecast-reach-record-highs-2024-2025-eia-says-2024-09-10/
- Disobey. About – Organising hacker culture events since 2015 [online]. Disobey, [Accessed 18 August 2025]. Available from: https://disobey.fi/2026/about A major cybersecurity and hacker culture event held annually in Helsinki, Finland at Kaapelitehdas. The event brings together a vibrant community of cybersecurity professionals, ethical hackers, researchers, and enthusiasts.
- DLA PIPER. *Data protection laws in Germany* [online]. 2025 [Accessed 11 May 2025]. Available from: https://www.dlapiperdataprotection.com/?t=law&c=DE
- DLA PIPER. *Data Protection Laws of the World – Argentina*. [s.l.]: DLA Piper, [n.d.] [Accessed 11 May 2025]. Available from: https://www.dlapiperdataprotection.com/index.html?c=AR&t=law
- EKOPARTY. *Official website of Ekoparty* [online]. [Accessed 1 June 2025]. Available from: https://ekoparty.org/.
- Ekoparty Security Conference. *Ekoparty* [online]. [Accessed 18 April 2025]. Available from: https://ekoparty.org/
- EL CRONISTA. *Christian Findling – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/christian-findling/.
- EL CRONISTA. *Florencia Pulla – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/florencia-pulla/
- EL CRONISTA. *Hernan de Goni – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/hdegoni/.
- EL CRONISTA. *Horacio Riggi – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/hriggi/.
- EL CRONISTA. *Juana Posbeyikian – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/juana-posbeyikian/.
- EL CRONISTA. *Walter Brown – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/wbrown/.
- EUROPEAN COMMISSION. *Federal Office for Information Security (BSI)*. Brussels: European Commission, 2025 [Accessed 11 May 2025]. Available from: https://digital-skills-jobs.europa.eu/en/organisations/federal-office-information-security-bsi
- EUROPEAN PATENT ORGANISATION. *European Patent Convention (EPC)* [online]. Munich: European Patent Office, 2020 [Accessed 11 May 2025]. Available from: https://www.epo.org/en/legal/epc/2020/convention.html
- EUROPEAN UNION. *Data Protection under the General Data Protection Regulation (GDPR)*. Brussels: European Union, 2025. Available at: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
- EUROPEAN UNION. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Luxembourg: Publications Office of the European Union, 2022 [Accessed 11 May 2025]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- EUROPEAN UNION. *NIS2 Directive: New rules on cybersecurity of network and information systems*. Brussels: European Commission, 2025 [Accessed 15 May 2025]. Available from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *Who We Are* [online]. Athens: European Union Agency for Cybersecurity. [Accessed 1 June 2025]. Available from: https://www.enisa.europa.eu/about-enisa/who-we-are

- Evento PUMM [online]. Buenos Aires: Chicas en Tecnología, [Accessed 16 August 2025]. Available from: https://chicasentecnologia.org/eventopumm/
- EWING, Greg; JODKA, Sara H. *But really, what cybersecurity requirements and standards does my company need to follow and why?* Reuters, 31 July 2024 [Accessed 11 May 2025]. Available from: https://www.reuters.com/legal/legalindustry/really-what-cybersecurity-requirements-standards-does-my-company-need-follow-why-2024-07-31/
- Facultad de Ciencia y Tecnología – UADER. El LASI y la Municipalidad de Paraná organizan el Hacking Day 2025 [online]. FCyT UADER, [Accessed 16 August 2025]. Available from: https://fcyt.uader.edu.ar/el-lasi-y-la-municipalidad-de-parana-organizan-el-hacking-day-2025/
- FARADAY. *Federico Kirschbaum at the Santiago Chamber of Commerce: key insights on cybersecurity* [online]. Faraday, 21 April 2025 [Accessed 12 May 2025]. Available from: https://faradaysec.com/federico-kirschbaum-at-the-santiago-chamber-of-commerce/
- FARADAY. *Good practices in cybersecurity – Part 3: Groundhog Day security*. [online]. 29 May 2024 [Accessed 15 April 2025]. Available from: https://faradaysec.com/good-practices-in-cybersecurity-part-3/
- FARADAY. *Official website* [online]. [no date] [Accessed 27 March 2025]. Available from: https://faradaysec.com/
- FARADAY. *Pricing* [online]. [no date] [Accessed 10 April 2025]. Available from: https://faradaysec.com/pricing/
- FARADAY SECURITY. BizzTech Retail Ciberseguridad [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/feed/update/urn:li:activity:7361417337725419520/
- FARADAY SECURITY. BlackHat & Car Hacking at DEFCON [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_blackhat-carhacking-defcon-activity-7360770644894007296-y8kJ
- FARADAY SECURITY. CEO Federico Kirschbaum in Uruguay [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_last-week-our-ceo-and-cofounder-federico-activity-7298341543705210881-4DV6
- FARADAY SECURITY. Estuvimos presentes en el Encuentro Empresarial de Ciberseguridad [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_estuvimos-presentes-en-el-encuentro-empresarial-activity-7332789865647910914-LO1v
- FARADAY SECURITY. H2H [online]. Linkedin, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_h2h-activity-7274431098703540227-5zIK. H2H is a Brazilian information security conference organized by individuals actively involved in information security research and development. It's a platform for sharing knowledge about information security through training and lectures presented by researchers and experts from the corporate, research, and underground communities.
- FARADAY SECURITY. Hablar de seguridad todo el día en el Encuentro Empresarial [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_hablar-de-seguridad-todo-el-d%C3%ADa-en-el-activity-7338925852644040706-4A0L
- FARADAY SECURITY. Our COO Martín D. Tartarelli is also a professor at Universidad Austral [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_our-coo-martin-d-tartarelli-is-also-activity-7275166591883902978-3hHX
- FARADAY SECURITY. Participamos del evento Ekoparty Hack the Signal [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_participamos-del-evento-ekoparty-hack-the-activity-7345871519589236737-k8l7
- FARADAY SECURITY. Participamos en BSides Córdoba [online]. LinkedIn, [Accessed 18 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_bsidescaejrdoba-bsidescaejrdoba-activity-7337914544368893952-AWOK[2](https://www.linkedin.com/embeds/publishingEmbed.html?articleId=7079208955850672993)
- FARADAY SECURITY. Se viene agosto en Faraday: desde conferencias hasta capacitaciones [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_se-viene-agosto-en-faraday-desde-conferencias-activity-7355987264188887041-MRCY
- FEDERAL AGENCY FOR INNOVATION IN CYBERSECURITY (Cyberagentur). *About Us* [online]. Halle (Saale): Federal Agency for Innovation in Cybersecurity. [Accessed 1 June 2025]. Available from: https://www.cyberagentur.de/agentur/ueber-uns/
- FEDERAL CHANCELLERY OF GERMANY. *Federal Chancellors since 1949*. Berlin: Press and Information Office of the Federal Government. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bundeskanzler.de/bk-en/chancellery/federal-chancellors-since-1949

- FEDERAL COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION (BFDI). *Organizational Structure* [online]. Bonn: Federal Commissioner for Data Protection and Freedom of Information. [Accessed 1 June 2025]. Available from: https://www.bfdi.bund.de/DE/BfDI/UeberUns/Organisation/organisation-node.html
- Federal Council for Transparency (CFT). *Portal of the Federal Council for Transparency* [online]. [Accessed 1 June 2025]. Available from: https://portalconsejofederal.transparencia.gob.ar/
- FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA). *Official website of FEMA* [online]. [Accessed 19 May 2025]. Available from: https://www.fema.gov/
- FEDERAL FOREIGN OFFICE. *Leadership*. Berlin: Federal Foreign Office. [Accessed 1 June 2025]. Available from: https://www.auswaertiges-amt.de/en/about-us/leadership-federal-foreign-office
- FEDERAL GOVERNMENT OF GERMANY. *The Energy Efficiency Act: the public sector is set to become a role model*. Berlin: Federal Government of Germany, 2022. [Accessed 11 May 2025]. Available from: https://www.bundesregierung.de/breg-de/service/archiv/the-energy-efficiency-act-2184958
- FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION (BMWK). *Federal Ministry for Economic Affairs and Climate Action*. Berlin: Federal Ministry for Economic Affairs and Climate Action. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmwk.de/Navigation/DE/Home/home.html
- FEDERAL MINISTRY FOR EDUCATION, FAMILY AFFAIRS, SENIOR CITIZENS, WOMEN AND YOUTH (BMFSFJ). *Leadership* [online]. Berlin: Federal Ministry for Education, Family Affairs, Senior Citizens, Women and Youth. [Accessed 1 June 2025]. Available from: https://www.bmfsfj.de/bmfsfj/ministerium.
- FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION, NUCLEAR SAFETY AND CONSUMER PROTECTION (BMUV). *Leadership* [online]. Berlin: BMUV. [Accessed 1 June 2025]. Available from: https://www.bmuv.de/ministerium/hausleitung.
- FEDERAL MINISTRY OF DEFENCE (BMVg). *Federal Ministry of Defence*. Berlin: Federal Ministry of Defence. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmvg.de/de/ministerium
- FEDERAL MINISTRY OF EDUCATION AND RESEARCH (BMBF). *Leadership*. Berlin: Federal Ministry of Education and Research. [Accessed 1 June 2025]. Available from: https://www.bmbf.de/DE/Ministerium/Hausleitung/hausleitung_node.html
- FEDERAL MINISTRY OF JUSTICE AND CONSUMER PROTECTION (BMJV). *Leadership*. Berlin: Federal Ministry of Justice and Consumer Protection. [Accessed 1 June 2025]. Available from: https://www.bmj.de/DE/ministerium/hausleitung/hausleitung_node.html
- FEDERAL MINISTRY OF LABOUR AND SOCIAL AFFAIRS (BMAS). *Minister and Senior Officials* [online]. Berlin: Federal Ministry of Labour and Social Affairs. [Accessed 1 June 2025]. Available from: https://www.bmas.de/DE/Ministerium/Ministerin-und-Hausleitung/ministerin-und-hausleitung.html
- FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY (BMI). *Leadership. Berlin: Federal Ministry of the Interior and Community.* [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmi.bund.de/DE/ministerium/leitung/leitung-node.html
- FEDERAL OFFICE FOR ECONOMIC AFFAIRS AND EXPORT CONTROL (BAFA). *Organizational Structure* [online]. Eschborn: Federal Office for Economic Affairs and Export Control. [Accessed 1 June 2025]. Available from: https://www.bafa.de/DE/Bundesamt/Organisation/Aufbau/aufbau_node.html
- FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). *German IT Security Congress – 30 Years BSI* [online]. Bonn: Federal Office for Information Security. [Accessed 1 June 2025]. Available from: https://www.bsi.bund.de/EN/Service-Navi/Veranstaltungen/Deutscher-IT-Sicherheitskongress-30-Jahre-BSI/deutscher-it-sicherheitskongress-30-jahre-bsi_node.html
- FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). *Leadership* [online]. Bonn: Federal Office for Information Security. [Accessed 1 June 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/Leitung/leitung_node.html
- FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). *The Alliance for Cyber Security. Bonn: BSI, 2025.* [Accessed 11 May 2025]. Available from: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/ACS/acs_node.html
- FEDERAL OFFICE OF CIVIL PROTECTION AND DISASTER ASSISTANCE (BBK). *Leadership* [online]. Bonn: Federal Office of Civil Protection and Disaster Assistance. [Accessed 1 June 2025]. Available from: https://www.bbk.bund.de/DE/Das-BBK/Das-BBK-stellt-sich-vor/Leitung/leitung_node.html
- FEDERAL TRADE COMMISSION (FTC). *About the FTC*. [n.d.] [Accessed 1 June 2025]. Available from: https://www.ftc.gov/about-ftc
- FEDERAL TRADE COMMISSION (FTC). *FTC en Español* [online]. Washington, D.C.: FTC, 2025 [Accessed 11 May 2025]. Available from: https://www.ftc.gov/es
- Federico Pacheco | LinkedIn. [online]. Available at: https://www.federicopacheco.com [Accessed 18 May2025].
- Forbes Argentina. *Seguridad informática: de una necesidad básica a una cultura organizacional* [online]. 13 December 2021 [Accessed 18 April 2025]. Available from: https://www.forbesargentina.com/innovacion/seguridad-informatica-una-necesidad-basica-una-cultura-organizacional-n10833
- FORBES BURTON. *Market development: Unlocking growth through new market opportunities* [online]. Forbes Burton, 2023 [Accessed 13 June 2025]. Available from:

https://www.forbesburton.com/insights/market-development-unlocking-growth-through-new-market-opportunities
- FOURRAGE, Ludo. *Germany Cybersecurity Job Market: Trends and Growth Areas for 2024*. Nucamp, Seattle, 2024. [Accessed 11 May 2025]. Available from: https://www.nucamp.co/blog/coding-bootcamp-germany-deu-germany-cybersecurity-job-market-trends-and-growth-areas-for-2024
- FRANCE 24. *Germany's Economy Ahead of the Elections: Europe's Locomotive Running at Half Speed*. Paris: France 24, 22 February 2025 [Accessed 11 May 2025]. Available from: https://www.france24.com/es/programas/econom%C3%ADa/20250222-la-econom%C3%ADa-alemana-ante-las-elecciones-la-locomotora-europea-opera-a-media-marcha
- FRAUNHOFER INSTITUTE FOR SOLAR ENERGY SYSTEMS ISE. 2025. *Public Electricity Generation 2024: Renewable Energies Cover More Than 60 Percent of German Electricity Consumption for the First Time*. Freiburg: Fraunhofer ISE. [Accessed 11 May 2025]. Available from: https://www.ise.fraunhofer.de/en/press-media/press-releases/2025/public-electricity-generation-2024-renewable-energies-cover-more-than-60-percent-of-german-electricity-consumption-for-the-first-time.html
- FUNDACIÓN SADOSKY. Fundación Sadosky [online]. Buenos Aires: Fundación Sadosky, [Accessed 16 August 2025]. Available from: https://fundacionsadosky.org.ar/. A public-private foundation that promotes science and technology education in Argentina. Through its Cybersecurity Program, it offers webinars, school outreach, and training for public sector employees. It also collaborates with universities and government agencies to strengthen cybersecurity capabilities.
- GARCIA, Marcos. *Secure Podcast*. [online] [Accessed 18 May 2025]. Available from: https://securepodcast.com
- GENERAL DATA PROTECTION REGULATION (GDPR). *Subject-matter and objectives*. [online]. 2025 [Accessed 25 May 2025]. Available from: https://gdpr-info.eu/art-1-gdpr/.
- GERMAN BUNDESRAT. *President and Presidium*. Berlin: German Bundesrat. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bundesrat.de/DE/bundesrat/praesidium/praesidium-node.html
- GERMAN BUNDESTAG. *Wolfgang Schäuble elected new President of the Bundestag*. Berlin: German Bundestag, 24 October 2017 [Accessed 1 June 2025]. Available from: https://www.bundestag.de/en/documents/textarchive/constituent-sitting-529998
- GERMAN INSTITUTE FOR STANDARDIZATION (DIN). *Executive Board* [online]. Berlin: DIN. [Accessed 1 June 2025]. Available from: https://www.din.de/en/din-and-our-partners/din-e-v/organization/executive-board
- GERMAN PATENT AND TRADE MARK OFFICE (DPMA). *About Us* [online]. Munich: DPMA, 3 April 2025 [Accessed 11 May 2025]. Available from: https://www.dpma.de/english/our_office/about_us/index.html
- GERMANY. *Cyber Security Strategy for Germany.* Bonn: Federal Office for Information Security (BSI), 2016 [Accessed 11 May 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Strategie/strategie_node.html
- GERMANY. *Employed Persons Working from Home*. Wiesbaden: Federal Statistical Office of Germany, 2025 [Accessed 11 May 2025]. Available from: https://www.destatis.de/EN/Themes/Labour/Labour-Market/Quality-Employment/Dimension3/3_11_homeoffice.html
- GERMANY. *IT Security Act (IT-Sicherheitsgesetz)*. Bonn: Federal Ministry of the Interior, Building and Community, 2015 [Accessed 11 May 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig.html
- GERMANY. *Telemedia Act* (TMA) [online]. Berlin: Federal Ministry of Justice, 26 February 2007 [Accessed 11 May 2025]. Available from: https://www.hunton.com/privacy-and-information-security-law/assets/htmldocuments/uploads/sites/18/2016/02/Telemedia_Act__TMA_.pdf
- GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. ¿Quiénes somos y qué hacemos? [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/jefaturadegabinete/centro-de-ciberseguridad/quienes-somos-y-que-hacemos
- GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. Cybercity: V Jornada de Ciberseguridad Ciudadana [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, 30 April 2025 [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/noticias/cybercity-v-jornada-de-ciberseguridad-ciudadana
- GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. La Ciudad ofrece charlas gratuitas de ciberseguridad en las comunas para prevenir engaños [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, 1 March 2024 [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/noticias/la-ciudad-ofrece-charlas-gratuitas-de-ciberseguridad-en-las-comunas-para-prevenir-enganos
- GOLEM.DE GMBH. *Impressum*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.golem.de/sonstiges/impressum.html
- GONZÁLEZ, Paloma. *USA: Increased Investments in Cybersecurity Amid Rising Data Breaches*. Buenos Aires: Asociación Argentina de Compañías de Seguros (AACS), 5 September 2024 [Accessed 11 May 2025]. Available from:

https://novedades.aacs.org.ar/eeuu-intensifican-inversiones-en-ciberseguridad-ante-el-aumento-de-las-filtraciones-de-datos/
- GRUPO CLARÍN. *Management*. [online] [Accessed 20 May 2025]. Available from: https://ir.grupoclarin.com/management/.
- GRUPO CLARÍN. *Virginia Messi - Clarín*. [online]. [Accessed 20 May 2025]. Available from: https://www.clarin.com/autor/virginia-messi.html.
- Hack El Valle. Hack El Valle official website [online]. [Accessed 16 August 2025]. Available from: https://hackelvalle.org/
- HASSO PLATTNER INSTITUTE (HPI). *Potsdam Cybersecurity Conference 2025 – Registration* [online]. Potsdam: Hasso Plattner Institute. [Accessed 1 June 2025]. Available from: https://hpi.de/en/registration/2025/potsdam-cybersecurity-conference/.
- HEISE GRUPPE. *Dr. Volker Zota wird Chefredakteur von heise online*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.heisegroup.de/presse/Personalien-Heise-Medien-6522370.html#:~:text=Dr,Leitmedium%20ausbauen.
- HEISE GRUPPE. *Über uns.* [n.d.] [Accessed 30 May 2025]. Available from: https://www.heisegroup.de/ueber-uns.html#:~:text=match%20at%20L259%20Karsten%20Marquardsen%2C,Verlag%20Dumrath%20%26%20Fassnacht%20übernommen.
- Honorable Cámara de Diputados de la Nación Argentina. *Comisión de Ciencia, Tecnología e Innovación Productiva* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/ccytecnologia
- HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA. *Comisión de Defensa del Consumidor, del Usuario y de la Competencia* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/cdconsumidor
- HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA. *Comisión de Defensa Nacional* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/cdnacional
- Honorable Cámara de Diputados de la Nación Argentina. *Comisiones Permanentes* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/
- Honorable Senado de la Nación Argentina. *Comisión de Ciencia y Tecnología* [online]. [Accessed 20 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/info/68
- Honorable Senado de la Nación Argentina. *Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión* [online]. [Accessed 17 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/info/74
- Honorable Senado de la Nación Argentina. *Comisiones* [online]. [Accessed 17 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/?lista=comision
- IBM. *What is Endpoint Detection and Response (EDR)?*. IBM, 2025. [Accessed 11 May 2025]. Available from: https://www.ibm.com/es-es/topics/edr
- IBM. *What is vulnerability management?* [online]. August 24, 2022 [Accessed 3 April 2025]. Available from: https://www.ibm.com/think/topics/vulnerability-management
- IDG COMMUNICATIONS MEDIA AG. *Impressum*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.computerwoche.de/impressum
- INFOBAE. Argentina. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com.
- INFOBAE. *Daniel Hadad*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/daniel-hadad/.
- INFOBAE. *Desiree Jaimovich – Infobae*. [online]. [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/desiree-jaimovich/
- INFOBAE. *Gabriel Zurdo – ataque informático*. Buenos Aires: Infobae, 11 June 2023 [Accessed 30 May 2025]. Available from: https://www.infobae.com/economia/2023/06/11/al-cabo-de-4-dias-la-comision-nacional-de-valores-logro-aislar-y-controlar-un-ataque-informatico-y-manana-lo-denunciara-a-la-justicia/.
- INFOBAE. *Javier Sinay*. Buenos Aires: Infobae, 29 December 2021 [Accessed 30 May 2025]. Available from: https://www.infobae.com/america/soluciones/2021/12/29/desconectarse-es-una-de-las-formas-de-evitar-ciberestafas-en-ano-nuevo-y-vacaciones/.
- INFOBAE. *Juan Diego Ríos*. Buenos Aires: Infobae, n.d. [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/juan-diego-r%C3%ADos/
- INFOBAE. *Mariano Thieberger*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/mariano-thieberger/.
- INFOBAE. *Romina Stekar*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/economia/networking/2021/05/06/el-interactive-advertising-bureau-de-argentina-renovo-autoridades-de-su-consejo-directivo/.
- INFO-CYBER. *Cybersecurity and Digital Forensics Journal.* Buenos Aires: InFo-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/revista-info-cyber.

- INFO-LAB. *Informe de Gestión 2024*. Buenos Aires: Info-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/images/2022/Papers/2024/Informe_de_Gestion_2024.pdf
- Instagram. (n.d.). Eduardo Aliverti – Instagram profile. Instagram. [Accessed 18 May 2025]. Available from: https://www.instagram.com/eduardoalivertiok/?hl=es
- Instagram. (n.d.). Federico Wiemeyer – Instagram profile. Instagram. [Accessed 30 May 2025]. Available from: https://www.instagram.com/wiemeyer/?hl=es
- Instagram. (n.d.). Julio Lopez – Instagram profile. Instagram. [Accessed 18 May 2025]. Available from: https://www.instagram.com/julitolopez/?hl=es
- Instituto Argentino de Normalización y Certificación (IRAM). *Official website of the Argentine Institute of Standardization and Certification* [online]. [Accessed 1 June 2025]. Available from: https://www.iram.org.ar/
- INTER-AMERICAN DEVELOPMENT BANK. *Cybersecurity for Critical Information Infrastructure Program (AR-L1343)*. Washington, D.C.: IDB, 2023. [Accessed 11 May 2025]. Available from: https://www.iadb.org/en/project/AR-L1343
- International Energy Agency. 2024. *CO_2 Emissions in 2023*. Paris: IEA. [Accessed 11 May 2025]. Available from: https://iea.blob.core.windows.net/assets/33e2badc-b839-4c18-84ce-f6387b3c008f/CO2Emissionsin2023.pdf
- INTERNATIONAL ENERGY AGENCY. 2025. *Argentina – Energy Profile*. Paris: International Energy Agency. [Accessed 11 May 2025]. Available from: https://www.iea.org/countries/argentina.
- INVESTOPEDIA. *Remote Work Is Here to Stay, New Data Shows*. New York: Dotdash Meredith, 2024 [Accessed 11 May 2025]. Available from: https://www.investopedia.com/remote-work-is-here-to-stay-new-data-shows-8671287
- ISOC Argentina. Internet Society – Argentina Chapter official website [online]. ISOC Argentina, [Accessed 19 August 2025]. Available from: https://isoc.org.ar/. Is a nonprofit organization that promotes the open development, evolution, and use of the Internet for the benefit of all people throughout the world.
- Jefatura de Gabinete de Ministros. *Mapa del Estado* [online]. [Accessed 18 May 2025]. Available from: https://mapadelestado.jefatura.gob.ar/
- JOHNSON, L. 2025. *Trump pauses renewable projects leasing on federal lands, waters*. ESG Dive, 29 January. [Accessed 11 May 2025]. Available from: https://www.esgdive.com/news/trump-pauses-renewable-projects-leasing-on-federal-lands-waters-interior-executive-order/738647/.
- K, Anjali. *Cybersecurity Services Cost in the USA: What to Expect in 2024*. LinkedIn, 12 September 2024 [Accessed 11 May 2025]. Available from: https://www.linkedin.com/pulse/cybersecurity-services-cost-usa-anjali-k-iriuf/
- KEEFER, Philip; ROSETH, Benjamin; SANTAMARIA, Julieth. G*eneral Skills Training for Public Employees: Experimental Evidence on Cybersecurity Training in Argentina*. Washington, D.C.: Inter-American Development Bank, 2024. (IDB Working Paper Series; No. IDB-WP-1643) [Accessed 11 May 2025]. Available from: https://doi.org/10.18235/0013202
- KUMAR, Vineet. *Making "Freemium" work* [online]. Harvard Business Review, May 2014 [Accessed 11 May 2025]. Available from: https://hbr.org/2014/05/making-freemium-work
- LA NACIÓN. *Fernán Saguier es nuevo director de LA NACIÓN* [online]. [Accessed 24 May 2025]. Available from: https://www.lanacion.com.ar/sociedad/fernan-saguier-es-nuevo-director-la-nacion-nid2513760/
- LA NACIÓN. *Ricardo Sametband - LA NACIÓN* [online]. [Accessed 20 May 2025]. Available from: https://www.lanacion.com.ar/autor/ricardo-sametband
- LA NACIÓN. *Victoria Menghini - LA NACIÓN*. [online] [Accessed 20 May 2025]. Available from: https://www.lanacion.com.ar/autor/victoria-menghini/.
- LEGAL INFORMATION INSTITUTE (LII). *Berne Convention* [online]. Ithaca, NY: Cornell Law School, 2021 [Accessed 11 May 2025]. Available from: https://www.law.cornell.edu/wex/berne_convention
- LINARES, Gustavo. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/gustavo-linares-705713b/?originalSubdomain=ar
- LinkedIn. (2025). Esteban Bruno – LinkedIn profile. LinkedIn. [Accessed 25 May 2025]. Available from: https://www.linkedin.com/in/esteban-bruno-722018115/
- LinkedIn. (2025). Federico K – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/fedek/?originalSubdomain=ar.
- LinkedIn. (2025). Gustavo Marcelo Moccia – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lic-gustavo-marcelo-moccia-89769a132/
- LinkedIn. (2025). Joshua Mador – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/joshuamador/
- LinkedIn. (2025). Martín D. Tartarelli – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://ar.linkedin.com/in/tartamar
- LinkedIn. (2025). Red Link S.A. – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/company/red-link-s-a-/?originalSubdomain=ar.
- LinkedIn. (2025). Santiago Fernández Boccacci – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/santiago-fernandez-boccacci-16522854/?originalSubdomain=ar.
- LinkedIn. (n.d.). Adrian Godoy – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/adrian-godoy-b4b7a1120/

- LinkedIn. (n.d.). Agustín Baranowski – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/agustinbaranowski/
- LinkedIn. (n.d.). Alejandro Schiavi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/alejandroschiavi/
- LinkedIn. (n.d.). Alex Fitzsimmons – LinkedIn profile. LinkedIn. [Accessed 29 May 2025]. Available from: https://www.linkedin.com/in/alexfitzsimmons/
- LinkedIn. (n.d.). Alex Mena – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/alex-mena-9475856/
- LinkedIn. (n.d.). Alina Silvia Di Lernia – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/alina-di-lernia-a2849816/?originalSubdomain=ar
- LinkedIn. (n.d.). Andrea Lindholz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/andrea-lindholz-891310250/
- LinkedIn. (n.d.). Andreas Bovenschulte – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/andreas-bovenschulte-a0b24a65/
- LinkedIn. (n.d.). Andreas Harlt – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/andreashartl/?originalSubdomain=sg
- LinkedIn. (n.d.). Andres Tamburi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andrestamburi/
- LinkedIn. (n.d.). Andrew Couts – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andrew-couts-5922412a/
- LinkedIn. (n.d.). Andy Greenberg – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andygreenbergjournalist/
- LinkedIn. (n.d.). Anette Kramme – LinkedIn profile. LinkedIn. [Accessed 24 May 2025]. Available from: https://www.linkedin.com/in/anette-kramme-bb428ab6/
- LinkedIn. (n.d.). Ansgar Heise – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/ansgar-heise-0a958019/
- LinkedIn. (n.d.). Ariane Wolf – LinkedIn profile. LinkedIn. [Accessed 22 May 2025]. Available from: https://www.linkedin.com/in/ariane-w/
- LinkedIn. (n.d.). Ariel Torres – LinkedIn profile. LinkedIn. [Accessed 17 May 2025]. Available from: https://www.linkedin.com/in/arieltorres/
- LinkedIn. (n.d.). Ariel Waissbein – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/arielwaissbein/
- LinkedIn. (n.d.). Barbara Diederich – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/dr-barbara-diederich-5b0299191/
- LinkedIn. (n.d.). Bärbel Kofler – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/dr-b%C3%A4rbel-kofler/
- LinkedIn. (n.d.). Beatriz Anchorena – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/beatrizanchorena/
- LinkedIn. (n.d.). Becky Bracken – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/becky-bracken-65aa857/
- LinkedIn. (n.d.). Bernhard Klutting – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/bernhard-kluttig-002802225/
- LinkedIn. (n.d.). Bert Habets – LinkedIn profile. LinkedIn. [Accessed 3, June 2025]. Available from: https://www.linkedin.com/in/berthabets1/
- LinkedIn. (n.d.). Beth Meinert – LinkedIn profile. LinkedIn. [Accessed May 26, 2025]. Available from: https://www.linkedin.com/in/beth-meinert-95ab832a/.
- LinkedIn. (n.d.). Birgit Wentzien – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/birgit-wentzien-93151372/
- LinkedIn. (n.d.). Björn Böhning – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/bj%C3%B6rn-b%C3%B6hning-84507a180/
- LinkedIn. (n.d.). Bob Rudis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/hrbrmstr/
- LinkedIn. (n.d.). Brent Dirks – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/brentdirks
- LinkedIn. (n.d.). Bridget Bean – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/bridget-bean/
- LinkedIn. (n.d.). Bruce Sussman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/brucesussman/
- LinkedIn. (n.d.). Bryan Krebs – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/bkrebs/
- LinkedIn. (n.d.). Carina Martinez – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/carina-mar/cmartinez/
- LinkedIn. (n.d.). Carlos Garay – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/carlos-garay-4396ba25/?originalSubdomain=a

- LinkedIn. (n.d.). Carlos Horacio Torrendell – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/carlos-horacio-torrendell-ab4939142/
- LinkedIn. (n.d.). Carlos Manfroni – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/carlosmanfroni/
- LinkedIn. (n.d.). Carlos Piro – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/carlos-piro-795bbb104/
- LinkedIn. (n.d.). Carsten Schneider – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/carsten-schneider-482ba6205/
- LinkedIn. (n.d.). *Cecilia Garmendia* – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/ceciliagarmendia/
- LinkedIn. (n.d.). Cherilyn Pascoe – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/cherilynpascoe/.
- LinkedIn. (n.d.). Chris Brook – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/chris-brook-91223712/
- LinkedIn. (n.d.). Chris Castellino – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/chriscastellino/
- LinkedIn. (n.d.). Christian Bauab – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christianbauab/
- LinkedIn. (n.d.). Christian Hummert – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/christian-hummert-b60844208/
- LinkedIn. (n.d.). Christian Wegner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christian-wegner-89852541/
- LinkedIn. (n.d.). Christine Baratta – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christine-baratta-1a2a13a/
- LinkedIn. (n.d.). Christine Fiumefreddo – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christina-fiumefreddo/
- LinkedIn. (n.d.). Christof Klaus – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christof-klaus-4b2286a6/
- LinkedIn. (n.d.). Christoph de Vries – LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/christoph-de-vries-89684a1b2/
- LinkedIn. (n.d.). Christoph Winterhalter – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christoph-winterhalter/
- LinkedIn. (n.d.). Claudia Plattner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/claudiaplattner/
- LinkedIn. (n.d.). Claudia Vizcarra – LinkedIn profile. LinkedIn. [Accessed 15 June 2025]. Available from: https://www.linkedin.com/in/claudiavizcarra/?originalSubdomain=ar
- LinkedIn. (n.d.). Claudio G. Wendler – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/claudio-wendler-175035263
- LinkedIn. (n.d.). Claudio Terrés – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/claudioterres/
- LinkedIn. (n.d.). Cristian Borghello – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/cristianborghello/?locale=es_ES
- LinkedIn. (n.d.). Cristian Gastón Verzi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/cristian-gast%C3%B3n-verzi-28128132/
- LinkedIn. (n.d.). Cynthia S. – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/cynthia-s-4793949/
- LinkedIn. (n.d.). D. Criswell – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/deanne-criswell-862bb2a/
- LinkedIn. (n.d.). Daniela Ludwig - LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/daniela-ludwig-400873240/
- LinkedIn. (n.d.). Daniel Schmidt – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/daniel-schmidt-ek/
- LinkedIn. (n.d.). Daniel Terdiman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/danielterdiman/
- LinkedIn. (n.d.). Dave Bittner – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dave-bittner-27231a4/
- LinkedIn. (n.d.). David Alejandro Kraus – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/david-alejandro-kraus-a3893b56/
- LinkedIn. (n.d.). Deb Fischer – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/company/u-s-senator-deb-fischer/
- LinkedIn. (n.d.). Debora Slotnisky – LinkedIn profile. LinkedIn. [Accessed 20 May 2025]. Available from: https://www.linkedin.com/in/deboraslotnisky/
- LinkedIn. (n.d.). Denis Fernando Romero – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/denis-fernando-romero/?originalSubdomain=ar

- LinkedIn. (n.d.). Dennis Rohde – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dennis-rohde-0a6a381b0/
- LinkedIn. (n.d.). Dennis Velez – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dennis-velez-39562515/
- LinkedIn. (.linkedin.com/in/doreen-hemlock-783953/
- LinkedIn. (n.d.). Dorothee Bär – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/dorobaer/
- LinkedIn. (n.d.). Dustin Gard-Weiss – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dustin-gard-weiss-4323121/
- LinkedIn. (n.d.). Emanuel Rufino – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/emanuel-rufino-1a97428/
- LinkedIn. (n.d.). Emiliano Piscitelli – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/emilianopiscitelli/?originalSubdomain=ar
- LinkedIn. (n.d.). Emiliano Villa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/villaemiliano/
- LinkedIn. (n.d.). Ernesto Claudio Balloffet – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/ernesto-claudio-balloffet-a64177252/
- LinkedIn. (n.d.). Eva Schmierer – LinkedIn profile. LinkedIn. [Accessed 31 May 2025]. Available from: https://www.linkedin.com/in/eva-schmierer-abb791186/
- LinkedIn. (n.d.). F. K. – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/fedek/
- LinkedIn. (n.d.). F. Müller Amato – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/franamatok/
- LinkedIn. (n.d.). Fabienne Tegeler – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: http://linkedin.com/in/fabienne-tegeler-941b37238/?originalSubdomain=de
- LinkedIn. (n.d.). Fabio Guanca Jaimes – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/fabio-guanca-jaimes-7bb1451b8/
- LinkedIn. (n.d.). Facundo Biffi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/facundo-biffi-947375244/
- LinkedIn. (n.d.). Facundo MP – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: http://linkedin.com/in/facundomp
- LinkedIn. (n.d.). Federico Kreplak – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/fedek/
- LinkedIn. (n.d.). Florencia Migliorisi – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/flormigliorisi/
- LinkedIn. (n.d.). Florian Hahn – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/florian-hahn-3290541a0/
- LinkedIn. (n.d.). Francisco Müller Amato – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/famato
- LinkedIn. (n.d.). Frank Schwabe – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/frank-schwabe-738b8741
- LinkedIn. (n.d.). Friedrich Merz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/friedrich-merz/
- LinkedIn. (n.d.). Gastón Aznárez – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/gastonaznarez/
- LinkedIn. (n.d.). Georg Pietsch – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/georg-pietsch-5901b6136/
- LinkedIn. (n.d.). Gregory D Evans – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/gregorydevans/
- LinkedIn. (n.d.). Gunther Krichbaum – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/gunther-krichbaum-49a76b345/
- LinkedIn. (n.d.). Harry Coker – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/harry-coker-4263979/.
- LinkedIn. (n.d.). Harry Mc Cracken – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/harrymccracken/
- LinkedIn. (n.d.). Himaja Motheram – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/himaja-m/
- LinkedIn. (n.d.). Holger Beutel – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/holger-beutel-26123071/
- LinkedIn. (n.d.). Howard W. Lutnick – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/howardwlutnick/
- LinkedIn. (n.d.). J. Basaldúa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jbasaldua
- LinkedIn. (n.d.). J. P. D. Borgna – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jpdborgna/

- LinkedIn. (n.d.). Jake Denton – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/thejakedenton/.
- LinkedIn. (n.d.). James Faber – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/james-faber-82052666/
- LinkedIn. (n.d.). Jay Obernolte – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/jayobernolte/
- LinkedIn. (n.d.). Jeff Moss – LinkedIn profile. LinkedIn. [Accessed May 24, 2025]. Available from: https://www.linkedin.com/in/jeffmoss/.
- LinkedIn. (n.d.). Jennifer Eiben – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jennifer-eiben/
- LinkedIn. (n.d.). Jens Ihlenfeld – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/ihlenfeld/
- LinkedIn. (n.d.). Jens Roemer – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/jens-roemer-82bb57125/?miniProfileUrn=urn%3Ali%3Afs_miniProfile%3AACoAAB713OMBqPmGbXDI6ZbniJ4b5Ho-Za8m4_k
- LinkedIn. (n.d.). Jochen Flasbarth – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: http://linkedin.com/in/jochen-flasbarth-886039322/
- LinkedIn. (n.d.). Joe Robertson – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/joerobertson1/
- LinkedIn. (n.d.). Johannes Bauer – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/johannes-bauer-6b0267198/
- LinkedIn. (n.d.). Johannes Dimroth – LinkedIn profile. LinkedIn. [Accessed 28 May 2025]. Available from: https://www.linkedin.com/in/johannes-dimroth-11259a318/
- LinkedIn. (n.d.). Johannes Hauner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/haunerjo/
- LinkedIn. (n.d.). Johann Saathoff – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/johann-saathoff-34ba78123/
- LinkedIn. (n.d.). Johann Wadephul – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/johann-wadephul-a09861a3/
- LinkedIn. (n.d.). John Ashley – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/johnhashley/
- LinkedIn. (n.d.). John K. Guenther – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/john-k-guenther-a44321174/
- LinkedIn. (n.d.). Jorge A. Teodoro – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jorge-teodoro-7990485/
- LinkedIn. (n.d.). Jorge Abanto – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/jorge-abanto-peru/
- LinkedIn. (n.d.). Jörg Schieb – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/schiebde/
- LinkedIn. (n.d.). José Del Rio – LinkedIn profile. LinkedIn. [Accessed 23 May 2025]. Available from: https://www.linkedin.com/in/jos%C3%A9-del-rio-5a413512/
- LinkedIn. (n.d.). Josephine Ortleb – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/josephineortleb/
- LinkedIn. (n.d.). Joshua Amador – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/joshuamador/
- LinkedIn. (n.d.). Juan Brodersen – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/juan-brodersen/
- LinkedIn. (n.d.). Juan Facundo Etchenique – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-facundo-etchenique-86034155/
- LinkedIn. (n.d.). Juan José Serventi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-jose-serventi-48308210/
- LinkedIn. (n.d.). Juan Mamani (Aka. z1ro) – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/z1ro/
- LinkedIn. (n.d.). Juan Martín Ozores – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-martin-ozores-5b055617/
- LinkedIn. (n.d.). Juhan Lepassaar – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/juhan-lepassaar-961205340/
- LinkedIn. (n.d.). Julia Klöckner – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/julia-kl%C3%B6ckner-0a751923a/
- LinkedIn. (n.d.). Jürgen Freudenberger – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/j%C3%BCrgen-freudenberger-02988520/
- LinkedIn. (n.d.). K. S. Evans – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/karensevans/
- LinkedIn. (n.d.). Karin O Leary – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/karin-o-leary-20233a101

- LinkedIn. (n.d.). Karl Ulrich – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/karl-ulrich-07b135197/
- LinkedIn. (n.d.). Karsten Marquardsen – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/karsten-marquardsen/
- LinkedIn. (n.d.). Katharina Reiche – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/katharina-reiche-0aa257163/
- LinkedIn. (n.d.). Kathy Cherpelis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kathy-cherpelis-b5850aa/
- LinkedIn. (n.d.). Katie Drummond – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/katie-drummond-75ba6313/
- LinkedIn. (n.d.). Kelly Jackson Higgins – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kellyj2/
- LinkedIn. (n.d.). Kersten Auel – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/kersten-auel-57a6b68b/
- LinkedIn. (n.d.). Kevin Flynn – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kevin-flynn-5b603660/
- LinkedIn. (n.d.). Kristina Beek – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kristina-beek/
- LinkedIn. (n.d.). L. Pigñer – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lpigner/
- LinkedIn. (n.d.). Lars Klingbeil – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/lars-klingbeil/
- LinkedIn. (n.d.). Laura Toledo – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/laura-toledo-331030114/
- LinkedIn. (n.d.). Lilian Tschan – LinkedIn profile. LinkedIn. [Accessed 25 May 2025]. Available from: https://www.linkedin.com/in/lilian-tschan-164287105/?originalSubdomain=de
- LinkedIn. (n.d.). Lili Colon – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/lilicolon/
- LinkedIn. (n.d.). Lily Hay Newman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lilyhnewman/
- LinkedIn. (n.d.). Lisa Laporte – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lisadlaporte/
- LinkedIn. (n.d.). Lisa Villalobos – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lisavillalobos
- LinkedIn. (n.d.). Lora Kolodny – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lorakolodny/
- LinkedIn. (n.d.). Louisa Specht-Riemenschneider – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/louisa-specht-riemenschneider-141617238/
- LinkedIn. (n.d.). Lucas Turturro – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/lucasturturro/?originalSubdomain=ar
- LinkedIn. (n.d.). Lucía Mauritzen – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/luciamauritzen/
- LinkedIn. (n.d.). Mara Winn – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/marabishopwinn/
- LinkedIn. (n.d.). Marcela Pallero – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/marcelapallero/
- LinkedIn. (n.d.). Marcos Ayerra – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/marcos-ayerra-8317b634/
- LinkedIn. (n.d.). Marcos Carabajal – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/marcos-carabajal-87119137/
- LinkedIn. (n.d.). Mareike Wulf – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/mareike-lotte-wulf/?originalSubdomain=d
- LinkedIn. (n.d.). María Luciana Carrasco – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/mar%C3%ADa-luciana-carrasco-b185aa228/?originalSubdomain=ar
- LinkedIn. (n.d.). Mariana Echeverría – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/marianaecheverria/
- LinkedIn. (n.d.). Mark Sullivan – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/thesullivan/
- LinkedIn. (n.d.). Marsha Blackburn – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/senator-marsha-blackburn/.
- LinkedIn. (n.d.). Martina Becker-Zahn – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/martina-becker-zahn/?locale=es_ES
- LinkedIn. (n.d.). Martin Bayer – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/martin-bayer-7664881/

- LinkedIn. (n.d.). Martín D. Tartarelli – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/tartamar/
- LinkedIn. (n.d.). Martin Siracusa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/martinsiracusa/
- LinkedIn. (n.d.). Matías Massut – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/matias-massut-a7453914a/
- LinkedIn. (n.d.). Matt Bromiley – LinkedIn profile. LinkedIn. [Accessed May 25, 2025]. Available from: https://www.linkedin.com/in/bromiley/.
- LinkedIn. (n.d.). Matt Burns – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mjburnsy/
- LinkedIn. (n.d.). Matthias Hauer – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/matthias-hauer-616471172
- LinkedIn. (n.d.). Matthias Kranz – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/matthiaskranz
- LinkedIn. (n.d.). Mauro Brandi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mauro-brandi-b36b1b10/
- LinkedIn. (n.d.). Maxi Costantinis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/maxicostantinis
- LinkedIn. (n.d.). Maxi Soler – LinkedIn profile. LinkedIn. [Accessed date unknown]. Available from: https://www.linkedin.com/in/maxisoler/?originalSubdomain=a
- LinkedIn. (n.d.). Mayank Grover – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mayank-grover/
- LinkedIn. (n.d.). Merlin Müller Amato Espert Pucheu – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/merlin-m%C3%BCller-amato-espert-pucheu-4a2044218/
- LinkedIn. (n.d.). Michael Domberg – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/michael-domberg-885aa1a7/
- LinkedIn. (n.d.). Michael Schrodi – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/michael-schrodi-b1a64b134/
- LinkedIn. (n.d.). Miguel Ángel Casares – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/miguel-angel-casares-ab149716/
- LinkedIn. (n.d.). Mohit Kumar – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mohitkumar09/
- LinkedIn. (n.d.). Morgan Adamski – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/morgan-adamski-501094240/
- LinkedIn. (n.d.). Nancy Mace – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/macenancy/
- LinkedIn. (n.d.). Natalia I. Avendaño – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/nataliaiavendano/
- LinkedIn. (n.d.). Nicolás Bunader – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/nicolasbunader/
- LinkedIn. (n.d.). Nils Hillmer – LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/nils-hillmer-061433127/?originalSubdomain=de
- LinkedIn. (n.d.). Norberto Zocco – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/norbertozocco/
- LinkedIn. (n.d.). Octavio Boggiano – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/octavioboggiano/
- LinkedIn. (n.d.). Octavio Gianatiempo – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/octavio-gianatiempo/
- LinkedIn. (n.d.). Oliver Diedrich – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/oliverdiedrich/
- LinkedIn. (n.d.). Omid Nouripour – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/nouripour/
- LinkedIn. (n.d.). Pablo Martín Costa – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/pablo-mart%C3%ADn-costa-4034a9118/?originalSubdomain=ar
- LinkedIn. (n.d.). Paul Rand – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/in/drrandpaul/.
- LinkedIn. (n.d.). Pete Waterman – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/petewaterman/.
- LinkedIn. (n.d.). P Navarro – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/pnavarro/
- LinkedIn. (n.d.). Ralph Jensen – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/ralph-jensen-452b353/
- LinkedIn. (n.d.). Reem Alabali-Radovan – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/reem-alabali-radovan-6a2776178/

- LinkedIn. (n.d.). René Funk – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/ren%C3%A9-funk-191a95237/
- LinkedIn. (n.d.). Rita Cuevas – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/rita-cuevas/
- LinkedIn. (n.d.). Rita Schwarzelühr-Sutter – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: http://linkedin.com/in/rita-schwarzel%C3%BChr-sutter-472451132/
- LinkedIn. (n.d.). Roberto Focke – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/roberto-focke-305043332/
- LinkedIn. (n.d.). Rodrigo Picó – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/rodrigo-pic%C3%B3-3160931b3/
- LinkedIn. (n.d.). Rolf Bösinger – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/rolf-b%C3%B6singer-9a1513174/
- LinkedIn. (n.d.). S. García Larraburu – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/garcialarraburu/
- LinkedIn. (n.d.). Sandra Pettovello – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/sandra-pettovello-243328a/
- LinkedIn. (n.d.). Santiago do Rego – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/santiagodorego/?originalSubdomain=ar
- LinkedIn. (n.d.). Santiago Fernández Boccacci – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/santiago-fernandez-boccacci-16522854/
- LinkedIn. (n.d.). Santiago González Bellengeri – LinkedIn profile. LinkedIn. [Accessed 29 May 2025]. Available from: https://www.linkedin.com/in/santiago-gonz%C3%A1lez-bellengeri-07386714/?originalSubdomain=ar
- LinkedIn. (n.d.). Santiago Pordelanne – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/santiagopordelanne/
- LinkedIn. (n.d.). Sebastián Davidovsky – LinkedIn profile. LinkedIn. [Accessed 20 May 2025]. Available from: https://www.linkedin.com/in/sebasti%C3%A1n-davidovsky/
- LinkedIn. (n.d.). Sebastian Hartmann – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/in/sebastian-hartmann-b79073bb/
- LinkedIn. (n.d.). Serap Güler – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/serap-g%C3%BCler-34a728228/
- LinkedIn. (n.d.). Silke Launert – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/silkelaunert/
- LinkedIn. (n.d.). Silvia Maruccio – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/silvia-maruccio-7983a81b9/?originalSubdomain=ar
- LinkedIn. (n.d.). Silvio Szostak – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/silvio-szostak-1a62016/
- LinkedIn. (n.d.). Stefan Raue – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/stefanrau/
- LinkedIn. (n.d.). Stefan Rouenhoff – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/stefan-rouenhoff-82414b18/
- LinkedIn. (n.d.). Steffen Meyer – LinkedIn profile. LinkedIn. [Accessed 31 May 2025]. Available from: https://www.linkedin.com/in/steffen-meyer-226479157/
- LinkedIn. (n.d.). Stephen Lawton – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/stephenlawton/
- LinkedIn. (n.d.). Susanne Nolte – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/susanne-nolte-9b0b1b268/
- LinkedIn. (n.d.). Swati Khandelwal – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/swati-khandelwal-4566b78a/
- LinkedIn. (n.d.). Tara Seals – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/tara-seals-763a2155/
- LinkedIn. (n.d.). Ted Cruz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/cruzted/
- LinkedIn. (n.d.). Thomas Caspers – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/thomascaspers/
- LinkedIn. (n.d.). Thomas Jennen – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/thomas-jennen-08713614b/
- LinkedIn. (n.d.). Thom Tillis – LinkedIn profile. LinkedIn. [Accessed May 29, 2025]. Available from: https://www.linkedin.com/in/thomtillis/
- LinkedIn. (n.d.). Tim Wilson – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/tim-wilson-ba5a082a/
- LinkedIn. (n.d.). Todd Blanche – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/toddblanche/
- LinkedIn. (n.d.). Tomás Balmaceda – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/tomasbalmacedahuarte/

- LinkedIn. (n.d.). Tomáš Minárik – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/tom%C3%A1%C5%A1-min%C3%A1rik-819b1448/?originalSubdomain=cz
- LinkedIn. (n.d.). Tom Spring – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/zpring/
- LinkedIn. (n.d.). Venio Quinque – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/venioquinque/?originalSubdomain=de
- LinkedIn. (n.d.). Vinod Sreeharsha – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/vinod-sreeharsha-51317b/
- LinkedIn. (n.d.). Wilfried Karl – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/wilfried-karl-67785571/
- LinkedIn. (n.d.). Will Douglas Heaven – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/will-douglas-heaven-843358b/
- LinkedIn. (n.d.). Wolfgang Schmidt – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/wolfgang-schmidt-18213b4/
- LinkedIn. (n.d.). Wolf Hosbach – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/wolfhos/
- LinkedIn. Federico Pierri – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/federicopierri
- LÖLFING, Nils; HEMBT, Simon; BELITZ, Oliver; KARCHER, Benjamin. *Artificial Intelligence 2024 – Germany: Trends and Developments*. Chambers and Partners, London, 2024. [Accessed 11 May 2025]. Available from: https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/germany/trends-and-developments
- MCKINSEY & COMPANY. *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers* [online]. 27 October 2022 [Accessed 12 April 2025]. Available from: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
- Meet the hacker. [online] [Accessed 18 May 2025]. Available from: https://podimo.com/shows/meet-the-hacker
- MÉNDEZ, Flavia. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/flaviamendez/?originalSubdomain=ar
- MICHAEL BAILEY ASSOCIATES. *Flexible Working in 2023 – Germany*. Düsseldorf: Michael Bailey Associates GmbH, 2025 [Accessed 11 May 2025]. Available from: https://www.michaelbaileyassociates.com/app/public/pdf/Flexible-working-in-2023-germany.pdf
- Ministerio de Ciencia, Tecnología e Innovación de la Nación Argentina. *Fondo Argentino Sectorial (FONARSEC)* [online]. [Accessed 20 May 2025]. Available from: https://www.argentina.gob.ar/ciencia/agencia/fondo-argentino-sectorial-fonarsec
- Ministerio de Ciencia, Tecnología e Innovación de la Nación Argentina. *Fondo para la Investigación Científica y Tecnológica (FONCYT)* [online]. [Accessed 25 May 2025]. Available from: https://www.argentina.gob.ar/ciencia/agencia/fondo-para-la-investigacion-cientifica-y-tecnologica-foncyt
- MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN. Con Vos en la Web [online]. Buenos Aires: Argentina.gob.ar, [Accessed 16 August 2025]. Available from: https://www.argentina.gob.ar/justicia/convosenlaweb
- MITRE CORPORATION. *National Cybersecurity FFRDC*. [n.d.] [Accessed 2 June 2025]. Available from: https://www.mitre.org/our-impact/rd-centers/national-cybersecurity-ffrdc
- MORDOR INTELLIGENCE. *Argentina Cybersecurity Market – Size, Share & Trends*. Hyderabad: Mordor Intelligence, 2025. [Accessed 11 May 2025]. Available from: https://www.mordorintelligence.com/industry-reports/argentina-cybersecurity-market
- MOSS, Jeff. LinkedIn profile [online]. Washington, D.C.: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/jeffmoss/
- MYRA SECURITY GMBH. *Myra Minds.* [online]. [Accessed 31 May 2025]. Available from: https://www.myrasecurity.com/en/news/myra-minds/
- National Communications Entity (ENACOM). *Official website of the National Communications Entity* [online]. [Accessed 1 June 2025]. Available from: https://www.enacom.gob.ar/
- NATIONAL CYBERSECURITY CENTER OF EXCELLENCE. *National Cybersecurity Center of Excellence (NCCoE)*. National Institute of Standards and Technology (NIST). [n.d.] [Accessed 14 June 2025]. Available from: https://www.nccoe.nist.gov/
- NATIONAL CYBER SECURITY CENTRE. *Penetration testing* [online]. [no date] [Accessed 15 April 2025]. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.nist.gov/director/leadership
- NETENRICH. *What is a bug?* [online]. [no date] [Accessed 18 April 2025]. Available from: https://netenrich.com/glossary/bug
- ODATA. *Revolutionizing Data Infrastructure: Understand the Role of Energy Self-Production*. ODATA, 8 May 2024. [Accessed 11 May 2025]. Available from: https://odatacolocation.com/en/blog/energy-self-production/

- OFFICE OF THE NATIONAL CYBER DIRECTOR (ONCD). *Office of the National Cyber Director*. Washington, D.C.: The White House, 2025 [Accessed 27 May 2025]. Available from: https://www.whitehouse.gov/oncd/
- OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (OUSD[I&S]). *Official website of OUSD(I&S)* [online]. [Accessed 19 May 2025]. Available from: https://ousdi.defense.gov/
- OTERO, Mariana. Los 'cybercirujas', el movimiento que desafía el 'usar y tirar' de la tecnología en Argentina [online]. Madrid: El País, [Accessed 16 August 2025]. Available from: https://elpais.com/america-futura/2024-09-02/los-cybercirujas-el-movimiento-que-desafia-el-usar-y-tirar-de-la-tecnologia-en-argentina.html
- OWASP Foundation. *OWASP* [online]. [Accessed 18 April 2025]. Available from: https://owasp.org/
- PÁGINA12. *Las mujeres tienen mucho que aportar en la ciberseguridad – Mariana Carbajal* [online] [Accessed 29 May 2025]. Available from: https://www.pagina12.com.ar/794250-las-mujeres-tienen-mucho-que-aportar-en-ciberseguridad.
- PÁGINA12. *Nora Veiras – Página 12* [online] [Accessed 29 May 2025]. Available from: https://www.pagina12.com.ar/autores/2333-nora-veiras.
- PERFIL. *Ciberseguridad oficial vulnerada – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/noticias/cordoba/ciberseguridad-oficial-vulnerada-el-pedido-de-un-experto-tras-el-ataque-a-la-web-del-gobierno.phtml.
- PERFIL. *Darío Silva D'Andrea – Perfil.* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/dsilva.
- PERFIL. *Equipo de Editorial Perfil* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/staff
- PERFIL. *Francisco Larez – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/autores/franciscolarez.
- PERFIL. *Gabriel Zurdo – Perfil* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/gabrielzurdo.
- PERFIL. *Sergio Marín – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/Personalidaes/sergio-marin.
- PERFIL. *Walter Curia – Perfil.* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/waltercuria
- PODCASTAI. *Cybersecurity entschlüsselt.* [online]. [Accessed 31 May 2025]. Available from: https://podcastai.com/shows/fpvwxj-cybersecurity-entschluesselt
- Presidencia de la Nación Argentina. *Agencia Nacional de Promoción de la Investigación, el Desarrollo Tecnológico y la Innovación (Agencia I+D+i)* [online]. [Accessed 19 May 2025]. Available from: https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/agencia
- PROUP. *Sitio web oficial de iProUP*. Buenos Aires: iProUP [Accessed 30 May 2025]. Available from: https://www.iproup.com.
- PUJOL, Laurence. *Making freemium work* [online]. Harvard Business Review, May 2014 [Accessed 13 June 2025]. Available from: https://hbr.org/2014/05/making-freemium-work
- QUIÉN ES EDUARDO GONZALEZ - EL DESTAPE. [online] [Accessed 30 May 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos
- QUILL CREATIVE STUDIO. *Brand color theory: Why color matters for your brand* [online]. May 22, 2023 [Accessed 3 April 2025]. Available from: https://www.quillcreativestudio.com/blog/brand-color-theory-why-color-matters-for-your-brand
- REDFOX SECURITY. *The evolving penetration testing ecosystem: Global insights* [online]. LinkedIn Pulse, 2023 [Accessed 13 June 2025]. Available from: https://www.linkedin.com/pulse/evolving-penetration-testing-ecosystem-global-insights-redfoxsec-kysfc/
- RESEARCH AND MARKETS. *Germany Cybersecurity Market Share Analysis, Industry Trends & Growth Forecasts 2024–2029*. Research and Markets, Dublin, 2024. [Accessed 11 May 2025]. Available from: https://www.globenewswire.com/news-release/2024/09/16/2946526/28124/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html
- REVISTA MERCADO. *Contenidos*. Buenos Aires: Mercado [Accessed 29 May 2025]. Available from: https://mercado.com.ar/revista/edicion-enero-febrero-n1234/contenidos/.
- REVISTA MERCADO. *Juan Martinez*. Buenos Aires: Mercado [Accessed 30 May 2025]. Available from: https://mercado.com.ar/author/juanpmartineznotasgmail-com/.
- REVISTA MERCADO. *Mercado*. Buenos Aires: Mercado [Accessed 29 May 2025]. Available from: https://mercado.com.ar.
- SALTA CYBERSECURITY CLUB. Salta Cybersecurity Club [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/salta-cybersecurity-club/
- SALTA CYBERSECURITY CLUB. Salta Cybersecurity Club [online]. Salta: Salta Cybersecurity Club, [Accessed 16 August 2025]. Available from: https://saltacybersecurity.club/. A community of students, professionals, and enthusiasts passionate about cybersecurity that aims to create a shared space where people can discuss, learn, and share knowledge.

- SANS INSTITUTE. *Official website of the SANS Institute*. [n.d.] [Accessed 1 June 2025]. Available from: https://www.sans.org/.
- SECURANCES. Awareness [online]. Buenos Aires: Securances, [Accessed 16 August 2025]. Available from: https://securances.org/web/awareness/
- SECURE PODCAST. [online] [Accessed 18 May 2025]. Available from: https://securepodcast.com
- SHEHABI, A., SMITH, S. J., HUBBARD, A., NEWKIRK, A., LEI, N., SIDDIK, M. A., HOLECEK, B., KOOMEY, J. G., MASANET, E. R. & SARTOR, D. A. 2024. *United States Data Center Energy Usage Report*. Berkeley: Lawrence Berkeley National Laboratory, 19 December 2024. [Accessed 11 May 2025]. Available from: https://eta-publications.lbl.gov/sites/default/files/2024-12/lbnl-2024-united-states-data-center-energy-usage-report.pdf
- STATISTA. *Cybersecurity – United States*. Hamburg: Statista, 2025 [Accessed 11 May 2025]. Available from: https://www.statista.com/outlook/tmo/cybersecurity/united-states
- SUEDDEUTSCHE.DE. *Verlag: Impressum – Chefredaktion*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.sueddeutsche.de/projekte/artikel/verlag/artikel-e287935/#:~:text=Chefredaktion.
- SUEDDEUTSCHE.DE. *Wolfgang Krach.* [n.d.] [Accessed 1 June 2025]. Available from: https://www.sueddeutsche.de/autoren/wolfgang-krach-1.1143286.
- Swiss Cyber Security Days (SCSD). *Swiss Cyber Security Days 2025* [online]. [Accessed 18 April 2025]. Available from: https://scsd.ch/de
- TANG, D. *What implications do advancements in cybersecurity technologies have on the competitive dynamics within Porter's Five Forces?* [online]. Flevy, [no date] [Accessed 14 June 2025]. Available from: https://flevy.com/topic/porters-five-forces/question/impact-cybersecurity-tech-porters-five-forces-strategy
- THE CYBER EXPRESS. *Germany State of Cybersecurity 2024 Report*. The Cyber Express, 9 May 2025. [Accessed 11 May 2025]. Available from: https://thecyberexpress.com/germany-state-of-cybersecurity-2024-report/
- THE WHITE HOUSE. *The Administration* [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/administration/
- THE WHITE HOUSE. *The Cabinet* [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/administration/the-cabinet/
- TORRES, César. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/c%C3%A9sar-torres-748b78103/?originalSubdomain=ar
- U.S. CYBER COMMAND. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.cybercom.mil/Leadership/
- U.S. DEPARTMENT OF COMMERCE. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.commerce.gov/about/leadership
- U.S. DEPARTMENT OF ENERGY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE (CESER). *CESER Leadership* [online]. [Accessed 21 May 2025]. Available from: https://www.energy.gov/ceser/ceser-leadership
- U.S. DEPARTMENT OF ENERGY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE (CESER). *CESER Leadership* [online]. [Accessed 21 May 2025]. Available from: https://www.energy.gov/ceser/ceser-leadership
- U.S. DEPARTMENT OF ENERGY. *Our Leadership & Offices* [online]. [Accessed 2 June 2025]. Available from: https://www.energy.gov/our-leadership-offices
- U.S. DEPARTMENT OF HOMELAND SECURITY. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.dhs.gov/leadership
- U.S. DEPARTMENT OF JUSTICE. *Organizational Chart* [online]. [Accessed 2 June 2025]. Available from: https://www.justice.gov/agencies/chart/map
- U.S. Energy Information Administration. 2024. *U.S. Energy Facts Explained – Consumption and Production*. Washington, D.C.: U.S. Department of Energy. [Accessed 11 May 2025]. Available from: https://www.eia.gov/energyexplained/us-energy-facts/
- U.S. Energy Information Administration. 2025. *Short-Term Energy Outlook*. Washington, D.C.: U.S. Department of Energy, 6 May. [Accessed 11 May 2025]. Available from: https://www.eia.gov/outlooks/steo/
- U.S. GENERAL SERVICES ADMINISTRATION (GSA). *FedRAMP: Federal Risk and Authorization Management Program*. [n.d.] [Accessed 28 May 2025]. Available from: https://www.fedramp.gov/
- U.S. GENERAL SERVICES ADMINISTRATION (GSA). *Technology Transformation Services*. [n.d.] [Accessed 1 June 2025]. Available from: https://tts.gsa.gov/
- U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON ENERGY AND COMMERCE. *Official website of the Committee on Energy and Commerce* [online]. [Accessed 21 May 2025]. Available from: https://energycommerce.house.gov/
- U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY. *Official website of the Committee on Homeland Security* [online]. [Accessed 24 May 2025]. Available from: https://homeland.house.gov/
- U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY. *Official website of the Committee on Oversight and Accountability* [online]. [Accessed 21 May 2025]. Available from: https://oversight.house.gov/

- U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY. *Official website of the Committee on Science, Space, and Technology* [online]. [Accessed 21 May 2025]. Available from: https://science.house.gov/
- U.S. SENATE, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION. *Official website of the Committee on Commerce, Science, and Transportation* [online]. [Accessed 23 May 2025]. Available from: https://www.commerce.senate.gov/
- U.S. SENATE, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS. *History* [online]. [Accessed 26 May 2025]. Available from: https://www.hsgac.senate.gov/about/history/
- U.S. SENATE, COMMITTEE ON THE JUDICIARY. *Official website of the Committee on the Judiciary* [online]. [Accessed 23 May 2025]. Available from: https://www.judiciary.senate.gov/
- U.S. SENATE, OFFICE OF SENATOR CHUCK GRASSLEY. *Official website of Senator Chuck Grassley*[online]. [Accessed 2 June 2025]. Available from: https://www.grassley.senate.gov/
- U.S. SENATE, OFFICE OF SENATOR TOM COTTON. *Official website of Senator Tom Cotton* [online]. [Accessed 2 June 2025]. Available from: https://www.cotton.senate.gov/
- U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE. *Official website of the Select Committee on Intelligence* [online]. [Accessed 23 May 2025]. Available from: https://www.intelligence.senate.gov/
- UNITED STATES. *About CISA*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/about
- UNITED STATES. *CISA Cybersecurity Awareness Program*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025. [Accessed 11 May 2025]. Available from: https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program
- UNITED STATES. *Cybersecurity Awareness Month*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2024 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/cybersecurity-awareness-month
- UNITED STATES. *Cybersecurity Information Sharing Act of 2015*. Washington, D.C.: U.S. Cybersecurity and Infrastructure Security Agency, 2015 [Accessed 11 May 2025]. Available from: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf
- UNITED STATES. *FBI Releases Annual Internet Crime Report*. Washington, D.C.: Federal Bureau of Investigation, 23 April 2025. [Accessed 11 May 2025]. Available from: https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
- UNITED STATES. *Leveraging AI to Enhance the Nation's Cybersecurity*. Department of Homeland Security, Science and Technology Directorate, Washington, D.C., 17 October 2024. [Accessed 11 May 2025]. Available from: https://www.dhs.gov/group/13025/news/2024/10/17/feature-article-leveraging-ai-enhance-nations-cybersecurity
- UNITED STATES. *National Cybersecurity Protection System*. Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2025. [Accessed 11 May 2025]. Available from: https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system
- UNITED STATES. *Security Awareness and Training*. Washington, D.C.: Department of Health and Human Services, Office of the Chief Information Officer, 2024. [Accessed 11 May 2025]. Available from: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html
- UNITED STATES. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology, 2024 [Accessed 11 May 2025]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- UNITED STATES SECRET SERVICE. *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.secretservice.gov/about/leadership
- Universidad Austral – Facultad de Ingeniería. Diplomatura en Gestión y Estrategia en Ciberseguridad [online]. Universidad Austral, [Accessed 16 August 2025]. Available from: https://www.austral.edu.ar/ingenieria/ingenieria-posgrados/ciberseguridad/diplomatura-en-gestion-y-estrategia-en-ciberseguridad/
- USUARIA. *Asociación Argentina de Usuarios de la Informática y las Comunicaciones* [online]. [Accessed 2 June 2025]. Available from: https://www.usuaria.org.ar/
- WAGLE, K., YOUSUF, S., ALSWAILEM, Y., ALMENGASH, M., and ALTURKISTANI, F. *Turning a cybersecurity strategy into reality: A holistic performance management framework* [online]. Boston Consulting Group, 8 August 2022 [Accessed 14 June 2025]. Available from: https://www.bcg.com/publications/2022/cybersecurity-performance-management-framework
- WALTZMAN, Howard W.; LILLEY, Stephen; HICKEY, Adam S. *White House releases National Cybersecurity Strategy Implementation Plan, Version 2.* Chicago: Mayer Brown LLP, 14 May 2024 [Accessed 27 May 2025]. Available from: https://www.mayerbrown.com/en/insights/publications/2024/05/white-house-releases-national-cybersecurity-strategy-implementation-plan-version-2
- WHITE HOUSE OFFICE OF THE NATIONAL CYBER DIRECTOR. *Office of the National Cyber Director*. The White House [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/oncd/

- WIKIPEDIA CONTRIBUTORS. *Stefan Gödde*. Wikipedia, n.d. [Accessed 31 May 2025]. Available from: https://en.wikipedia.org/wiki/Stefan_Gödde
- WIRED. (n.d.). Matt Burgess – Author profile. Wired. [Accessed 2 June 2025]. Available from: https://www.wired.com/author/matt-burgess/
- WORLD BANK. *Argentina – World Bank Open Data*. Washington, D.C.: World Bank, 2025 [Accessed 11 May 2025]. Available from: https://data.worldbank.org/country/argentina
- WORLD ECONOMIC FORUM. *Global Cybersecurity Outlook 2024* [online]. 11 January 2024 [Accessed 14 June 2025]. Available from: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Paris Convention for the Protection of Industrial Property* [online]. Geneva: WIPO, 20 March 1883 [Accessed 11 May 2025]. Available from: https://www.wipo.int/treaties/en/ip/paris/
- WORLD TRADE ORGANIZATION. *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)* [online]. Marrakesh: WTO, 15 April 1994 [Accessed 11 May 2025]. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

Appendices

Annex 1: Deep understanding of leaders biography

Federico Kirschbaum - CEO & Co-Founder

Federico Kirschbaum is the Chief Executive Officer (CEO) and co-founder of Faraday Security. With over 20 years of experience in the cybersecurity field[117] Kirschbaum is known for combining deep technical expertise with a strategic vision that emphasizes accessibility and innovation in security practices. He is also one of the co-founders of Ekoparty (Electronic Knock Out Party)[118], one of the most important cybersecurity conferences in Latin America. Through this platform, Kirschbaum has helped build a strong regional community around ethical hacking and information security, fostering collaboration and knowledge sharing. Passionate about demystifying cybersecurity, Kirschbaum promotes the idea that security should be proactive and accessible. His leadership at Faraday reflects this mission, helping companies of all sizes better understand and address their digital vulnerabilities[119].

Martin D. Tartarelli - COO

Martin D. Tartarelli[120] is the Chief Operating Officer (COO) at Faraday. With over two decades of experience in the field, he has held key positions in companies such as Interservices Management Company and Red Link S.A[121], where he served as Head of Information Security Engineering. He joined Faraday in 2014, where he leads operations and strategy, helping organizations strengthen their cybersecurity posture. Tartarelli is also an active member of the global infosec community, currently serving as the Buenos Aires Chapter Leader for OWASP (Open Worldwide Application Security Project)[122] Academically, he earned a degree in Systems Engineering from the Universidad Abierta Interamericana, a diploma in Managerial Administration from ITBA, and completed the Entrepreneurship 101 Bootcamp from MITx.

---

[117]LinkedIn. (2025). Federico K – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/fedek/?originalSubdomain=ar.
[118]Ekoparty Security Conference. *Ekoparty* [online]. [Accessed 18 April 2025]. Available from: https://ekoparty.org/
[119]Forbes Argentina. *Seguridad informática: de una necesidad básica a una cultura organizacional* [online]. 13 December 2021 [Accessed 18 April 2025]. Available from: https://www.forbesargentina.com/innovacion/seguridad-informatica-una-necesidad-basica-una-cultura-organizacional-n10833
[120]LinkedIn. (2025). Martín D. Tartarelli – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://ar.linkedin.com/in/tartamar
[121]LinkedIn. (2025). Red Link S.A. – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/company/red-link-s-a-/?originalSubdomain=ar.
[122]OWASP Foundation. *OWASP* [online]. [Accessed 18 April 2025]. Available from: https://owasp.org/

Santiago Fernandez Boccacci - CFO

Santiago Fernández Boccacci[123] is the Chief Financial Officer (CFO) at Faraday. As part of the leadership team, he plays a crucial role in strategic decision-making and shaping the company's financial direction. Santiago holds a degree in Business Administration from Universidad de Palermo in Argentina and has a robust background in the financial sector, having held significant positions prior to joining Faraday. His expertise extends beyond financial management, as he has been instrumental in driving operational efficiency and financial strategy at Faraday. Santiago is also an active participant in the global cybersecurity community, engaging in industry events such as the Swiss Cyber Security Days 2025,[124] where he contributed to discussions on cybersecurity innovations. Under his leadership, Faraday has strengthened its financial and operational position in the rapidly evolving cybersecurity landscape.

Joshua Mador - VP of Business Development and International Sales

Joshua Mador[125] is the Vice President of Business Development and International Sales at Faraday. Based in Buenos Aires, Argentina, he has been instrumental in expanding the company's global presence and fostering key international partnerships. Before joining Faraday, he served as the North American Account Manager at Infobyte LLC, where he played a pivotal role in driving business growth and managing client relationships. Joshua holds a degree in Political Science from SUNY Geneseo and a Bachelor of Arts in Psychology from UC San Diego Extended Studies. He is also active in the cybersecurity community, participating in major industry events such as Black Hat U.S.[126], where he has represented Faraday and engaged with global professionals to discuss cybersecurity innovations.

Annex 2: Transcript 1st Interview 03/04.pdf

Transcribed on April 3, 2025 at 15:57 by Minutes AI

Speaker 1 (00:01)
We, sorry, to answer your first question, we arrived because I started first with the search for companies and we had a hard time finding one that operates in Argentina, in the USA. maybe in some other country as well to which we have a certain

[123]LinkedIn. (2025). Santiago Fernández Boccacci – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/santiago-fernandez-boccacci-16522854/?originalSubdomain=ar.
[124]Swiss Cyber Security Days (SCSD). *Swiss Cyber Security Days 2025* [online]. [Accessed 18 April 2025]. Available from: https://scsd.ch/de
[125]LinkedIn. (2025). Joshua Mador – LinkedIn profile. LinkedIn. [Accessed 18 April 2025]. Available from: https://www.linkedin.com/in/joshuamador/
[126]Black Hat. *Black Hat Official Website* [online]. [Accessed 18 April 2025]. Available from: https://www.blackhat.com/

proximity. And I ended up finding Martín Tartarelli. He happens to be a very good friend of my uncle's, my uncle got married and I met him at the wedding and well, it came up there and I swear, I fell for him. We were there in search of a company. Well, we know.

However, before we get started, I would also like to point out that there is a lot of information that you deal with that is confidential. We take that into account, we know that. Of course.

There are some that you won't be able to pass on to us. We are aware of them.
But also to put your mind at ease, everything you pass on to us is between us and the teachers. It is not published anywhere. In fact, knowing the type of company were to work with, the professors said this is not published in
the faculty.
Nothing, it remains between us because we understand that, well, there is information that is sensitive.

Speaker 2 (01:14)
Yes, all right, let's go anyway.

Very good.
I believe that we are going to see how you are progressing, how the structure is and as I see
information that I do not have at my right now, I may have to get it and so on, but we are going to see at every opportunity.
I can't give you the exact information, but I can you, well, we are in between so much and so much and so on.

Speaker 1 (01:41)
Yes, great.

Speaker 3 (01:41)
Yes, we have.

Speaker 2 (01:44)
Dale.

Speaker 3 (01:44)
No, no, nothing, we have a couple of questions that we put together to guide us, but anyway,
tell us a little about what they do and everything you can think of.

Speaker 2 (01:54)
And after that they're a little bit internalized from Faraday?
Were you able to do any prior research?
Where we started, we did some research.

Speaker 1 (02:0G)
And I don't think I speak only for myself, but for all of us, because we got into a new world that we were quite unfamiliar with.
I personally cybersecurity, I kind of started to investigate after Faraday. But yes, yes, we were
doing previous research.

Speaker 2 (02:25)

Well, great. What I propose to you is, now I will tell you a little bit, the truth is I do not have it prepared, but let me be able to use it so that we have a common thread.
I have a kick off that we usually do with new entries, where I tell them.

Speaker 2 (02:43)
Faraday, where we operate from, what are our markets, what is our purpose. Well, a little bit to
see if this is the right one.
I have in English.
How do you deal with English?
Any of them well?
Because the race is bilingual, so ok, well, great.
So if I speak half bilingual, I won't be offended?

Speaker 4 (03:14)
No, not at all.
We're used to sanglish, so okay, great.

Speaker 2 (03:20)
Well, then if I talk, I closed the meet by accident.
Are they there?

Speaker 1 (03:25)
Yes, yes, we hear you.

Speaker 2 (03:27)
I have so many tabs open that mine was closed.
And I'm telling them a little bit that helps me to keep a common thread. Well, I don't see it. Give me 1 s. I'm not used to being with a single screen.

Speaker 4 (04:12)
And I have a question for you, Cecilia.
This is used as an induction, isn't it?

Speaker 2 (04:21)
Yes, exactly. We're in. Well, first I introduce myself.
My name is Cecilia Garmendia, I am head of marketing for the company. I joined Faraday in 2021, three years ago.
The company has been going through several changes in the last three, four years.
And these changes, obviously, at the communication level, one has to go along with them when I join them.
At that time the project was more focused on scaling the product, on strengthening what we have
as a software solution.
And now that strategy has changed a little bit to show us as the brand we really are.
So what happens with this kick off? It's
something we do as a presentation.
In my case, I half it.

Many times we take on freelance collaborators and not necessarily interns, but it also works every time someone joins, as an onboarding.
So this would be a little bit of the presentation that I give from the brand side, not so much from

the human resources side.
That way it is understood.
Give me 1 s I have one that is, you made me remember, workshop mark, workshop with mark.
I'm over there.
Well, I'm going to start with this one and then I'll move on to the other one.
Well, let's do 1000 of the two because I didn't prepare it, so you tell me.
Well, I was telling you a little bit then, Faraday is a company that deals offensive cybersecurity.
As I was saying, if you are media, if it's fairly new, it's new to you, the industry, don't hesitate to
ask questions.
There are many words or terminologies that you may not know today, but if you are related to
information technology, everything has a way, as well as marketing, there are like True, it is
understood in a very simple way.
Paradis is dedicated to offensive cybersecurity, where we companies protect themselves from
potential attackers.
Within what is cybersecurity, a company can, well, I have an antivirus, I don't know, I generate
that all people enter with a login 1 access.
Well, that's more of a defensive security side of things.
You are not taking a proactive stance to ensure that no one steals your information.
If you are developing an application or a web page, well, I put it on this server sure you do all
the things that you think will prevent you from being hacked, but the reality is that you are only
having a passive, defensive posture.
This is what is known as blue Team.
It's different when you take an offensive stance, where you say, well, I'm going to knocking on the
windows to see which one is left open.
So, if one of those windows opens, that's a vulnerability. And that's a word
you're going to hear a lot.

Vulnerability.
That's where our team comes in, where they find vulnerabilities in companies to prevent them from
being hacked.
So the guys, the team and our tool go knocking on the various doors, test the equipment codes, test the web applications, test the systems, and make sure to see if they find any vulnerabilities.
So, hey, look, I went through this window and the developer changes the code and closes that
window.
This is a vulnerability.
Or also known as a bug. That there is a
bug.
Did you see that term?
There is a bug in the system.

Speaker 4 (08:38)

Kind of a bug, isn't it?

Speaker 2 (08:41)
Exactly.
So we found, there's a bug in the system. We found a bug,
that's a vulnerability.
After that, there is a whole world that this is a very nice thing about the industry, that it is a very collaborative industry.
We do an audit of our company and we find a bat sharing an image, we see that a hacker put a
code and so they access our system.
And well, then that discovery is published, it is reported, and there is an institution, an organization, that gives it a kind of patent number.
Then it says cbe, number such reported by such and such
company. And it gives you all the detail of what is involved.
It is an inspection and tells you what the vulnerability looks like.

So, what happens?
Why do I say it is collaborative?
Because that discovery and that they have reported it, it helps the neighboring company that if
they have that same system, they upgrade it, they change it, they mitigate the BAC.
So, I think it'easier to say it in English because I'm more used to it.
But that's what makes it collaborative, that everyone works in a way to say, well, don't let the
same thing happen to you that happened to me.
I warn you that I was robbed through this place and I tell you how to close it and cover it so that
the same thing does not happen to you.
So well, that's a little bit within the cybersecurity world.
You have different teams, the Blue Team, the Red Team, and well, teams that work more on
the development stage and the team that closes the macros.
Faraday is more focused on this Red Team, offensive cybersecurity posture, where we go out and
look for vulnerabilities within systems.
It's not that we stand around waiting to get hacked. So much
for a little bit of what the spectrum is.

Speaker 4 (10:3G)
Yes, great, perfect.

Speaker 2 (10:38)
Do you have questions, doubts?

Speaker 4 (10:43)
Is this thing where you kind of go around looking at vulnerabilities or finding bugs, is this something that you do constantly with all the companies that you work with or is it like periodically you focus on one and have like a process with one company and then move on to
the next?
Or is it an ongoing thing that they do it all the time with all the companies that they work with?

Speaker 2 (11:03)
Well, that has to do a lot, it's a good question, it has to do a lot with the level of maturity the
company is at and the industry it's in.
There are many companies, such as banks and financial companies, which are obliged to have a
pentesting audit, penetration testing.
That when it is contracts, they say I need a pentesting.
Penetration testing is when a team performs a penetration test on a project, on a web page and
so on.
What do they do?
They try to hack and find vulnerabilities.
So, one product we offer is an assessment of your security.
In this evaluation we do a pentesting that defines the scop, if it is only the web page, if it is the
whole system of the company.
Then it depends on the company.
Some companies, because they are very conscious and very responsible for their customers'
data, because of this and so on, call us and say, hey, I want to do one every month.
But a lot, the U0.
%.
Now, it is much less, because digitalization has made there is much more awareness and there has been a lot of information burst and companies are more aware.
You feel that if they steal your data, you lose customers, you lose reputation and so on.
They start doing it themselves more .
But at one stage, most of them, like banks, credit cards, payment systems, all of them are audited.
So they do have to do it on an ongoing basis because they have to submit it for compliance.
That answers your question a little bit.
Now, we, from the communication area, obviously promote and want to generate awareness
and raise awareness that this has to be something that someone does continuously, that it is
very costly if someone steals your data.
And obviously there is a.

Then I share with you the video we have now that talks a little bit about this, about this pain,
where if I run a penetration test, a pentest, I do an audit, my systems contract and we do the
work and we say, well, look, you have these three windows open, that person goes to close it
and doesn't do it again for a year.
Maybe the day after we fixed it, someone got it lodged and had it running for a year until it was
discovered again.
Is it understood?
So it is important to generate greater awareness, to generate one.
Did I answer your question?

Speaker 4 (13:40)
Yes, yes, yes, yes,
perfect.

Speaker 3 (13:42)
So it is not something that is not a company that is contracted all year round by a company and
that is working all the time on its website, let's say.
It is for work that he is called.

Speaker 2 (13:57)
We can name it if we have the two formats of our business model.
We have both.
We have, now let's see Faraday is a little bit of the nineteenth millennium between technology and
talent.
We can be hired for a project, which is what we call a one shot. It is a one shot project.
I am about to launch an application to the market and I need you to come and audit it.
It's a one shot and it's done.
Then we also get hired for, well, I want you to do a job for me once a month for so many hours.

The project is defined, the scope and everything, and a work is done, as to say, of hours, hours of the consulting team.
And we also have within our solutions a vulnerability management platform, Vulnerability Management.
This is a tool that I am now going to tell you about, which was developed by the partners of the
company doing their auditing work.
And doing that auditing work, them going into companies, discovering vulnerabilities and so on,
they found that they needed a tool that would make their job easier.
The most tedious part, which was not breaking and hacking and finding things, but keeping
track of what they were finding.
Which vulnerabilities, in which assets, assets on the web, on the printer, hardware, on which
attack surface they found it.
And they are terms that, well, where did they find it.
All this management, they developed a tool to make it easier.
This tool was developed as open source, which means open source.
Anyone can download it and install it and view the code and collaborate and so on.
It then caught the attention of other professionals like them and many within very large companies.
Kali Linux, which is an operating system like Windows, adopted it into its solutions.
Just as you enter Windows and you have Word, within Kali Linux, which is an operating system, you
also have Faraday in its open source version.
The guys kept developing the tool, monetizing, making more futures, more improvements for
those paid versions.
And today we also have what is called our tool, which I can tell you, if you have a security team

in your company, that they themselves do the pentesting, that you have a team that says, well, I
hire the tool, you implement it and you do a vulnerability management, looking at the risks, seeing which ones are important.
It is important to know that in the day-to-day work of a company dedicated to offensive security,
you can find 1000 vulnerabilities.

The issue is to know which are the ones that really compromise your infrastructure, because out of
those 1000, maybe only three are really relevant.
This tool helps you to have that visibility and management of vulnerabilities.

Speaker 1 (17:03)
Cecilia, is this platform that you offer paid or do you have a free version?

Speaker 2 (17:13)
The platform has a free version, as I was saying, which is the open source version or as you
can find it on our website, it is called Community.
That everything we Farada has as a purpose a vision of open source tools.
So it is not the only one we have, but you do have a free version called Community, which is a
version designed more for the community.
Ok.
So now if you want I can tell you a little bit about the model and how you will better understand the
products and what we offer and what we don't offer.
And thats the way we're going.

Speaker 3 (17:53)
Great.

Speaker 2 (17:54)
So okay, let's go Who we are and What we are about about our brand and about us, what's
happening in the marketplace.
And well, this was really more for another presentation, so the last two points then we see.
Paradise, there are only two ways of finding a vulnerability. Either you
do or someone else does.
In other words, what we want to promote is that vulnerabilities are found.

The point is that you better find it before an attacker does. Cybersecurity is all about being one step ahead.
What is our vision?
Our vision and mission is to help companies maximize resources of their teams.
We focus on centralizing all efforts and giving the organization ways to adapt its strategy and prioritize what is important to reduce the time exposed.
You're not running some kind of offensive security posture. Narrow the
gap where you're not living, whether or not there's a vulnerability.
We believe in simplifying the complex, stop thinking that cybersecurity is a myth, that everything is
only for a few.
Yes, there is a lot of shortage of talent and that makes it quite, the acquisition is quite, the

acquisition cost is quite high.
But what we want to do is to demystify that a little bit and understand that security is accessible to everyone, that there are different ways to start taking that first step, that it is not
a world I'd rather not get into.
Faraday is not an Isnote Conventional Security Company.
We focus on offensive security with techniques that go beyond the standard, discovering vulnerabilities that others see in 28 characters.
We hack better than the rest.
There is also a connotation of the word hacking as being negative. I was hacked,
I was robbed.
Well, there is a concept that is ethical hacker, which is also why one does not use the word hacker
much because it already carries a negative connotation.
But there is ethical hacking, which is more in line with what we .
This is a little bit of Faraday's history, as I was telling you, how its logo changed and how it evolved.
As we are an offensive security, it was very obvious, we identify very much with the Red Team.

These notes were taken with Minutes AI (https:// myminutes.ai)
The Red Team, when we talk about a Red Team, we are talking about an offensive security team
in hacker consulting and penetration testing, who are trying to find vulnerabilities that others do not
see.
The purpose, security is complex and we want to change that, we want to make it accessible.
Well, this is a bit more the word.
And this is a little bit of a snapshot of everything that cybersecurity is.
What's going on here?
Let's see if I can join them in this.
Can I draw or I wrong?
What's going on here?
This is a little bit what I was saying, when a cybersecurity professional has to do his job, there
are 1 million spaces where he can be looking for a vulnerability within the applications, in test
results, penetration, in scanner running all.
So what does our solution do?
You can inject all that information, import it, integrate it, and then, finally, here is all the work of
Vulnerability Management, what we were telling you about what happens, all the information
that a computer security expert collects and what he has to do afterwards.
It has to send a message saying, hey, this code has a vulnerability, somebody has to change it, it
has to be an Incident Response announcement, and so on.
So, that brings a graphic that kind of shows all the work that our tool does, so to speak.

Speaker 3 (22:11)
They also provide them with the solution.
That is, when they find the bug or what, I don't know, the window that if you also find out how to fix

it.

Speaker 2 (22:23)

Yes, advice is provided.
Is this very much how the are made up?
I don't know if any of you have experience of having worked in any , but it always happens that
you have the marketing area, the systems area, the legal area, the area of development.
So, let's pretend we are in Paradise, I am the marketing area.
We have the security guys and there is the development area that is developing the tool I am
telling you about.
So, the consulting guys, running a test inside our own product, say, hey, there's a problem in
the code and there's a vulnerability.
Then they go to the development area, to the one who is, let's say, in charge of that code. We
need them to change the code because there is a vulnerability.
They advise on how to do it and how to change it.
But the one who is going to change the code is the person who works the code.
Or they call , they say, Ceci, there is a vulnerability in our website, will it be fixed if you update it?
Well, that's it, we have to update the kid. And I tell
him, hey, check it out.
And then I him, look, I think I've solved it.
And they go and rerun the test and me, yes, it's already closed. No, it's not
closed, etc.
It would be the ideal world.
The biggest problem teams have is communication between teams and actually making it happen.
So the developer went in, changed the code, then he said well, try it and see if I closed it.
There's a lot of day to day stuff in there that, well, that's like the ideal world.

Speaker 3 (23:5U)

Inside Faraday.
Or with companies, with another company.

Speaker 2 (24:05)
That's the cycle.
Inside any given company there is the security team that finds that there is a possible information leak and talks to the key holder of that door to lock it.
Then there is the day-to-day work of getting that person to close it and re-running the test to
confirm that it was closed.
That is the cycle of the offensive security process.
I'm going to change, it seems to me that there is one that goes around.
I'm going to submit this one instead of that one because it looks to me like it's going to be more.
There you see,
right? Ok, great.
Well, I already told you about this.
Who are our partners and founders? Well, I was

telling them a little bit about this.
Fede and Francisco are the founders and Martinez are our partners.
All three are well known in the cybersecurity industry and are co-founders of Coparty.
Coparty is the largest hacker conference in Latin America. So, nothing,
here is a little bit of what our logo said.
And this is a little bit of what I was answering before about what is inside our Faraday brand,
inside our proposals.
We have the platform in its various versions.
See the mouse
there? Yes.
We have the platform, the tool, which is Community, is the open source, professional and corporate version.

Then we have the consulting team, and within the consulting team we have Faraday Labs, which is precisely the offensive security team.
They are the ones who do these tests that a bank hires us and they go and try to hack the bank
and tell them how they stole information and so on.
Then we have the research team, which is really what the guys do is, well, they're looking for
vulnerabilities.
For example, in the last few years, vulnerabilities were found and reported globally within the
routers we have, in the most sold router in Mercado Libre, and that one recently made the news
again because it was exploited by Home Routers.
And that vulnerability that the guys found, they report it to the company, the company thanks
them and the company has a time, a period to close that vulnerability and then we make the
publication.
It is given or not.01 fifth.
And that's how each vulnerability starts to have its own number. That's
what the Research team does.
In the last year they have given talks about vulnerabilities they found in Draytek routers, IP device
cameras, the ones you put in your house to film and record and watch and observe.
And last but not least, they developed a tool to detect vulnerabilities in car systems.
Today's cars are all connected by software.
Well, those are systems that can be hacked, like this, that open the alarm, you connect the alarm
and it doesn't connect, things like that.
This is the Research team.
This is more than anything, it is not something that we sell or anything, but it is the equipment
that the company has just for the community and to have papers and documentation of the work we do.

Speaker 1 (28:00)
They do that, I mean, it's all kind of free.

Speaker 2 (28:0G)

These notes were taken with Minutes AI (https:// myminutes.ai)

Yes, you can't see that.
Obviously their expertise applies to our tool, consulting team and Incident Response work. That is, if you monetize when we have a project that needs your expertise. And well, but you
don't discover these vulnerabilities.

Speaker 1 (28:24)
For example, in the cameras in the houses.
But that company does not hire you for no, 1 time you do not discover and you approach it to them. It is not remunerated either.

Speaker 2 (28:3G)
Yes, there are companies that have a Bug Bounty program that will listen to it, which is just the
way they are.
Bug Bounty is a reward for the bug you found. So, well, it depends on the company.
Does it have any recognition for the team or well, no.
Google has giant Back Bounty programs where depending on the vulnerability you find, they
give financial recognition and so on.
It has its own ranking and so on.
That program that Google has is a way for them too, no, that's fine, thank you. So they have
Bamban programs, that is, in this case us.
Now, why it is important to the company.
The laugh team, from the communication side, helps us generate a lot of content for an industry 1 audience of interest that goes online, positioning us as the experts we are in the field and the team we have, obviously, everything.
And at the skills level, the guys who work in that area, give those talks and so on, are guys who really apply all their knowledge to projects for which we are lacking.
So well, then, on the other hand, what you see at the end that says product tools, here I need to
update with two more that we already have, which are these open source tools that are being
developed.

For example, the one above, you can enter a web page, put your site, if it is the same as your
at, I don't know.
We are the website faradysec and my email is aradesec.
I can run a free scan on my website to see if it finds any vulnerabilities.
And then, on the other hand, you have Emploleaks, which is also a free tool. Companies can link personnel.
The weakest link is always the human, the human factor.
So, this tool allows you to say, well, out of all my employees, who have cracked passwords?
Because it is not atypical that I use the same password for my personal email as for my company
email.
So, that also helps them to have an idea of how vulnerable they are. On that side, the human factor.

Well, let's see, for the side, this is kind of everything within the Faraday brand and so on, and in what
we call all in one offense for agile, all in one offensive cybersecurity solution.
What is our purpose?
How to make security more , more scalable, more organized and more efficient?
Where did it all start and what is our vision?
Well, a little bit is doing cybersecurity, specialty.
Why am I you today?
Because they are going to be working a little bit on the company's communication.
Faraday for a long time positioned itself as a brand that offered a tool, a tool, a product, a software.
And at the end of last year it was decided to show us as the company we really are, which is
the company I am telling you about, that you are seeing, because many of the clients were already paying us for that, for the 1000 between the software and the consulting hours.
Then, we had to define a proposal, to show how we are really an offensive company that presents solutions and platforms to companies with a high level of quality.

And that's how today we present for the 10 years, we present the new logo, which is the fusion
between talent and technology.
And well, this is the one you see here.
You will not see it on the website yet because we are just working on it.
If you see these concepts at the communication level, you will see it in the social networks.
But well, we are just in this migration today, what we need to do is to take all this know how we have
had in the last year to the web page.

Speaker 4 (32:47)
Cecilia, may I ask you a
question? Oh, sorry.
I was looking at, I was trying to analyze the previous logo that was made with a graphic design
company.
Was this design also done with an agency or do you have an in-house team that created it?

Speaker 2 (33:05)
With an internal team we created it with Mati and myself. An
internal team.
They are a company, a small area and in many situations we also have collaboration, we work
with freelancers and agencies.
Depending on the project, we outsource or not.
But well, this was something that happened quite organically because we had been working on
it for a long time and it came out of a proposal and well, it seemed to integrate the red that we
had left aside and it showed a little bit of the ninth thousandth between the two.

Speaker 1 (33:38)
I have a question.

Do you now have an area that is dedicated to marketing or communication in the company or
is it sort of mixed in with others?

Speaker 2 (33:4U)
We have an area that is dedicated to marketing and communication, which is my area, I am
marketing.
And we are in charge of both branding and demand generation, as well as collaborations for the
human resources area and others.
We generate organic content, we generate paid communications, we generate and generate
everything related to image and branding.
They ask.
Well, this is a little bit of what I was telling you.
We are an offensive security company.
Over the last decade we have expanded our services to meet the needs of our clients.
We offer a comprehensive set of Red Team 1 services, a complete vulnerability management
suite designed to optimize the work of security teams, a Vulnerability Management solution,
which is our Cybersecurity platform, consulting services and the World Class Research team's
World Class Research.
Our expertise we have been a provider of offensive security since the beginning.
The pension, the attention to detail of the torment, allowed our teams to identify vulnerabilities that
others do not see.
Do we focus on providing risk assessment of vulnerabilities, what it represents for an organization,
what is our market?
The truth is that we are industry agnostics, because you can imagine that everything I have
just told you is pretty much across the board.
From someone who is developing an e-commerce application to someone who works in a bank or, I don't know, in healthcare, an insurance or social security company, or a company
that provides logistics services, trucks have tracking systems, those tracking systems can be
hacked, the truck can be tracked and the merchandise can be stolen.
So it's all pretty industry agnostic.
Obviously there are industries that we mostly work with because they are more aware of the
risks.

But where are we today?
We are in North America, Europe and Latin America.
And who we are talking to, and this is where the difficulty comes in, we are talking to IT security experts and those responsible for the security of a company who do not necessarily
have the same level of knowledge.
In other words, I can be the IT manager of a multinational, but not necessarily.

And I am responsible for the security of a company, that we are not hacked, that information is not
stolen, but I don't necessarily have the background in offensive security.
I come from the security world.
This is a person who is responsible for the security of the company, but does not necessarily have
the expertise or background in security.
And then if we talk to a more technical profile, who are responsible for the security of the company, but they do have a background in cybersecurity.
And that's where ISOs and security experts come in, where all this terminology, which for some
of you today is quite new to them, is in the day-to-day, where for someone I have to tell you
today, just as I had to tell you today what a vulnerability is about, what services they should
perform and so on, it happens to us with customers, they are responsible for security in the
company and they do not know what they have to do there.
They manage a gigantic capital and have no security posture whatsoever. So much for that.

Speaker 1 (37:32)
One thing, sorry, I saw that they are in Europe, North America, I also saw that they have headquarters in Florida and then they also have offices here in Argentina.

Speaker 2 (37:45)
Yes, we have headquarters in Florida, but we do not have equipment.
We have an office to be able to work with the mercatino. At one point we
were going to have offices.
We already have an agency that we work with on the financial side, but we don't have an active resource there.

At one point one of the partners was going to go and live there, but well, the pandemic delayed that and opened other doors that were not necessary.

Speaker 1 (38:17)
That just the same for what you do, you can do everything online, let's say.

Speaker 2 (38:27)
Yes, yes, it depends on the project.
We have been called to test one of the bank terminals, ATM terminals.
This is hardware that must be tested in person.
But yes, generally the same, because they also sent one to test, because physical hardware,
but yes, well.
So, what's going on in the market and what are we going to be working on?
There is an exponential growth of the attack surface that brings greater risks and complexities.
The lack of communication between each surface generates that the security teams cannot have
a cross vision.
They see the website on one side and they see the enterprise system on the other. They are on different surfaces where to focus and where to prioritize.

Attackers take advantage of this to reach sensitive data undetected for weeks, months and even
years.
So it's important, it's said that by 202G organizations that have prioritized a continuous security
posture, based on a continuous security posture, are going to be much less likely to have those
reactions.
And this is where we see, we saw our opportunity, which is to consolidate everything into a single solution.
What you see here is Faraday as the core of our business, vulnerability management is our
core.
And what you see around you is the process I was telling you about before of offensive security.
There is a moment where you act, make an assessment, prioritize, act, make a re-assessment,
improve and make an assessment again.

These notes were taken with Minutes AI (https:// myminutes.ai)

That's the whole process, the cycle of an offensive security posture.
What is the challenge?
To present a solution that allows customers to be agile, to evolve in their security projects and
to be the ninety-ninth of technology and expertise.

Speaker 4 (40:40)
I have a question for you, Cecilia.
What you say about proactivity, about anticipating problems, is this something that as a company,
how it is instilled at the organizational level, how it is worked on, courses or workshops are held to
promote this state of proactivity.

Speaker 2 (41:03)
Being proactive in the face of offensive security?
We have to generate that in our customers.
We are an offensive security company and we have the talent.
What happens sometimes that our customers don't do that in a continuous way, for example, is
today is marketing the career, right?
To wear it.
Well, in this communication career, many times clients go for a project and then forget about it
and that's it, I have already developed my communication, I leave it in time and I don't adapt it,
I don't adapt the content, I don't adapt it to the market and so on.
So you are saying, hey, no, what you did once, you have to adapt it to the context in which you
live.
Improving communication. This is
the same.
We do give workshops, we do give workshops for clients.

It is not something we offer, but we do give it so that they can begin to more proactive. Today our Riser team is giving a workshop in one of the companies that is a client for all the
internal security team, so that they can start to have more knowledge.

I think your question was more on our , yes, we have workshops and so on.
So we are not so much focused on offensive security, but on other things that we need to improve on our side as a company.

Speaker 3 (42:28)
Cecilia, I'll cut you off for a second.
Now we're about to run out of meet, we wanted to know if we can go on a little longer or if you
have to leave.
And if not, that we ask you a couple of questions that we are going to keep by mail.

Speaker 2 (42:44)
I will finish this and if I can, no, I think we can do it in this little time. And if not, we make a second myth.
Send me an e-mail and I will let you know what I can.

Speaker 1 (42:53)
Okay, great.

Speaker 2 (42:55)
So I end this for you.
Well, and that's how this proposed all-in-one solution came about.
And this is what I was telling you is Faraday as the heart of
everything.
And here in what you see in each ring that is above the cycle, this whole ring, this shows a little bit
in the stage that each company is in.
In other words, the first point is to set the first stage, have an offensive security posture, then
make a management of those things that you find, then do it continuously and then have a complete vision of your whole surface behind, like each ring that is growing and in which posture you are growing in that cycle.
Here is how we present our solutions at each stage of this cycle.
What we believe today is that Faraday can accompany depending on each company at the
moment in which it finds itself.

On the one hand there is the platform that manages vulnerabilities, combining both talent and
technology to ensure security at every stage of the cybersecurity process.
And that is where the different types of solutions come in.
On-equal reliability management, managing your own attack surface, automated network team
simulations, optimizing your security posture and offensive security services.
And here you are going to see how this looks in a graphic, you see the mouse where, for example, FaradayOps will manage your own attack surface.
Within that we have attack, surface management, threat intelligence, continuous scanning, cloud

security, a lot of these things.
It is like the nineteenth millennium, training and research.
For example, Faraday Ops will be U0 % platform, 10 % resources, consulting hours, mostly
platform, continuous automating, network teaming is a bit more.
The one thousand and ninth is consulting with a little platform.
And so what is in yellow is almost U0 % consulting, 1 10 % platform.
Then, depending on the pain or need the client has, we adapt the solution to what they are looking for.
Is that understood?
Later I can pass you a brochure that I have in Spanish and English of the latest version of this,
which is not going to be on the web page, so that you have all this plus a brochure that we had
in an event that is also digital.

Speaker 4 (45:25)
Thank you very
much.

Speaker 2 (45:27)
Great.

Speaker 1 (45:2U)
Let's go, guys, if you want, with the document of the questions that were left hanging, if any of
you have it, if not, I have it here.

These notes were taken with Minutes AI (https:// myminutes.ai)

Speaker 3 (45:3U)
Yes, yes, no, we wanted to ask you a couple of questions.

Speaker 4 (45:41) I
have it here.

Speaker 3 (45:44)
Well, go ahead.

Speaker 4 (45:45)
It would be good to go more into the questions that may not have been answered with the PowerPoint, right?

Speaker 1 (45:50)
Yes, yes, total.

Speaker 4 (45:50)
Because I think a lot of them were answered with all this introduction.

Speaker 1 (45:54)
Well, anyway.

Speaker 3 (45:58)

More than culture, which is not so much about what you know, but about what you experienced
while working there, we are interested in a couple of things.
Do you handle any?
Do you want to ask questions?

Speaker 2 (4G:10)
Yes

Speaker 1 (4G:10)
Well, first is how is the structure organized?
What areas do they have?
How is there a leader in each area?
Is there more than one leader?
What is the structure of the company itself like?

Speaker 2 (4G:2U)
It is quite horizontal in this sense, a very horizontal company.
Each area has a team leader and each team leader answers to what is called a c level or a
chief in his or her area, depending.
So, if you have, for example, the product area and the development area, the product area has its
leader, the development area has its leader, and they respond to.
The development responds, in our case, to the Project Owner, for a issue, but they respond to the
Chief, the Co, Martin, Tarta that you met.
And the same goes for the director's.
The Cro, who is the Chief Revenue Officer in this company, has the sales area, which is the sales
area, and in my , the marketing area.
When I joined, marketing was actually a separate area of sales that answered directly to the
CoO, because we were more focused on product marketing.
And now, in recent years, we are more focused on accompanying the sales day.
So, today we answer to the Cro, who answers to the CoO or the CEO.
Then you have the.
Sorry, sorry, if not, those are.
Then there is the human resources area, which answers to the CEO, the finance area, which
has its CFO, and the consulting area, which is the Red Team, which has its offensive security
lead, who answers to the COO.

And so each area has a leader who responds to a code.

Speaker 1 (48:2G)
How many employees are in the company?
I know you also said that it has a lot of independent work and so on, but we were looking for it and
we couldn't find it.
How many of you are currently there at Faraday?

Speaker 2 (48:42)

And today we are I think we are close to 40.
I would have to give you the updated number because there were a couple of additions and so on,
but I think we are being.

Speaker 1 (48:52)
Okay, great.
Then the next question is how would you, being , define the internal culture of the organization?
What values are there that one perceives in this way also on a basis, shall we say?

Speaker 2 (4U:11)
Well, here I am going to tell you the word is that there is a lot of collaboration, a lot of collaboration. As if there is a purpose that motivates everyone to work.
But I think the word that sums it all up a bit is collaboration and that talent comes first.
Then I tell you 2 minutes of my personal story, a little of what led me to come to Faraday or to
make the change from the company where I was coming from, where I had been.
I come from a career of more than 11 years, in a very large group that went from one company to another, taking quite important roles in the companies.
But what I liked about Faraday was that it offered me a culture that was more coherent with my
way of being, my way of working, with my line of work, with the company I was in, which was a healthier balance between the professional and the personal.

But also a collaborative culture, where questions are well received, where when someone has
this, as the industry has, of finding a vulnerability and not keeping it and no, I do not want them
to know that I was wrong or not, I do not want my neighbor to know that I have this vulnerability
to my competitor, but on the contrary, to expose it and think that this information can be useful
to the other and help him, even if he is a competitor, even if he is a customer, even if he is a
client, no matter what.
And that is also taken to the culture within the company, that way of operating. So,
well, nothing, very collaborative on that side.

Speaker 1 (50:55)
Great.
Well, let's see, then, well, you already developed this a little bit, but how is the treatment with
the employees, this collaboration thing, if they are satisfied with the work environment, with
the salary, how is that, that side of it too.

Speaker 2 (51:17)
Employees.
Yes, I think it is an internal survey, but the employees are generally satisfied with the salary
band, and the work dynamics also have a lot to do with it.
This is a company that for many is their first job, or well, many times what we know, feedback

from time to time someone who has left complained about something that later in the other company they are asked three times more than what they are asked here.
So but in general there is a high level of acceptance in the culture, in the salary band there is
always room for better, right?

Speaker 1 (52:05)
Okay, but not because of the company itself or because it's just it's a sector where it's not, an industry, let's say, sorry?

Speaker 2 (52:1G)
No, it is not a ruble, it is a generation 1, an area in which there is a lot of turnover.
We are not oblivious to all that, but it does not stop.

These notes were taken with Minutes AI (https:// myminutes.ai)

And the people who come in, there are enough of them, they stay.
We don't have this thing where, oh no, he was there for two years, he left, I trained him and he left.
The truth is that since I have been here, they have gone for personal projects, it is very low,
the truth is that there is not much rotation and in the context in which we are today, I would say that it is quite admirable.
It is a segment that is a very well remunerated profile in the world. And well, we are
a national company with the challenges that support.

Speaker 1 (53:03)
Yes, yes, total.
Well.

Speaker 3 (53:08)
We are short of time, but we still have several important questions more oriented to the point,
which would be communication and marketing, if you will, what do we do?

Speaker 2 (53:21)
We used some time ago, I have to, now I have to cut it because I have to go to the bank, but if
you have no problem I can do it tomorrow at this time so that you have them before I go on vacation.

Speaker 1 (53:33)
If you like, I'll send you everything by e-mail and you answer me when I can, if not.

Speaker 4 (53:37)
Or we can do one, you said you could do a meet tomorrow at this same time.

Speaker 2 (53:42)
Yes, I have no problem.

Speaker 4 (53:43)
Whatever you prefer.
We can send you the questions or we can do a meet, as you feel like.

Speaker 2 (53:51)
I feel more comfortable telling him about it because it may lead him to doubts that I may be able to answer, which I can't explain to him by writing.
And on the other hand, if there is anything pending, send them to me later and we will complete and continue writing.
Unless they need to reinforce with a third min. At
some point, but we'll give it that way.

Speaker 1 (54:10)
Good.

Annex 3: Transcript 2nd Interview 05/04.pdf
Transcribed on April 8, 2025 at 18:2U by Minutes AI

Speaker 1 (00:02)
They had been left hanging from Thursday.
The first one is a little bit about the history of the company, the founders.
Well, at the last meeting you told us a little bit about who the leaders or most prominent people
were, but we wanted to know how the company started.

Speaker 2 (00:28)
Well, Farsi starts a little bit what I had told you.
The founders of Faraday are Francisco Amato and Federico Kirchn, doing their consulting work in cybersecurity or for companies, to work a tool that would make their work easier.
Then, not finding something that suited their needs, they developed their own tool, which caught the attention of other computer security specialists just like them.
Then it began to be used within the cybersecurity world, so they continued to develop it with better
futures, with better implementations to adapt it a little more to the needs of today's companies.
This tool is today used in its open source version by more than 2,000 users per day.
And, well, then the customer software version has reached companies that are part of the top
500.
We have customers in the USA.
in Argentina, in Europe, a large part of the market.
The kids also had a collaborative purpose of sharing information, of giving talks about things they
were learning.
And they started with a small group of 12 people in a room telling the discoveries they had made, what they had developed, and today it has become the largest hacking conference in
Latin America.

So well, that's how today Faraday after 10 years becomes the company, which is an offensive
cybersecurity company, which provides consulting services and has its own software that it
develops for companies to protect their information.
That should still be on the web, in various places, we must have it somewhere.

We have given interviews, the guys were part of the new promises, the 30 promises of Forbes,
that is, there are like a lot of press links that a bit of his career in so well, on the one hand, for one purpose emerged the Ecoparty, which they are the co-founders and another initiative emerged what today is, at the time it was called Infobyte and today is called Faraday.

Speaker 1 (03:37)
Well, you told us the countries where they operate or in which they are present.
What we have left pending is to ask you the size of the market in which you operate.

Speaker 2 (03:52)
How is the size as far as I do not know well the question out there.

Speaker 1 (04:04)
No, no, sorry.
That there are other companies offering, there are many people offering the same service, it's like
a smaller market.

Speaker 2 (04:18)
Yes, cybersecurity is a small market, but there are many competitors.
There are many, many, many tools within cybersecurity and there are many, many competitors.
There may not be one that is 100% equal, because you attack two problems and the other one
works only one and so on.
But there are many, many companies that in the U.S. market there are many more tools, many
more developments and so on.
And well, in the more consulting profile there are also other companies that do the same.

These notes were taken with Minutes AI (https:// myminutes.ai)
It is quite competitive and in the last few years vendors have grown a lot, it is said how many vendors
there are in cybersecurity.

Speaker 1 (05:08)
And what do you think is the advantage over other companies that Faraday has?

Speaker 2 (05:21)
That we are a solution that is very holistic and that is very integrated and adapts to many tools.
That is to say that we have the capacity to integrate any type of tools that the company is already using and the IT security expertise we have.
All this expertise is given both in the jobs we have and in the tool we develop.
And our open source DNA, this value of being a company that has and continues to develop its
open source version, allows people out there who are entering, who do not have the elements
to buy or pay for a service, to have the possibility of using the Open Source version as a community purpose.
But well, in summary it would be our Open Source DNA, which has many implications in four

values: the IT security expertise that we have within the team, the talent that this brings to our
solution and the ability of our entire solution to adapt to the needs of the company.
Because it integrates all kinds of tools, both IT security and ticketing, which are important in
the cybersecurity process.

Speaker 1 (0G:51)
Then, do they have any sustainability measures? Do they
work with any measures that do not, or.

Speaker 2 (07:02)
In other words, we have been part of projects to analyze the carbon footprint and give back.
In that sense we are a very conscious company, but we do not have any sustainability program
or campaign.

These notes were taken with Minutes AI (https:// myminutes.ai)
We are more concerned with campaigns or promoting issues that concern , which has to do
with having greater diversity in the world of cybersecurity.
So we always encourage women to be encouraged to learn.
It is not for a cultural issue of there being a rejection, but it is for an issue of women being encouraged into the world of computer science and developing in the world of computer science so that there are more women in the world of cybersecurity.
But it's more like giving them platforms so they feel confident enough to enter.

Speaker 1 (08:00)
It's true, it's a world that is as one prejudges it and it's very masculine, but well.

Speaker 2 (08:10)
Yes, so it is male, but not because of a cultural issue, but because of an issue of, I think, having more space where they are encouraged to enter, because it is not that there is rejection, that is, there is not an issue of.
Then on the other , we are more, for me, what has to do with sustainability actions and campaigns, CRI and certification and things like that.
In our case, I always try to focus more on what our company does in the context in which it works, in the community in which it is.
So being open source is part of our, let's say, our CER program, continuing to make a free version
that is accessible to everyone and continuing to put muscle into that.
And it also comes more from the side of inclusion, but speaking of inclusion more than anything else because of the inclusion that one can, I am not finding the right word, because it
is not the inclusion that one thinks of at the level of gender, but it is more inclusion through the
fact that it is generally a group that many people are very introverted, they learn by themselves, so social skills are the ones that they need to develop the most.
So maybe we think more about that kind of program. I would have to
find the right words.

These notes were taken with Minutes AI (https:// myminutes.ai)

But well, today we don't have something in line with environmental sustainability.
Yes, we have done independent projects, but nothing, great.

Speaker 1 (0U:58)
Yes, in fact, we have a sort of a guide of questions already established, and just as we ask you
outside, there are others who are asking companies that work with plastics and others.

Speaker 2 (10:10)
So, well, yes, no, let's see, I have also been for many years and always being part of a company and being part of a company leads you to have this line of social responsibility, but it
is always more important than just the environment.
What do I always give?
What is my service?
And what is the solution I give, what is my service?
Well, in this case, if I were a company that generates a lot of plastic and generates a lot of waste, I would think about a project that is more linked to sustainability and how to reduce the
footprint I leave behind.
If it was in the community I'm in, how do I give back to the company in the city I'm in, to the community I'm in, how do I help with the community.
Then yes, obviously on the environmental side it is as if you have several legs.
In the case of always, at least when we have to face within the companies in which there is
some kind of program or project, you say well, and what is our pain?
What shortcomings do we see, if there is a theme, if there is a theme of inclusion, if there is a
theme of diversity, if there is a theme.
And based on that you train and generate workshops to try to minimize where you see the pain.
In this case and in this project is something that we have been talking about in the last months of
human resources, people and culture, as we say, it is good, in this line, as we say, well, our
community, cybersecurity group and generate awareness of how to protect information, that your
data is not stolen, make the world a little safer for the day to day.

But then, well, that is the challenge, to find where you really have a pain and improve the space where you live, where you are and coexist socially and in terms infrastructure and so on.

Speaker 1 (12:1G)
Well, then Buenos Aires, tell us a little about the logo, how it changed and that now they are about
to implement a new one.
We wanted to know about the last one you told me about, yes, that you did it there with people
from Faraday, but do you usually work with agencies as well or is the communication part handled by your area and nothing else?

Speaker 2 (12:51)

An agency that worked on the project was hired to accompany the project.
The agency was not only responsible for the logo, but also for the new market proposal.
In other words, he proposed a whole new vision in terms of the platform, the lookalike it had to have,
what the ui kit was and so on.
He made a whole proposal based on who the target market was, the market he was going to
enter, and the solution they were getting into.
He made quite a strong change.
That's why he also went over the red.
Well, no, that was now.
And that was a project that the agency entered for that project and accompanied the company
for almost two years, for a year and a half, which was a study and took charge of the whole
project.

Speaker 1 (13:43)
Great.
And currently communication, such as internal communication more than anything else, is managed by you and your team?

Speaker 2 (13:57)

These notes were taken with Minutes AI (https:// myminutes.ai)
Internal communication is handled by the People and Culture team, which is the one responsible for and with me in our area.
In order to start communicating, you always have to start internally and then outwards.
So it is a work, let's say, collaborative, where for us it is important for the construction of the
sea that the internal personnel have a sense of belonging, know the company they work for,
know the things we do, a lot of things.
And this is also one of the focuses of the People Culture team in order to avoid turnover, to
have a good adhesion to the company.
So we work with our area, with my area and with the vision of the People team.

Speaker 1 (14:54)
Will you be able to provide us with an organizational chart later?

Speaker 3 (15:00)
How.

Speaker 1 (15:01)
To understand how many people you have in each area?
I know there are a lot of freelancers, we.

Speaker 2 (15:05)
You told me, sorry, I got cut off, that you asked me to pass you, right?

Speaker 1 (15:10)
If you have an organizational chart, do you have ?
Where they are all the last, but the most important for us to understand.

Well, yesterday you explained to us what each area responded to and so on, but visually like to have it too.

These notes were taken with Minutes AI (https:// myminutes.ai)

Speaker 2 (15:35)
I will ask the human resources department for it later, at least so that they have no name with
the areas and I will share it with them.
Well, we are a small company, 40 employees.
What you will not see in the organization chart is the type dependencies. There
are not so many of them.

Speaker 1 (15:57)
Yes, yes, more than anything else to, well, then, how are the communication channels you have?
Now we know about the networks, you mentioned that to us, we have been looking around, but
internally, how are they managed?

Speaker 2 (1G:18)
The company handles internally as the main channel and way of working.
It is a company that works remotely, mainly with some face-to-face formats during the week,
but we use a platform called Slack, which is a collaborative platform that you can have channels by team, by projects.
That's like the main communication channel of the company. All kinds
of communication goes through that.
Then we rely on e-mail for other types of mail, for some more formal flows, to talk to customers
or some procedures, I don't know, administration requests rather than logistical ones.
And finally, the most informal channel, only for various, let's say, unofficial dealings, is WhatsApp.
The company has a WhatsApp group and, well, there are also some smaller groups, either management or area groups, but these are the most informed channel.
Then towards customers we have channels, depending, we adapt to our customer profile, so
we opened a teams platform, which is a Microsoft that has more openness.
And on a day-to-day basis we have back and forth support with customers on that side, obviously by email, with customers, suppliers and everything else.

And for dissemination and communication channels, we use mailing , the website and social
networks.
And well, we have the blog, everything that can be considered as inside. We do sometimes
webinars, we've had some streaming.
These are the most important channels for dissemination and communication.
And internal communication we also have some standardized communications that have to do
with a monthly newsletter, announcements of new revenue, changes, or in the defined channels, communication, for example, where we put all the news of the month and we make a

summary, it is sent by mail and at the same time it is notified through Slack that the mail was
sent.
Then we have the sporadic communications through a specific Slack channel, saying welcome, birthdays, events and so on.

Speaker 4 (18:57)
Perfect.
Well, can you hear me well or not?
Is there?
Perfect.
Since we are talking a bit about communication and all that internal communication, how is the
company's own communication area structured?
I don't know if I'm making myself clear.

Speaker 2 (1U:13)
No?
In what sense, sorry?

Speaker 1 (1U:15)
You don't have a communication department, but you manage it between Human Resources and
Marketing, right?

Speaker 2 (1U:21)

These notes were taken with Minutes AI (https:// myminutes.ai)

And the communication department would be marketing.
Now, if you are talking about communication, Human Resources has to give a statement regarding salary adjustments and a more formal channel is used.
And it depends on what we are talking about, if it is something general for the company, it is
done by Human Resources, if it is something particular for each area or specific for each person, it is transferred to the leader.
All communication is based on what we want to communicate and we work a little bit with me to
define the best channel.
And the communication structure would be me defining based on what the company often does on a basis, in what is the responsibility of the management and in what is the responsibility of human resources, that it is my responsibility to raise my hand and say che,
this has to be communicated to the rest of the team, because it can generate an overlapping
and something that is positive can become negative and well, that dynamic happens, but that's
a little bit of it.
Then it happens where the director doesn't feel comfortable communicating something and
that's going to happen.
Any company, an area wants to do it, the final decision is made by the director, the CEO, but it
does not happen.

There is a lot here, it is very fluid.
Well, yes, that's the structure, so to speak, of diffusion communication.
Yes we do, there is a purpose in terms of very open communication, it is very horizontal and
talent comes first.

Speaker 1 (21:03)
And are you currently in the middle of a communication campaign that you tell us about or were
you recently in the middle of?

Speaker 2 (21:13)
Inward or ?

Speaker 1 (21:15)
External also.

These notes were taken with Minutes AI (https:// myminutes.ai)

Internal or external that you can mention?

Speaker 2 (21:21)
And look, externally, we are just doing what I was telling you about, the rebranding, let's say, of
our proposal, where we went from being a solution where we offered through our communication channel only a software, to the fact that we also have consulting services and
we are not only a software.
So we are with that rebranding. For a year we
were working on that.
And the truth is that the first staging of all this was last year at an event in October, where the
whole stand, the communication, the brochures, the video, everything went with this proposal
where Faraday is the ninety-ninth thousandth between talent and technology.
Where you don't see that yet, which is what we are working on, is on the website.
So we are just working on this Q, the first Q of the year, on moving everything.

Speaker 1 (22:23)
That.

Speaker 2 (22:25)
Brand concept to our website and digital channels.

Speaker 1 (22:2U)
And of all the digital channels, social networks that you manage, do you think Instagram is the
strongest?

Speaker 2 (22:37)
No, in our case it is ex Twitter because of the market we operate in and LinkedIn because we are
a company at that level of priorities.

At the community level it is twitter, x, then follows LinkedIn and well, and now that we are more
present in a Latin American market, follows Instagram and trailos de meta.

These notes were taken with Minutes AI (https:// myminutes.ai)

Speaker 1 (23:03)
Are the networks managed by you or do you now have someone external?

Speaker 2 (23:08)
No, we work with my team, I have a community manager who is in charge of all the digital content
and the content we also generate the articles to generate information, the interviews, so we have internally.
Great.

Speaker 4 (23:31)
I'm sorry, did you , kind of talking about the networks like that, did you ever have a crisis that
you had there with X or Twitter or some network like that?
Any communication crisis?

Speaker 2 (23:45)
No, no, not because of the communicational crises that are so important.
We had to be very careful because the company underwent a restructuring and we had to sit
down and talk about how we weregoingto manage communication internally so as not to generate a radio corridor and so on.
But the truth is that it flowed very well.
It was good that we were also able to put that on the table when important decisions were being made at the construction level and we did not want it to affect the company and the company's motivation.
But after the crisis at a public level, yes, we are in a very interesting niche and we have been
called as experts from Clarín or as news programs to talk to partners to understand situations
that happen from crypto theft and so on in the world, but we have not been in the eye.
We have had, sorry, yes, it could be a case where we had a situation where they discovered a
bug in our product and well, and the intention is always to warn, well, this happened to us, they
told us that we had this, we solved it, it was solved like this, this is what was affected.

These notes were taken with Minutes AI (https:// myminutes.ai)
And there is this concept of crisis work that is called incident response in cybersecurity, that is,
apart from trying to put out the fire or trying to prevent data from being stolen, you have a channel of well, what do I do at the communication level, what do we do?
What communication policy is in place when we suffer an attack.
That happens a lot in cybersecurity and many companies have such crisis policies.

Speaker 4 (25:45)
Thank you very
much.

Speaker 1 (25:47)
Well, then we move on to public issues and stakeholders. We are almost at the end.
We wanted to ask you who are the main stakeholders or audiences you currently deal with?

Speaker 2 (2G:07)
Stakeholders as shareholder, the owners are the founders, the three partners as of today.
At some point, a couple of years, we went out to look for investments.
Well, it hasn't yet, but if you want, I can put those questions in writing.
But it is a company that is autonomous, sustainable, I mean, I can't think of the word now, but it is
managed with its own capital.
She is my
daughter.
Sorry.

Speaker 1 (2G:42) Hi,
great.

Speaker 2 (2G:47)

These notes were taken with Minutes AI (https:// myminutes.ai)

Yes, yes.

Speaker 1 (2G:48)
It really goes more to what actors are involved with the company. They can be technicians, groups, companies, even individuals.

Speaker 2 (27:05)
Today the partners are the Martin Cartarelli family.
We do not belong to an investment group, nor to a group, nor a folding of companies. So nothing, that's it.
The capital is the company's own capital.

Speaker 1 (27:22)
When you think about communication, to whom do you talk to? I mean, how do you talk to this, to companies, to people, to future clients?

Speaker 4 (27:37)
To the customers they already have.

Speaker 1 (27:38)
Now also, what characteristics does this entity you are talking about have to have?

Speaker 2 (27:44)
Let's just say, we are already a BB company.
We have clients, they hire other companies and we have, to say, two large audiences.
On the one hand is the community, which is the group of cybersecurity experts, for which we
develop more technical content, we talk about open source tools and so on, which generates a

lot of presence and brand positioning and a lot of recognition.
And then an audience that is more targeted by what is called an ICP, which is a specific profile
of future or prospective customers, which within each company we do not speak to someone
in particular.

These notes were taken with Minutes AI (https:// myminutes.ai)

We talk to someone in particular, we don't talk to the company.
Then we try to detect within the company who is the role we are talking to.
Obviously, from the commercial side, they will always tell you that I want to talk to a decision
maker, because they are the ones who basically make the decision whether or not to hire the
service.
But the reality is that we talk to those who are responsible for the security of the company.
Many times they are not the decision makers, but they are the ones who bring the solution to the
table, as if to say I need to hire this type of service.
On the one hand we talk to the community and on the other hand, within a company, we talk to the
CISO CTO, the IT security manager who may or may not, as I was saying yesterday, have a
background in security.
So sometimes we have to do very, very technical content. That's the
content that generally has the greatest reach.
And then content around what we say, more high-level, where it is more the talk like the one I
had with you, where the example a little bit of what would be the first steps to take into account
when you have to consider some kind of solution or what to do when you have to protect your
company.

Speaker 1 (2U:54)
And do you always work with or target private companies or have you also worked with public
entities?

Speaker 2 (30:02)
No, we work with public entities and organizations.

Speaker 1 (30:0U)
Well, we talk about customers.
Now, what are the competitors that you currently have or so the best known?
We are still trying to learn a little bit because we are just getting into cybersecurity.

These notes were taken with Minutes AI (https:// myminutes.ai)

It was thanks to Faraday, so a little at a time.

Speaker 2 (30:31)
Look, I can pass you. It

depends on the market.
Right now we are seeing new benchmarks and new competitors.
Because one of the things as a strategy is that first of all we have to position ourselves in the
country where we are, which is Argentina.
So that I can pass it to you if you like the question you have pending? I pass you the links so you can see the webs and so on.
And then we have other more referents that have been our competitors, but in the market, such as
the USA.
and so on, which are like different branches of competence.
Some are benchmarks and others are competitors based on markets.

Speaker 1 (31:11)
Well, as far as.

Speaker 2 (31:21)
I need to hire this type of service, on the one hand we talk to the community and on the other
hand, within a company we talk to Ciso, CTO, the IT security manager, who may or may not,
as I was saying yesterday, have a background in security.
So sometimes we have to do very, very technical content. That's the
content that generally has the greatest reach.
And then content around what we say, more , where it's more the talk like the one I had with
you yesterday, where I explain a little bit of what would be the first steps to take into account
when you have to consider some kind of solution, like what to do when you have to protect your company.

Speaker 1 (32:13)
And do you always work with or target private companies or have you also worked with public
entities?

These notes were taken with Minutes AI (https:// myminutes.ai)

Speaker 2 (32:21)
No, we work with public entities and organizations.

Speaker 1 (32:28)
Well, we talk about customers.
Now, what are the competitors you currently have?

Speaker 2 (32:40)
Look, I can show you, I'll give you the links so you can see the websites and so on.
Some of them are referents, competitors based on markets.

Speaker 1 (32:50)
Well, as far as questions, that's what we had.
If it is pending, if you want I will send it to you by message because it is very punctual.
Well, we had agreed on the size of the employees or the organization chart.

Then we need, if you can't pass it specific, even if it is on a spectrum of annual income and
salaries.
And clients, well, on the web they have several clients, so let's look.

Speaker 2 (33:20)
Of those, yes, we have had, let's see, we have clients as in the web, we also have, there are
new clients that are not in the web.
We have many banks, current banks, many of the banks in Argentina, some of them cannot
be on the web.

Speaker 1 (33:42)
I imagine there are a lot that can't even say they work. Speaker 2 (33:4G)

These notes were taken with Minutes AI (https:// myminutes.ai)

Yes, there are many who, by contract, ask you not to expose, right?
That you can't say you work with them, but we can't use it as a logo in our communication.
Which is always a big part of the challenge and the work we have with commercial is to get
customer testimonials.
Look for signatures, we can use your logo.
Many times you go for the logo, sometimes on the commercial side.
And well, we always try to.
We have a supplier, a client which is Live Nation, it's like telling you the ticket tech in the US.
is huge and well, nothing, we don't have it in our logos and so on.
Then we have some very small ones that are suppliers of the mining companies' software for tractors and trucks, which is different safety software.
The effect is very large.
But then you have virtual wallets and so on.
The three biggest of all, the three biggest are going to be at the wedding. It could be Lufthansa, it could be kpmg.
Well, until not too long ago we had Aruba, which are not as well known, but they are giants.

Speaker 1 (34:55)
Great.
Good.
Well, guys, I don't know if you have any questions left.

Speaker 3 (35:03)
Hi, sorry, I joined a little later and didn't want to interrupt. Speaker 2 (35:08)

These notes were taken with Minutes AI (https:// myminutes.ai)

No, no problem.

Speaker 3 (35:0U)
How are you, Cecilia?
I think the last thing that remains to be seen, which you may have talked about before, is whether

you have any direct links with the government.
That is, if they work or have certain regulations or decrees that are conditioned by the government, so to speak.
Because in the analysis of the environment we have to analyze how all this political part that can
affect the company.

Speaker 2 (35:3U)
We are not an industry that has to comply with any kind of government regulation, other than
the obvious ones of taxes and so on, but we are not a company that is regulated by the government like a bank or a virtual wallet can be.
They do have to comply with payroll certifications that we are trying to generate.
A certification that will also give us clients that do respond to certifications, such as the government, to hire, if that answers your question, service providers.
Since we provide services to many important companies, and they do comply with many regulations
and well, we try to get the certifications, it allows them to work with us, because they, for example, cannot hire companies that do not have ISO certifications, I don't know what, and so
on.

Speaker 3 (3G:55)
Well, perfect.

Speaker 1 (3G:5G)
I was raised, sorry, from this, the doubt of you need, that is, is there a fight for this to be more
regulated or not?
So it makes it difficult for them beyond the certifications?

These notes were taken with Minutes AI (https:// myminutes.ai)
No, I mean, you saw that nowadays in digital it is very difficult because it is very difficult to pigeonhole it and now it is growing exponentially, but there are times when there is not so much
regulation in this regard.
Is that an advantage or a disadvantage for you?

Speaker 2 (37:31)
I don't know if certification is an advantage or a disadvantage whether or not there certifications or regulations.
It is an issue that is a challenge for all companies and even for governments, speed with which
digitization and these types of mechanisms and agencies advance can harm the health of a
state or citizens.
We are trying to support companies that provide all kinds of services to individuals or entities,
so that they can keep up with the new problems presented by digitization and the emergence of
so many technologies that can increasingly compromise the rules and regulations.
And this will be a personal perception.
The State has to be very ayornado to get something that is at the height of what happens ,

which was what has happened generally cases like Facebook and others that have gone to
the state, what has happened is that they come to take care of people because they do not
know how technology works.
So what they put out to the public or the standards they put out are not in line with what the
product or the technology really is.
I believe that for us today our advantage bar challenge is that people and companies are aware of what we experience every day.
It's like the trauma doctor is very aware of the dangers he can see, I don't know, child with dog,
because he sees it every day in his work.
We see every day at work how companies are very vulnerable to any kind of theft and need to
generate awareness.
Is it understood?
I made an odd comparison, but it's a bit like this.
So our work, don't wait to be hacked before because it is very exposed. And there we are trying to raise awareness and show ourselves as a possible solution.

These notes were taken with Minutes AI (https:// myminutes.ai)

Speaker 1 (3U:40)
Great.

Speaker 2 (3U:42)
Well, do you want to send me?
I'm running out of battery and I'm afraid of that map and I don't have the charger nearby, but if
you want to send me the questions and I will answer those that are pending and you already
have my WhatsApp and mail, so whatever you need to advance or material or content, let me
know, sorry.

Speaker 1 (40:0G)
Next week.

Annex 4: Transcript 3rd Interview 21/04.pdf

Faraday Meeting
Mon, Apr 21, 2025
0:00 - Micaela Wasserman
Well, Cecilia, how are you? Can you hear me well? Yes, everybody, yes. Hello. The interference, I think it was Ignacio's. How are you doing? Very well. Well, thanks for space again. We think it will be the last.
0:19 - Cecilia Garmendia
No, no problem, it's fair.
0:22 - Micaela Wasserman
Well, spectacular. So, we can start. Well, it turns out that we have to analyze the

environment, more of the macro environment, so to speak, in Argentina, in the United States
and they ask us for the country that is the biggest operating market. That is to say, the country where you mostly work. We believe it is the United States, but we wanted to ask you
from the outset which country you might recommend to us or in which country you have more
influence or more work to be able to analyze that country.
1:10 - Cecilia Garmendia
OK. Yes, most of the country today, let's see how. Yes, we, our largest market is the United States, but well, we are just having a transition from that more Argentinean or Latin American participation. This had to do with gifts for customers and I believe that today that transition is stronger. Ah, no. No, no. Yes, it is. Well, 50-50, I tell you the truth, because for them, you find it more interesting, because we have many customers in the United States, and then you add some in Spain, in Germany, in France, quite globalized. So, I think that if we distribute the share, to say, well, Argentina, Latin America, see your countries, San Francisco, United States, they are half mixed. So I think we are just in a transition and gaining market share in Latin America and you can see it. So if you want to go for the market that for years was our majority, yes, it is the United States. If not, I mean, now it is more recent and I don't know how much you have to go deeper, let's go with the one you find more interesting to do the study. Either of the two will have good metrics.
In the United States we have more brand penetration and communication, think. Hello, Cecilia.
2:49 - manuel
Is everything all right? No, it seems to me that for the job we have to do both marked, Isn't it? Of course, of course. I don't know if it was understood correctly.
3:04 - Micaela Wasserman
Which third country, having done the analysis of Argentina and the United States, would you
say is the one with the highest market share or activity?
3:23 - manuel
Third country, I think, I mean, it would be some foreign company that you work for and work for. That is, if there is more than one, to be able to compare or not.

3:37 - Unidentified Speaker
Yes.
3:38 - Cecilia Garmendia
It could be. It could be that way. Uruguay or Spain. There is more than one company. I have
an average, I don't know, in Uruguay there are three companies. In Spain there are three companies. Well, I have that I have not identified. There are in Chile, Ecuador, I do not know.
The market they are interested in, maybe we have a customer. In Germany we have two quite large companies. It may be in Germany that we have one of our best, we have Lufthansa in Germany.
Perfect, perfect.
4:29 - Micaela Wasserman
Well, if that's what we're going with, we're going to find out what market we're interested in and go for some of those countries. But what today is that they don't have a market that works in most of them. I mean, that would be the United States.
4:46 - Unidentified Speaker
No.

4:47 - Cecilia Garmendia
Today our, yes, our, the market in which we operate the most is the United States, but we are in a transition to gain market share in Latin America. And, well, there is a fairly equal participation among new customers. The customers we had historically. Just this year, 24-25, was a bizarre year where we started to focus more on services in Latin America. And today it is already reflected a little bit in the client portfolio that we have. So I would say two
big markets, Argentina and the United States. And then we have a fairly 1-1-3 distribution in
different countries. So at the communication level we are focused on the United States and
Latin America at the communication level. Then the arrival of customers, well, maybe that has been reflected or not in the customers or not.
5:45 - Unidentified Speaker
Great.
5:45 - Micaela Wasserman
Perfect. Well, and with respect to Argentina and the United States, we have been looking for
a little bit and we have to understand a little bit which are the main competitors of Faraday. We looked on the Internet, I do not think this is perhaps correct, but we saw in Argentina, for
example, BU Security, BTR Consulting, Snoop Consulting. If you want, you can tell me the main competitors or if not, I can tell you the names and can tell me if they are correct.
6:19 - Cecilia Garmendia
Yes, I can tell you which are the competitors, which we have for reference. Just a second. Let me see. Let me tell you. Some competitors and references we have 7 What is it? What is it? What is it? What is it? What is it?
7:11 - Micaela Wasserman

What is it?
7:18 - Cecilia Garmendia
at the level... Yes, actually many of them are competitors because of the type of service and
product they offer, but in terms of size, dimension of the company or the capabilities they have, they are... So, some tools that we consider or consulting firms that we consider competitors are bought by giants and are part of a giant group. So, they have much more resources than we can get or investment. Is that understood? Perfect. Mica, it is silenced, I
think.
8:15 - manuel
And, sorry, now you continue, Mica, but I wanted to ask you, I mean, for example, talking about the U.S. market, what part of the market do they cover? I mean, I understand that, well, there are much larger companies, at least these 3, which are much larger. But do you have any statistics on that or what part of what would be cybersecurity?
8:43 - Cecilia Garmendia
The market is huge. There are thousands and millions of charts. We are more positioned in
the verticals that have to do with penetration testing and bull management. We would like to
aspire and we are continuously aspiring to what is called CTEM, which is continuous security. Well, continuous security, continuous cybersecurity. But at the vertical level it's gigantic. It is not a niche in itself, but you can have tools like an antivirus and we are not in that vertical. Or you can have a tool that does code scanning and we are not in that vertical.

Or you have tools that do management and there, yes, we are a little bit there. So, our product is more positioned in offensive cybersecurity, which has to do with Google Management tools. And then within Google Management you have tools that make reports,
tools that make content, tools that make content. So, it's a good question, but it's more complex than it seems. The challenge is always to position yourself in one of those markets.
But whether you like it or not, the reality, outside the books, is that you attack a problem and
many when a client comes to you, you end up giving him a solution beyond the problem he
has. So, yes, at a communication level it is always good to find your market fit, where is your
value proposition, whether in reporting, scanning, or doing, because you can't do everything.
But in reality it is as if today we are trying to position ourselves in a sensation where there is
a real need to be one step ahead of the attackers and that implies that the biggest problem
that companies have today is that there are many, many, many tools, many ways to be attacked and they have many tools. So today we are more focused on incorporating and integrating all kinds of cybersecurity tools within what is vulnerable and Red Team Services.
And those are more our platforms. But well, there is a lot, there is a portal called Gartner, which is like the TripAdvisor of software platforms, which is a review platform. And they kind
of condition the names of the verticals, which are the verticals that are going to get more invasion, which are the verticals that are going to generate the most traffic, and, well, I think
that, Perfect.

11:58 - manuel
For, and in Argentina, that is, what is the difference with the United States? In Argentina there are fewer, more companies? Is it very different or is the framework very similar?
12:15 - Cecilia Garmendia
No, in Argentina it is different in the state the company is in. And at the level, it's kind of at a
more initial stage in taking an offensive security posture.
So the message is clearer and it is, we are part of your team, we are the mix between talent
and technology, because many times our technology, our tool, needs to imply that there is knowledge of information security within the company, or that you have someone who knows how to use it, who has that technical knowledge, it is not, it is accessible, it is understandable, but you need someone who knows what they are doing. It's like giving a design program to someone who doesn't know how to design, they're going to know how to
navigate it, they're going to know, but they're not going to get the most out of it. Or an autocad, someone is going to know it, an architect, it's different what someone can do being
that someone, I don't know, from one side I design with the other, and so on.
13:25 - manuel
That is, maybe this offensive security posture here in Argentina is still not well adopted. That is to say, it is not so. It is the conscience.
13:36 - Cecilia Garmendia

It's not so, yes, exactly. And it's not just awareness, because probably the one we're talking
to is super aware of what's involved. The issue is that, generally, he needs a budget to be approved. And, well, the challenge is that those who run the company or those who have the power, let's say, to distribute resources within a company, say, well, I give more resources to marketing to generate things for customers and communication. Or I give budget to the security systems team, who are responsible for the security of our company, to prevent something from happening. It depends on the industry they are in, if it's someone
who is in fintech, in banking or so on, they are much more aware of the risks they suffer, of that risk. Now, if it is someone who is, I don't know, in the last one, in 2024, the two groups that hit the hardest in terms of hacking were the San Cristobal group, which is in insurance,
and the group, a group of laboratories, which I don't know the name now, but it is also very well known and they didn't have it as part of their management agenda. In other words, probably the resources that the system has are very few or in security or none at all. And well, I think the challenge is to generate that awareness, not only in those who are dealing with the problem, but also in those who make the decisions, so that they understand the risk
of not being protected.
15:12 - Cecilia Garmendia
Perfecto.
15:12 - manuel
Well, Mica, Sori, do you want to continue with the questions that you came there in order? Or? SORIYA YODANISHI LEONENBURGUEY FOR INTERPRETER Dale.
15:21 - Micaela Wasserman

Well, with respect to the competitors, we are seeing that, at least in the message that they convey on the website and so on, they talk about Faraday being the market leader. Is that the case? I mean, do you stand out against competitors or do you have an advantage? Against your competitors? Yes.
15:44 - Cecilia Garmendia
OK, perfect. Yes, it's like that. It's not like that from the side of... Yes, sorry.
15:53 - Lourdes Medrano
Would this All in One Solution be your advantage?
15:58 - Cecilia Garmendia
Or does it go that way? Yes, it goes that way because, as Manuel answered, our solution is
inclusive, it integrates many other tools. In other words, if you are using 5 different tools, whether artificial intelligence or scanning or whatever, we can integrate them into the Faraday tool and you can see everything in one place. And at the same time we have the consulting expertise and what, if you don't have an IT security team, we can do the work or
the IT security tasks. That's what the All in One Solution is all about. Why are we the market
leader? And this does not come from the fact that if we have more clients, that the rest does
not come at the leader level on that side, but that we really have the new proposal of the mix
between technology and experts and talent, it is because we have the best experts in IT security within the company. And that is reflected in our functions and in our tool and in the service that we provide. And it's a very scarce IT security resource. So it's always like, it's quite expensive because of the scarcity, so also by providing a service like this, you can lower the cost of the work a little bit. Super.

17:23 - Micaela Wasserman
Well, with competitors I think we are already there, because we needed to understand a little
bit more specific things. And now entering into the value chain, if the process applies. We were looking at, because they ask us to show the process from the time the service is acquired, so to speak, until the service is being executed. So, a little bit what we were looking at is understanding how it works from start to finish, right? Is there some kind of value chain that are following in all the processes that you have and all the services? Or does it depend a lot and is it relative depending on the company or the particular case? Yes.
18:24 - Cecilia Garmendia
Let's see, I think you have two branches, one when it is a 100% consulting service, which are hours that are delivered. And then another one when it is, or three, two big branches. When you have consulting hours included, which is an only one, where we have our team behind the client doing the information security work. Or another value chain when it's an only one they hire the software and they use it themselves. And the two present totally different challenges. We say onboarding to the client, don't we? Why? Because we are not a
B2C. The normal value chain would be, I purchase, I want to purchase a product from the moment I go to e-commerce and I get that product until I receive it, which was the moment I
had the most satisfaction I had, right? So that that

cycle repeats itself. And let's have that continuous flow model where the customer goes up buying. In our B2B model, the value chain is, from the moment a customer requests one of our sizes or asks for a proposal, the value chain starts there, because we want to manage the whole jinx as much as possible. He thought he was going to buy through the communication we gave him, through the meetings with sales, where they told him, well, look, you need this solution. And it really fulfilled that first need. OK, I was looking for a vulnerability management tool with help, with expertise. And when the time comes for the first proposal, whether or not it meets what we were saying. Then it's at the moment of delivery, the delivery, where it really starts to be use and changes. Like the moment of adoption of our service where we give them quite personal assistance so that they can see
the value of the changes in the reports of the work that is being done and so on, so that at the time of the renewal, on the one hand, I think that the need to show that generally their greatest interest is to show the rest of the company that they helped to work with us with a tool like ours and, well, we also accompany them in that challenge of defending internally the proposals or changes so that the cycle is renewed again. I do not know if this is understood.
21:08 - Micaela Wasserman
It is perfect, we see it as something more theoretical in the typical manufacturing industry procedure, there are processes, so it is very useful for us. And well, and also what we had seen is that you had mentioned that some parts were outsourced to other companies, we wanted to know in general what is outsourced.
21:39 - Cecilia Garmendia
At the communication level, within the marketing area, I outsource the management of ads or paid media. I take care of the management and strategic part. We also manage part of the graphic design resources, not UI or UX. And, well, and then they are outsourced. There
is a team, they have to do a lot with timing and need. Today there is an outsourced support
team to accompany customers during all these moments of adoption of the solution, so as not to have customers without response basically, so that the problems they have when

using the solution are solved as quickly as possible for everything related to customer retention. I think that is where we are very focused. More in the area of communication, generally acquiring a customer is always the highest investment, it is the most expensive. In
terms of muscle, in terms of investment, in terms of everything.
So, the challenge is always to try to retain them. And it would not be good that, for example,
in marketing we are sometimes getting so involved in the sales process because it is very difficult for us to reach the customers because they are lost because they have not been contacted for three days. The same thing happens with support and so on. So, in that sense,
all the fruits of the communication part, of finding the value proposition, of giving the right market fit and communication and what difference and so on, collapses if there is no fluid process at the time of acquisition and not only.... So a lot of our resources are there to reinforce that moment of adoption of our solutions. And, well, then in the communication area, the ones I told you about, more than anything else, a graphic designer who helps us with all the internal communication, which is very demanding. And a paid media that helps us with all the campaign management.

24:01 - Micaela Wasserman
Very good. That's perfect. And then, regarding the way of operating, speaking, if you want, you can refer to the TAM block and the United States, do you detect any significant difference in the way of operating in the different countries, as something that catches your attention, or do they generally work in the same way? If you operate, sorry, if you operate from their side or from our side, as I do not understand you as a company, when you work in the Argentine or Latam market, however you want to put it, or when you work with the United States, do you find in your way of working or of distributing Faraday's service, whatever service you choose, that there is a significant difference when working in different
countries?
24:56 - Cecilia Garmendia
Yes, yes, and that, well, culturally, we have a different work culture and that is marked, it is noticeable depending on the country you are in, with the clients you are with. Some are more
demanding, others need more support. The US market is more autonomous, more independent, also because we go to that market with a product that is more, yes, the product
we offer in the US market is more of a self-management tool, that is, unless they have a need, the invitation is that they download the tool, implement it and use it. The challenge in
the value chain is that there is adoption, because it has happened to us with clients that we
were going to renew after they had used it for a year and when we saw the use, they had not
used it for the whole year, right? But well, it is different with the product we are going to Latin
America, which is more of a continuous relationship, because there is a lot of consulting. So I
believe that the U.S. market will be a market more because of the experience, I have data to
prove it, but not because of the experience. It is a market, and also because of the product we offer, it is a market that has high levels of demand.
26:20 - Micaela Wasserman
And many informed too, right?

26:22 - Cecilia Garmendia
Yes, they have a higher maturity in terms of They have a higher, we call it maturity . The first
thing we do is an audit of the sales team to understand what stage the company that is looking for the service is at. What do we mean?
First is whether they have an offensive cybersecurity posture. That is, if they only have, if at
some point, beyond having a secure network or working in an infrastructure that they are scanning to see if someone enters or if there is an information leak, And they also generate
as penetration tests to see if they have any open windows. So, first of all, that is a posture. Then, if you already have that first offensive cybersecurity posture, where you say, OK, I want them to try to hack my application to see where there is a bug in our code that they can steal our information. That's the basis.
Start with that. It could be your faculty saying, I want you to come and scan the company's websites to see if somebody can get into the faculty and steal the students' data or the students' credit cards or whatever. Then there is, so the first thing that sales does is to understand at what level, what stage, what level the company is at to see if our product can
fit or we have to give them something that is more in line with what stage they are at. No

We want to, you don't want to, you can't start like that. We have to start, many companies say, I already want this solution and so on, but they have to take some previous steps. It doesn't matter, otherwise it's like running before starting to walk. So it is understood that in the United States we see, and also because of the product we go with, then I guess the clients we attract, that there is a level of maturity a little more awareness, more advanced than what one can see in Latin America. That level of maturity in Latin America is seen in the companies that are more audited by the industry in which they move, such as banks, fintech, the.... They are... Because they are in the financial and capital movement, they have
to comply with certifications and regulations that require them to have certain monthly reports from the security of their infrastructure. Perfect. Not with a question, not with a simple answer, I, sorry.
Take the choice aside.
28:57 - manuel
Hey, what do we need because you are answering us several questions by answer, so it's good. Sure, yes.
29:05 - Unidentified Speaker
Great.
29:05 - manuel
I don't know if there's any of this left, Mica, or... No, no, . From Value Chain we are.
29:13 - Micaela Wasserman I
don't know if this is what this
looks like?
29:16 - manuel
plus Faraday's customer in the two different markets, such as price, sustainability, innovation, I don't know, I don't know if they ask.
29:25 - Micaela Wasserman
Yes, maybe instead of doing so much, because I feel that we are not going to get there otherwise, maybe as we are seeing that you had told us that there were many types of clients such as companies, they also worked with the public, with banks and what do I know,
but they have some type of client, I mean, it is not that they have a fixed type of client. They

work with many industries at the same time, right?
29:51 - Cecilia Garmendia
Yes, we, yes, the one that is called the ICP, the ICP or the ID, the Customer Profile. The reality is that we are industry agnostic. Any company that today you don't tell me, hey, look,
I know if I have a company that is looking for a solution like yours. But obviously we don't talk to them. The whole company and the whole industry, because it is a lot to cover. So, we
focus on markets where we already have some examples, such as banks, we have many clients that are banks, large groups of banks. So, well, that is one of our industries. And then, it is around last year, we also defined to attack the insurance industry. We understood
that the context and the situation they were in, Faraday was going to present itself as an immediate need. Then we also have within the industries that we attack, we have, well, insurance, banking, fintech, a lot of that. Y

Then, well, as countries have some that are outside these industries, I do not know, from agriculture, some few, well, Lufthansa, which is aeronautics, virtual wallets, stadiums, soccer
clubs, in stadiums, soccer clubs we have, that is, the range begins to open, it is like when you position yourself as a leader or in Latin America we are well known by the founders and
work a communication that is half founder advocacy, where they work on their personal brand and their personal branding. And all that personal branding is reflected in our brand. We reach some clients a lot through this type of reference, right? Perfect. Super. Great.
31:51 - manuel
Well, and now I want to ask you a couple of questions about the products you have. In other
words, in this case they would be services. But you had told us last time. I don't know the different services you have, but to see if you are sticking with the ones you have or if you are
developing new ones all the time. And, well, if they have had any key launching of an application or a new service in the last few years and how they are doing.
32:34 - manuel
who don't need an hour of consulting or anything else. So what is it called?
32:37 - Cecilia Garmendia
What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is called What is called What is called What is called?
32:40 - manuel
What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is what is called What is called What is called What is called What is called?
32:59 - Cecilia Garmendia
What is it called? What is it called? What is it called? What is it called? What is it called? What is it called? In terms of our solutions, we have our Vulnerability Management platform,
which is a tool that centralizes and streamlines all vulnerability management, prioritizing those that really represent a risk. Then we have four, we are going to put four more solutions that are focused on solutions that are a mix between the platform and the consulting services or just the consulting services. Basically, Faraday has the Faraday Platform, the All-in-One service, which is a mix between the two, and the consulting service

alone. We're going to synthesize it very much along those lines, but I think those are the big
three. Then, within each of these three big ones, well, the Platform, yes, you always have plans, it works as a software, you have the professional or corporate plan, but it does not have another thing that is between or not. But then within the consulting and platform services, that is, well, I give you the license because that way I show you the work we do, but inside I do a continuous scanning, which includes equipment running every month, scanning and so on. Cloud Security, which is cloud security. And I do an administration, I do
all the part called Attack Surface Management, which has to do with all the management of
the entire attack surface. That is a mix. And then you have within the Red Team solution or consulting in offensive security, you have, we can run reports, we can do a penetration test,
which is called Penetration Testing, or do a test on an application, which is called Application Security, or a code review, which is like Review. And also an example of Phishing Attack, which is when someone sends you an email and,

Well, that's done as well. Companies hire that as being trying to do a phishing and see if someone from the company falls to see how, well, you're seeing there how skilled the company's staff is in that. So, what are the solutions? There we have those three big verticals that then open up in each of their sub-solutions based on the needs. And you had asked me something else, when did we launch? In 2021 Faraday focused its market fit on scaling in what was software and we did a launch of the new version of our platform with a whole new UI, an extremely user-friendly platform for navigation. IT security experts are more used to code and query terminals and so on. And this one had a really UX friendly approach. So, well. That was by the end of '21. We did a big launch of their version, of a freemium version that was called personal and so on. And with that we gained quite a bit of
recognition. In this 23-24, the strategy migrated to be one, because it was also this, to position ourselves in what the clients really end up hiring us. It is the mix between talent and
technology. And that is just now, it was presented in November 2024 in a hacking event with
all the new communication and branding proposal, and the big debt of that, that you are not
seeing, that there is only a banner on the home page, is the website. Today it still does not show what I am telling you The website does not reflect it that much. It still half software.
37:21 - Unidentified Speaker
Perfect.
37:22 - manuel
And what would be the solution of all these, the ones you have, the one that sells the most,
or the one that is generally used the most?
37:35 - Cecilia Garmendia

I believe it is Faraday Card, which is the Red Team's automated simulations. It's a one-in-one solution. Continuous Automate and Red Team, more. But those are good questions.

We're kind of just gaining new customers in this line and I'm little bit more mature to tell you.
37:55 - manuel
Let me give you a context.
37:57 - Micaela Wasserman

We are analyzing the BSG Matrix and we have to see which is the service, the solution that
generates the most revenue, right? To analyze a little bit the portfolio of solutions that you have. I mean, that's what the question is about. But it is perfect. OK.
38:12 - manuel
No, well, but with the previous thing you said about the launching they did, it is also good because we, also, I mean, I did not understand well, but it is something new what they did, this thing they launched in November, which would be like, let us say, a new solution that we
also do not know if it is going to work or not. That is, if it is still generating income or not.
38:40 - Cecilia Garmendia

Exactly, this is a new brand proposal, we did more of a rebranding and what we owed, how
was the rebranding process, we were asked the strategy to the communication team, the first stage involved generating all this type of content at a digital level so that the sales team
could go out and test the market. We took advantage of the fact that it was the 10-year anniversary last year and we already made a new logo proposal where the Roscoe concept
appeared within our logo, which is what represents the Reptims, which is more the offensive
party and all that was taken to communication, video and others that could be passed on to
you because it is on YouTube, now I am passing you the link and the only place that is still not there and I am also being chased by the management for this, is the web page, so all this is already being sold to the clients and the biggest problem we are having, or the biggest fault we have is that we say hey, we offer you all this and when the client goes to the web page, he has something else.
39:52 - Micaela Wasserman
Well, even that Cecilia, I think that after the analysis and when we put together the whole communication campaign, maybe we can send them to you and something can be useful in the future so that this can be implemented. Very good.
40:05 - Cecilia Garmendia
Suddenly I ask you,
hopefully.
40:07 - Micaela Wasserman
And of such quality that it can be of use to them.
40:12 - manuel
Buenísimo.
40:12 - Cecilia Garmendia
There I will pass on, no, I think it's great, and also, if you can also lean more on the history of our social networks, particularly LinkedIn, where you can see a little, there is little more infographics of what was the proposal of the 10 years and where we started to change our style of communication, an Only One solution. It was always a concept that we carried, but we always had it as a second, as an olistic, a formalistic, and also never as our main pitch because basically we were offering a software and we were not selling at that time the consulting hours. It was like an extra, an add-on that we were giving to the software, not as
the main solution of our portfolio, so to speak. I'm looking for the video, I'll pass it on to you.
41:06 - manuel
On that subject, one last question I was going to ask you, if at any time you launched any

product that did not work, as you expected or any product or service, sorry, a solution or an
application or , that did not come in the way you thought it was going to work, I don't know.
41:29 - Cecilia Garmendia
And it was a success from the arrival side that we had the personal version, the premium version of our system. It was a success. What was not a success was how we

we monetized that resource. It ended up being very costly. We didn't generate any customers. It's like we had more than 1,000 instances generated monthly and we didn't manage to monetize those instances into real customers, because it was a free version. So
the campaign, the communication, the acquisition was very good, but we could not find it, either because the product did not end up being, the product did not end up being friendly enough as it seemed, because we had failures in seeing it as one, in the execution of one I
think there was a lack of internal communication in the real focus of what was expected and
from my point of view it is like the product was strong, the communication was strong, we lacked the ability to understand the capabilities to make the most of it, it is not something that I would say was not useful but that we did not execute it well. I don't know if it is understood. I don't know if it's understood.
42:56 - manuel
I didn't quite get the part about monetizing it , didn't we monetize it right?
43:01 - Cecilia Garmendia
We launched a product that was free in order to reach more customers and using that free tool they would buy their paid requests from us. Like Spotify launches a free product and we
stayed in the premium stage. In other words, it was a free version that they reused and we couldn't get them to make the transition to one of the parks.
43:27 - manuel
Great. Ready? Anybody want to go on with this? Or Nacho? I'm next.
43:32 - Micaela Wasserman
Well, then, just to be clear, the freemium part, that doesn't exist anymore, that was the one that didn't work. Because on the web it still appears as an option for.... Yes, but it is for 15 days.
43:50 - Cecilia Garmendia
Is there a freemium version? Sorry, do you have a freemium version that is ours? Let's see how it is on the web.
44:00 - Unidentified Speaker
Sorry.
44:00 - Micaela Wasserman
In other words, there is the personal, the freemium, the professional and the corporate, I think it is. Of course.
44:08 - Unidentified Speaker
Good.
44:09 - Cecilia Garmendia
The product has been readapted. Before we gave you the full version, today this freemium version simply lets you scan your website and gives you a report by email. Before you had a
complete tool with less features, it was the freemium version. The free for all is a community. Yes, sorry. It's the first come, as we call it. You can run it,

at least have an idea of running it as much as you want, as long as it is yours, your ownership, and we will not be run. You can run it on Faraday. If you have a business and

your own website, you're going to be able to run it. And that gives you an idea, like when you run, I don't know, some trend platform on your website to see the, the, how it's doing, and well, that's free. Then the Free Forever version, it's like an adaptation of the original version of Personal, we take out, instead of giving you the full tool, we give you just the, the
scanning, of your website. And then, the community is open source. You have to install it, you have to know the terminal command and so on.
45:24 - Micaela Wasserman
Perfect. Perfect. Well, now with respect to everything that is internal, you internalize, inter, how do you say?
45:34 - Lourdes Medrano
Internalization.
45:34 - Micaela Wasserman
Internationalization of products and services. Well, you started in Argentina and, as you mentioned before, what is your decision when you want to enter a new market? I mean, does it depend on the customer's demand, there are customers from other markets that hire
you, so to speak, or do you have some kind of strategy, of alliances with other companies to
enter? It depends on the market and the barriers.
46:03 - Cecilia Garmendia
At the communication level is to find the pain that you have that Chile has a new cybersecurity law and well, we try to engage on that side to communicate and reach customers. Then there are the barriers that there are some countries that cannot hire international services, they need invoices, so there you operate with partners that help you to reach and generate greater penetration in the markets, but also in other things, or well, see how to... or put an office, so to speak. But at the communication level, in order to gain penetration, we look at what their pain is, and then there are, depending on the barriers we
have, whether or not we can reach that market. They can be barriers at the level of external
suppliers, they have that more in Latin America. They are very regulated to work with internal solutions and well, they start to have barriers every time they want an external solution. In our line of business, this has already been discussed because it is clear that a country can provide you with some solutions that have a more technological complexity, isn't
it? Or you have to look at it in dollars.
47:22 - Micaela Wasserman
Super, and do you have some kind of licensing type modality or...
47:26 - Cecilia Garmendia
We have a partner program when we work with partners and a referral program when a company comes for a partner or referrals. But then it is not a solution that we have to be patenting or generating international validations so that we can sell it as it can happen with hardware or something in between that you have to

comply with the requirements of that country. In software you don't have that, if it's healthy. Perfect.
48:01 - Micaela Wasserman
And then, changing the subject a little bit, with respect to the headquarters you have in the United States, do they work with the central headquarters, which coordinates with the Argentine headquarters, or is it because you had told us that it was a question that had been made for a reason, I don't know if it was a legal issue, but it was like they had to make
a headquarter in the United States?

48:26 - Unidentified Speaker
Claro.
48:26 - Cecilia Garmendia
When we attacked the U.S. market and we had to make a headquarter, because many of our
customers are there. But the headquarter is in Argentina and we are an Argentine company
that works abroad. And we have a headquarter in the United States, but we do not have today, for today, we do not have personnel there.
48:49 - Micaela Wasserman
OK. Excellent, well and going more to this communication issue, there are 11 left in the call
so if we can try to summarize, do you have to go or can you stay a little bit longer?
49:05 - Cecilia Garmendia
No, no, tell me, I have to go back to the agenda but let's use those 12 minutes and we'll stay for anything.
49:13 - Micaela Wasserman
Dale, excellent, well in terms of communication, from the company that you told them that they had had all these problems and so on. When you communicate in all the markets in which you operate, do you go for a standardized strategy or do you kind of adapt everything
in terms of communication? Also depending on, as you said, in the United States they are much more autonomous in providing perhaps less information. In other words, do you have a
strategy for all countries the same or do you use how you adapt it to each country?
49:43 - Cecilia Garmendia
No, we adapt it to each communication channel we use.
49:49 - Micaela Wasserman
And that is worked with. Perfect. And that's worked with internally. Because you said agencies used only for ads and so on.
49:58 - Cecilia Garmendia
Yes, we work internally, but as we have a strategy based on geographic segmentation, if we
are attacking Latin American countries, they envy us, we generate content, web pages and
things aimed at that market. And the same for the United States or other countries. You can
always go further down to the bone, but generally speaking

we try, at least apparently in those markets, to comply with good geographic segmentation behaviors.
50:28 - Unidentified Speaker
Excellent.
50:28 - Micaela Wasserman
And then, language-wise, they mostly use English, right? Like, most of the vocabulary that is
used is in English.
50:40 - Cecilia Garmendia
Yes, our communication is mainly in English. And as a second language and adapted when we do specific campaigns for Latin America, we do campaigns in Spanish. Or landing in Spanish or content in Spanish. Even today there is an issue at the level, important advance in terms of content. So, people are more permissive, except for the market, in the sense that if you put a video with a caption in Spanish, it does not generate rejection as it used to happen in other times. Although there are countries that are very

jealous of their language and that the content comes in their language, we try to do that more in the very mailing campaigns, which go directly to their mailbox.
51:29 - Micaela Wasserman
Perfect, perfect. Well, and then what we needed was if you had like the, organizational chart,
which we had talked about the other time, if you had some kind of structure, diagram, whatever it was to show us a little bit like the structure of the company at the organizational
level.
51:47 - Cecilia Garmendia
Yes, that is what I am sending them to you, and the human resources lady just shared one with me, but it seems to me that it is a little out of date, I will ask her to review it and I will share it with you and pass it on to you. I was looking at it to share it with you, but there are some things that are not updated. So well.
52:07 - Micaela Wasserman
Perfect, and one last question if we take advantage of these last eight minutes, maybe less,
is how, taking into account the whole macro environment and all the countries work in, nowadays with all the political and economic changes that are happening globally, is there any external factor, whether in Argentina or whatever, that is directly affecting you as a company? Is there anything that you highlight or that is relevant nowadays?
52:44 - Cecilia Garmendia
From my reading of the context, we are a company that our services are paid in dollars and
many times, or in pesos, depending, but well, the currency and currency fluctuations, sometimes positively and sometimes negatively affect the margins that the company manages and many of our resources are dollarized and well, that will also be a little complex, but nothing, we are not as conditioned as it has been in other companies in other industries out there,

by the country context in the Argentine case or by the context of some law that has arisen or
not.
53:29 - Unidentified Speaker
Super.
53:30 - Micaela Wasserman
Well, excellent. I think we are. Great. So, I owe you for the organization chart.
53:37 - Cecilia Garmendia
And whenever you want, write me and tell me what I can add. I hope I have not generated more confusion than answers.
53:47 - Micaela Wasserman
No, not at all. It is crystal clear.
53:50 - Lourdes Medrano
Thank you. No, no, no.
53:52 - Cecilia Garmendia
So nothing.
53:54 - Micaela Wasserman
For whatever you need they
are.
53:57 - Cecilia Garmendia
pass the companies in the chat before they leave, copy them and the link of the last video we made more allornado to the branding proposal we want to do now.
54:14 - Lourdes Medrano
Excellent. Well, thank you guys very much.

Annex 5: Government - Argentina[127]

Executive Power[128]

1. President: Javier Gerardo Milei
    1.1. Vice President: Victoria Eugenia Villarruel
        1.1.1. **General Secretary of the Presidency:** Karina Elizabeth Milei
            1.1.1.1. Undersecretary of Administrative Coordination Director: Esteban Bruno[129]
                1.1.1.1.1. General Director of IT and Telecommunications: Gustavo Marcelo Moccia[130]
                    1.1.1.1.1.1. Coordinator Communications and System: Emanuel Rufino[131]
                        1.1.1.1.1.1.1. Director of Information Security: Guido Paolini
                        1.1.1.1.1.1.2. Director of IT Management: Denis Fernando Romero[132]
        1.1.2. State Intelligence Secretariat: Sergio Darío Neiffert
            1.1.2.1. (SIA) Argentine Intelligence Service: Alejandro Walter Colombo
            1.2.2. (ASN) National Security Agency: Alejandro P. Cecati
            1.2.3. (AFC) Federal Cybersecurity Agency: Ariel Waissbein[133]

    1.2. **Chief Cabinet of Ministers:** Guillermo Alberto Francos
        1.2.1. Secretariat of Innovation, Science and Technology: Darío Leandro Genua
            1.2.1.1. Undersecretary of Information and Communications Technologies: César Leonardo Gazzo Huck

[127] *Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data.*
[128] Jefatura de Gabinete de Ministros. *Mapa del Estado* [online]. [Accessed 18 May 2025]. Available from: https://mapadelestado.jefatura.gob.ar/
[129] LinkedIn. (2025). Esteban Bruno – LinkedIn profile. LinkedIn. [Accessed 25 May 2025]. Available from: https://www.linkedin.com/in/esteban-bruno-722018115/
[130] LinkedIn. (2025). Gustavo Marcelo Moccia – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lic-gustavo-marcelo-moccia-89769a132/
[131] LinkedIn. (n.d.). Emanuel Rufino – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/emanuel-rufino-1a97428/
[132] LinkedIn. (n.d.). Denis Fernando Romero – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/denis-fernando-romero/?originalSubdomain=ar
[133] LinkedIn. (n.d.). Ariel Waissbein – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/arielwaissbein/

1.2.1.1.1. National Cybersecurity Director: Federico Sebastián Pierri[134]

1.2.1.1.1.1. Computer Systems and Network Security Prevention Director: Pablo Mariano Navarro[135]

1.2.1.1.2. Director National Information Technology Office: Emiliano Villa[136]

1.2.1.1.2.1. Director of Standards Development and Technological Opinions: Maximiliano Costantinis[137]

1.2.1.1.2.2. New Technologies Research Director: Rodrigo Alberto Pico[138]

1.2.1.2. Undersecretary of Innovation: Claudio Gustavo Wendler[139]

1.2.1.2.1. Director of Digitalization and Administrative Innovation: Rita Eugenia Dominguez Alonso

1.2.1.3. Undersecretary of Administrative Management of Innovation, Science and Technology: Diego Alejandro Nelli

1.2.1.3.1. Director of Infrastructure and Operations of Innovation, Science and Technology: Adrián Godoy[140]

1.2.1.3.2. Director of Information Systems for Innovation, Science, and Technology: Diego Alejandro López

1.2.2. **Minister of National Security:** Patricia Bullrich

1.2.2.1. Head of Advisory Cabinet Unit: Carlos Alberto Manfroni[141]

1.2.2.1.1. Administrative Coordination Office Secretary: Martín Siracusa[142]

---

[134]LinkedIn. Federico Pierri – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/federicopierri

[135]LinkedIn. (n.d.). P Navarro – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/pnavarro/

[136]LinkedIn. (n.d.). Emiliano Villa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/villaemiliano/

[137]LinkedIn. (n.d.). Maxi Costantinis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/maxicostantinis

[138]LinkedIn. (n.d.). Rodrigo Picó – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/rodrigo-pic%C3%B3-3160931b3/

[139]LinkedIn. (n.d.). Claudio G. Wendler – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://ar.linkedin.com/in/claudio-wendler-175035263

[140]LinkedIn. (n.d.). Adrian Godoy – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/adrian-godoy-b4b7a1120/

[141]LinkedIn. (n.d.). Carlos Manfroni – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/carlosmanfroni/

[142]LinkedIn. (n.d.). Martin Siracusa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/martinsiracusa/

1.2.2.1.1.1. Director of Information Technology: Jorge Adolfo Teodoro[143]

1.2.2.1.1.1.1. Information Systems Coordinator: Juan José Serventi[144]

1.2.2.1.1.1.2. Technological Infrastructure Coordinator: Miguel Ángel Casares[145]

1.2.2.1.2. Directorate of Cybercrime and Cyber Affairs: Santiago González Bellengeri[146]

1.2.2.1.2.1.

1.2.3. **Minister of Defense:** Luis Alfonso PETRI

1.2.3.1. Head of Advisory Cabinet Unit: Maria Luciana Carrasco[147]

1.2.3.1.1.1. Undersecretary of Administrative Management: Pablo Martín Costa[148]

1.2.3.1.1.1.1. Information Technology Department Director: Alina Silvia Di Lernia[149]

1.2.3.2. Secretariat of Strategy and Military Affairs: Marcelo Alejandro Rozas Garay

1.2.3.2.1. Undersecretary of Cyber Defense: Alberto Luciano Mario Corvalán

1.2.3.2.1.1. Director of Cyber Defense Coordination: José Gustavo Oyadomari

1.2.3.2.1.2. Director of the Cyber Defense System: Ernesto Claudio Balloffet[150]

1.2.4. **Ministry of Human Capital:** Sandra Viviana Pettovello[151]

---

[143]LinkedIn. (n.d.). Jorge A. Teodoro – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jorge-teodoro-7990485/

[144]LinkedIn. (n.d.). Juan José Serventi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-jose-serventi-48308210/

[145]LinkedIn. (n.d.). Miguel Ángel Casares – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/miguel-angel-casares-ab149716/

[146]LinkedIn. (n.d.). Santiago González Bellengeri – LinkedIn profile. LinkedIn. [Accessed 29 May 2025]. Available from: https://www.linkedin.com/in/santiago-gonz%C3%A1lez-bellengeri-07386714/?originalSubdomain=ar

[147]LinkedIn. (n.d.). María Luciana Carrasco – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/mar%C3%ADa-luciana-carrasco-b185aa228/?originalSubdomain=ar

[148]LinkedIn. (n.d.). Pablo Martín Costa – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/pablo-mart%C3%ADn-costa-4034a9118/?originalSubdomain=ar

[149]LinkedIn. (n.d.). Alina Silvia Di Lernia – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/alina-di-lernia-a2849816/?originalSubdomain=ar

[150]LinkedIn. (n.d.). Ernesto Claudio Balloffet – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/ernesto-claudio-balloffet-a64177252/

[151]LinkedIn. (n.d.). Sandra Pettovello – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/sandra-pettovello-243328a/

1.2.4.1. Secretariat of Legal and Administrative Coordination: Juan Facundo Etchenique[152]

1.2.4.1.1. General Director of Document Management, Integrity, and Transparency: Mauro Esteban Brandi[153]

1.2.4.1.2. Undersecretary of Administrative Management: Alejandro Gabriel Schiavi[154]

1.2.4.1.2.1. Director of Information and Cybersecurity Systems: Vacant

1.2.4.2. Secretary of Education: Dr. Carlos Horacio Torrendell[155]

1.2.4.2.1. Undersecretary of University Policies: Alejandro Ciro Alvarez

1.2.4.2.1.1. National Director for the Strengthening of University Technological Infrastructure: Fernando Figueira Lemos

1.2.4.2.2. Undersecretary of Educational Policy and Innovation: Alfredo Domingo Vota

1.2.4.2.2.1. Director of National Institute of Technological Education: Jorge Ludovico Grillo

1.2.5. **Ministry of Economy:** Luis Andrés Caputo

1.2.5.1. Secretary for Small and Medium Enterprises, Entrepreneurs and Knowledge Economy: Marcos Ayerra[156]

1.2.5.1.1. Undersecretary for Small and Medium Enterprise: Christian Federico Bauab[157]

1.2.5.1.2. Undersecretary for Knowledge Economy: Santiago Roberto Pordelanne[158]

1.2.6. **Ministry of Justice:** Mariano Cúneo Libarona

[152]LinkedIn. (n.d.). Juan Facundo Etchenique – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-facundo-etchenique-86034155/

[153]LinkedIn. (n.d.). Mauro Brandi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mauro-brandi-b36b1b10/

[154]LinkedIn. (n.d.). Alejandro Schiavi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/alejandroschiavi/

[155]LinkedIn. (n.d.). Carlos Horacio Torrendell – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/carlos-horacio-torrendell-ab4939142/

[156]LinkedIn. (n.d.). Marcos Ayerra – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/marcos-ayerra-8317b634/

[157]LinkedIn. (n.d.). Christian Bauab – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christianbauab/

[158]LinkedIn. (n.d.). Santiago Pordelanne – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/santiagopordelanne/

1.2.6.1.1. General Director of Information and Telecommunications Technologies: Juan Antonio Franchino

1.2.6.1.2. Director of Systems: Cristian Gastón Verzi[159]

1.2.6.1.3. Director of Technology and Security: José Núnez

Legislative Power

2. **Chamber of Deputies**[160]

2.1. President of Science, Technology and Productive Innovation Commision[161]: Daniel Gollán

2.2. Administrative Chief of National Defense Commission[162]: Juan Pedro Gardes

2.3. Administrative Chief Consumer Defense, User Rights and Competition Commission[163]: Fabio Guanca Jaimes[164]

3. **Senate of the Nation**[165]

3.1. President of Unicameral Committee on Science and Technology[166]: Silvina Marcela García Larraburu[167]

3.1.1. President of National Agency for the Promotion of Research, Technological Development, and Innovation[168]: Natalia Irene Avendaño[169]

---

[159]LinkedIn. (n.d.). Cristian Gastón Verzi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/cristian-gast%C3%B3n-verzi-28128132/

[160]Honorable Cámara de Diputados de la Nación Argentina. *Comisiones Permanentes* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/

[161]Honorable Cámara de Diputados de la Nación Argentina. *Comisión de Ciencia, Tecnología e Innovación Productiva* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/ccytecnologia

[162]Honorable Cámara de Diputados de la Nación Argentina. *Comisión de Defensa Nacional* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/cdnacional

[163]Honorable Cámara de Diputados de la Nación Argentina. *Comisión de Defensa del Consumidor, del Usuario y de la Competencia* [online]. [Accessed 17 May 2025]. Available from: https://www.hcdn.gob.ar/comisiones/permanentes/cdconsumidor

[164]LinkedIn. (n.d.). Fabio Guanca Jaimes – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/fabio-guanca-jaimes-7bb1451b8/

[165]Honorable Senado de la Nación Argentina. *Comisiones* [online]. [Accessed 17 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/?lista=comision

[166]Honorable Senado de la Nación Argentina. *Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión* [online]. [Accessed 17 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/info/74

[167]LinkedIn. (n.d.). S. García Larraburu – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/garcialarraburu/

[168]Presidencia de la Nación Argentina. *Agencia Nacional de Promoción de la Investigación, el Desarrollo Tecnológico y la Innovación (Agencia I+D+i)* [online]. [Accessed 19 May 2025]. Available from: https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/agencia

[169]LinkedIn. (n.d.). Natalia I. Avendaño – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/nataliaiavendano/

3.1.1.1. President Scientific and Technological Research Fund[170] (FONCYT): Rita Antonella Cuevas[171]

3.1.1.2. (FONARSEC) President Argentine Sectoral Fund[172]: Laura Andrea Toledo[173]

3.2. President Unicameral Committee on Systems, Media, and Freedom of Expression[174]: Eduardo Kueider

3.2.1. President of Federal Council for Transparency[175]: Beatriz Anchorena[176]

3.2.1.1.1. Director Committee on Transparency: Biffi, Facundo[177]

Regulatory entities

4. National Regulatory Authorities

4.1. (IRAM) Instituto Argentino de Normalización y Certificación[178]

4.1.1. President: Claudio Terrés[179]

4.2. (AAIP) Agencia de Acceso a la Información Pública

4.2.1. Director: Beatriz Anchorena[180]

4.3. (ENACOM) Ente Nacional de Comunicaciones[181]

4.3.1. Interventor: Juan Martín Ozores[182]

---

[170]Ministerio de Ciencia, Tecnología e Innovación de la Nación Argentina. *Fondo para la Investigación Científica y Tecnológica (FONCYT)* [online]. [Accessed 25 May 2025]. Available from: https://www.argentina.gob.ar/ciencia/agencia/fondo-para-la-investigacion-cientifica-y-tecnologica-foncyt

[171]LinkedIn. (n.d.). Rita Cuevas – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/rita-cuevas/

[172]Ministerio de Ciencia, Tecnología e Innovación de la Nación Argentina. *Fondo Argentino Sectorial (FONARSEC)* [online]. [Accessed 20 May 2025]. Available from: https://www.argentina.gob.ar/ciencia/agencia/fondo-argentino-sectorial-fonarsec

[173]LinkedIn. (n.d.). Laura Toledo – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/laura-toledo-331030114/

[174]Honorable Senado de la Nación Argentina. *Comisión de Ciencia y Tecnología* [online]. [Accessed 20 May 2025]. Available from: https://www.senado.gob.ar/parlamentario/comisiones/info/68

[175]Federal Council for Transparency (CFT). *Portal of the Federal Council for Transparency* [online]. [Accessed 1 June 2025]. Available from: https://portalconsejofederal.transparencia.gob.ar/

[176]LinkedIn. (n.d.). Beatriz Anchorena – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/beatrizanchorena/

[177]LinkedIn. (n.d.). Facundo Biffi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/facundo-biffi-947375244/

[178]Instituto Argentino de Normalización y Certificación (IRAM). *Official website of the Argentine Institute of Standardization and Certification* [online]. [Accessed 1 June 2025]. Available from: https://www.iram.org.ar/

[179]LinkedIn. (n.d.). Claudio Terrés – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/claudioterres/

[180]LinkedIn. (n.d.). Beatriz Anchorena – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/beatrizanchorena/

[181]National Communications Entity (ENACOM). *Official website of the National Communications Entity* [online]. [Accessed 1 June 2025]. Available from: https://www.enacom.gob.ar/

[182]LinkedIn. (n.d.). Juan Martín Ozores – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/juan-martin-ozores-5b055617/

Annex 6: Government - United States[183]

Executive Branch[184]

1. President: Donald J. Trump

1.1. Vice President: James David Vance

1.1.1.1. (ONCD) Office of the National Cyber Director[185]

1.1.1.1.1. Director of the Office of the National Cyber Director: Harry Coker Jr.

1.1.2. The Cabinet[186]

1.1.2.1. (DHS) Department of Homeland Security[187]

1.1.2.1.1.1. Secretary of Homeland Security: Kristi Noem

1.1.2.1.2. **(CISA) Cybersecurity and Infrastructure Security Agency**[188]

1.1.2.1.2.1. Acting Director: Dr. Madhu Gottumukkal

1.1.2.1.2.2. Executive Director: Bridget Bean[189]

1.1.2.1.2.3. Executive Assistant Director for Cybersecurity: Karen S. Evans[190]

1.1.2.1.3. (FEMA) Federal Emergency Management Agency[191]

1.1.2.1.3.1. Federal Emergency Management Agency (FEMA) Administrator: Deanne Criswell[192]

---

[183] Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data.

[184]THE WHITE HOUSE. *The Administration* [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/administration/

[185]WHITE HOUSE OFFICE OF THE NATIONAL CYBER DIRECTOR. *Office of the National Cyber Director*. The White House [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/oncd/

[186]THE WHITE HOUSE. *The Cabinet* [online]. [Accessed 19 May 2025]. Available from: https://www.whitehouse.gov/administration/the-cabinet/

[187]U.S. DEPARTMENT OF HOMELAND SECURITY. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.dhs.gov/leadership

[188]CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.cisa.gov/about/leadership

[189]LinkedIn. (n.d.). Bridget Bean – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/bridget-bean/

[190]LinkedIn. (n.d.). K. S. Evans – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/karensevans/

[191]FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA). *Official website of FEMA* [online]. [Accessed 19 May 2025]. Available from: https://www.fema.gov/

[192]LinkedIn. (n.d.). D. Criswell – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/deanne-criswell-862bb2a/

1.1.2.1.4. U.S. Secret Service[193]

1.1.2.1.4.1. Director of the U.S. Secret Service: Sean M. Curran

1.1.2.1.4.2. Deputy Director of the U.S. Secret Service: Matthew C. Quinn

1.1.2.1.4.3. Chief Operating Officer of the U.S. Secret Service: Cynthia Sjoberg Radway[194]

1.1.2.1.5. Science and Technology Directorate

1.1.2.1.5.1. Secretary for Science and Technology: Julie S. Brewer

1.1.2.2. Defense Department

1.1.2.2.1. Secretary of Defense: Pete Hegseth[195]

1.1.2.2.2. Office of the Under Secretary of Defense for Intelligence & Security[196]

1.1.2.2.2.1. Under Secretary of Defense for Intelligence & Security: Dustin Gard-Weiss[197]

1.1.2.2.3. USCYBERCOM – U.S. Cyber Command[198]

1.1.2.2.3.1. Commander: William J. Hartman

1.1.2.2.3.2. Deputy Commander: Dennis Velez[199]

1.1.2.2.3.3. Executive Director: Morgan Adamski[200]

1.1.2.2.3.4. Chief of Staff: Kenneth J. Burgess

1.1.2.2.3.5. Senior Enlisted Leader: Kenneth M. Bruce, Jr.

---

[193]UNITED STATES SECRET SERVICE. *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.secretservice.gov/about/leadership

[194]LinkedIn. (n.d.). Cynthia S. – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/cynthia-s-4793949/

[195]U.S. SENATE, COMMITTEE ON THE JUDICIARY. *Official website of the Committee on the Judiciary* [online]. [Accessed 23 May 2025]. Available from: https://www.judiciary.senate.gov

[196]OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (OUSD[I&S]). *Official website of OUSD(I&S)* [online]. [Accessed 19 May 2025]. Available from: https://ousdi.defense.gov/

[197]LinkedIn. (n.d.). Dustin Gard-Weiss – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dustin-gard-weiss-4323121/

[198]U.S. CYBER COMMAND. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.cybercom.mil/Leadership/

[199]LinkedIn. (n.d.). Dennis Velez – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dennis-velez-39562515/

[200]LinkedIn. (n.d.). Morgan Adamski – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/morgan-adamski-501094240/

1.1.2.3. Department of Justice[201]

1.1.2.3.1. Attorney General: Pamela Bondi

1.1.2.3.2. Deputy Attorney General: Todd Blanche[202]

1.1.2.4. Department of Commerce[203]

1.1.2.4.1. Secretary of Commerce: Howard Lutnick[204]

1.1.2.4.1.1. Acting General Counsel: John K. Guenther[205]

1.1.2.4.1.2. Director of the Bureau of Economic Analysis: Vipin Arora

1.1.2.4.2. (NIST) National Institute of Standards and Technology[206]

1.1.2.4.2.1. Deputy Director: Craig Burkhardt

1.1.2.4.2.2. Director for Innovation and Industry Services: Eric Lin.

1.1.2.4.3. (NTIA) National Telecommunications and Information Administration[207]

1.1.2.4.3.1. Deputy Administrator of the National Telecommunications and Information Administration (NTIA): Adam Cassady

1.1.2.4.3.1.1. Deputy Assistant Secretary for Operations and Administration: Karin O'Leary[208]

1.1.2.5. Department of Energy[209]

1.1.2.5.1. Secretary of Energy: Chris Wright

---

[201]U.S. DEPARTMENT OF JUSTICE. *Organizational Chart* [online]. [Accessed 2 June 2025]. Available from: https://www.justice.gov/agencies/chart/map

[202]LinkedIn. (n.d.). Todd Blanche – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/toddblanche/

[203]U.S. DEPARTMENT OF COMMERCE. *Leadership* [online]. [Accessed 2 June 2025]. Available from: https://www.commerce.gov/about/leadership

[204]LinkedIn. (n.d.). Howard W. Lutnick – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/howardwlutnick/

[205]LinkedIn. (n.d.). John K. Guenther – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/john-k-guenther-a44321174/

[206]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.nist.gov/director/leadership

[207]U.S. DEPARTMENT OF COMMERCE. *Leadership* [online]. [Accessed 19 May 2025]. Available from: https://www.commerce.gov/about/leadershi

[208]LinkedIn. (n.d.). Karin O Leary – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/karin-o-leary-20233a101

[209]U.S. DEPARTMENT OF ENERGY. *Our Leadership & Offices* [online]. [Accessed 2 June 2025]. Available from: https://www.energy.gov/our-leadership-offices

1.1.2.5.1.1. (CESER) Office of Cybersecurity, Energy Security, and Emergency Response[210]

1.1.2.5.1.1.1. Director: Alex Fitzsimmons[211]

1.1.2.5.1.1.2. Principal Deputy Director: Lili Colon[212]

1.1.2.5.1.1.3. Deputy Director, Preparedness, Policy, and Risk Analysis: Mara Winn[213]

Legislative Branch

2. House of Representatives

2.1. Committee on Homeland Security[214]: Mark Green / (202) 226-8417

2.1.1. Cybersecurity and Infrastructure Protection Subcommittee: Andrew Garbarino

2.1.2. The Emergency Management and Technology Subcommittee: Dale, Strong

2.1.3. Counterterrorism and Intelligence Subcommittee: August Pflunger

2.2. Committee on Oversight and Accountability[215]: James Comer

2.2.1. Cybersecurity, Information Technology, and Government Innovation: Nancy Mace[216]

2.3. Committee on Science, Space, and Technology[217]: Brian Balbin

2.3.1. Research and Technology Subcommittee: Jay Obernolte[218]

2.3.2. Investigations and Oversight Subcommittee: Rick McCormick

---

[210]U.S. DEPARTMENT OF ENERGY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE (CESER). *CESER Leadership* [online]. [Accessed 21 May 2025]. Available from: https://www.energy.gov/ceser/ceser-leadership

[211]LinkedIn. (n.d.). Alex Fitzsimmons – LinkedIn profile. LinkedIn. [Accessed 29 May 2025]. Available from: https://www.linkedin.com/in/alexfitzsimmons/

[212]LinkedIn. (n.d.). Lili Colon – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/lilicolon/

[213]LinkedIn. (n.d.). Mara Winn – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/marabishopwinn/

[214]U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY. *Official website of the Committee on Homeland Security* [online]. [Accessed 24 May 2025]. Available from: https://homeland.house.gov/

[215]U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY. *Official website of the Committee on Oversight and Accountability* [online]. [Accessed 21 May 2025]. Available from: https://oversight.house.gov/

[216]LinkedIn. (n.d.). Nancy Mace – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/macenancy/

[217]U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY. *Official website of the Committee on Science, Space, and Technology* [online]. [Accessed 21 May 2025]. Available from: https://science.house.gov/

[218]LinkedIn. (n.d.). Jay Obernolte – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/jayobernolte/

2.4. Committee on Energy and Commerce[219]: Brett Guthrie

2.4.1. Subcommittee on Communications and Technology: Richard Hudson

3. Senate

3.1. Homeland Security and Governmental Affairs Senate Committee[220]: Paul Rand[221]

3.1.1. Subcommittee on Emerging Threats and Spending Oversight: Margaret Wood Hassan

3.2. Commerce, Science, and Transportation Senate Committee[222]: Ted Cruz[223]

3.2.1. Consumer Protection, Technology, and Data Privacy Subcommittee: Marsha Blackburn[224], Tenn

3.2.2. Telecommunications and Media Subcommittee: Deb Fischer, Neb[225]

3.3. Senate Select Committee on Intelligence[226]: Tom Cotton[227]

3.4. Senate Judiciary Committee[228]: Chuck Grassley[229]

3.4.1. Subcommittee on Privacy, Technology, and the Law: Marsha Blackburn[230]

3.4.2. Subcommittee on Intellectual Property: Thom Tillis[231], Chai

Regulatory bodies

4. National Regulatory Authorities

---

[219]U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON ENERGY AND COMMERCE. *Official website of the Committee on Energy and Commerce* [online]. [Accessed 21 May 2025]. Available from: https://energycommerce.house.gov/

[220]U.S. SENATE, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS. *History* [online]. [Accessed 26 May 2025]. Available from: https://www.hsgac.senate.gov/about/history/

[221]LinkedIn. (n.d.). Paul Rand – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/in/drrandpaul/.

[222]U.S. SENATE, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION. *Official website of the Committee on Commerce, Science, and Transportation* [online]. [Accessed 23 May 2025]. Available from: https://www.commerce.senate.gov/

[223]LinkedIn. (n.d.). Ted Cruz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/cruzted/

[224]LinkedIn. (n.d.). Marsha Blackburn – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/senator-marsha-blackburn/

[225]LinkedIn. (n.d.). Deb Fischer – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/company/u-s-senator-deb-fischer/

[226]U.S. SENATE, SELECT COMMITTEE ON INTELLIGENCE. *Official website of the Select Committee on Intelligence* [online]. [Accessed 23 May 2025]. Available from: https://www.intelligence.senate.gov/

[227]U.S. SENATE, OFFICE OF SENATOR TOM COTTON. *Official website of Senator Tom Cotton* [online]. [Accessed 2 June 2025]. Available from: https://www.cotton.senate.gov/

[228]U.S. SENATE, COMMITTEE ON THE JUDICIARY. *Official website of the Committee on the Judiciary* [online]. [Accessed 23 May 2025]. Available from: https://www.judiciary.senate.gov/

[229]U.S. SENATE, OFFICE OF SENATOR CHUCK GRASSLEY. *Official website of Senator Chuck Grassley*[online]. [Accessed 2 June 2025]. Available from: https://www.grassley.senate.gov/

[230]LinkedIn. (n.d.). Marsha Blackburn – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/senator-marsha-blackburn/.

[231]LinkedIn. (n.d.). Thom Tillis – LinkedIn profile. LinkedIn. [Accessed May 29, 2025]. Available from: https://www.linkedin.com/in/thomtillis/

4.1. (NCCoE) National Cybersecurity Center of Excellence[232]: Cherilyn Pascoe[233]

4.2. (FedRAMP) Federal Risk and Authorization Management Program[234]: Pete Waterman[235]

4.3. (TTS) Technology Transformation Services[236]: Thomas Shedd

4.4. (FFRDC) National Cybersecurity Federally Funded Research and Development Center[237]: Beth Meinert[238]

4.5. (FTC) Federal Trade Commission[239]

4.5.1. Chief Technology Officer: Jake Denton[240]

4.6. (ONCD) Office of the National Cyber

4.6.1. Director: Harry Coker Jr.[241]

4.7. (FISMA) Federal Information Security Management Act

Annex 7: Government - Germany[242]

Executive Branch

1.1. Chancellery[243]

1.1.1. Federal Chancellor of the Federal Republic of Germany: Friedrich Merz[244]

1.1.1.1. Head of the Federal Chancellery and Federal Minister for

[232]NATIONAL CYBERSECURITY CENTER OF EXCELLENCE. *National Cybersecurity Center of Excellence (NCCoE)*. National Institute of Standards and Technology (NIST). [n.d.] [Accessed 14 June 2025]. Available from: https://www.nccoe.nist.gov/

[233]LinkedIn. (n.d.). Cherilyn Pascoe – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/cherilynpascoe/.

[234]U.S. GENERAL SERVICES ADMINISTRATION (GSA). *FedRAMP: Federal Risk and Authorization Management Program*. [n.d.] [Accessed 28 May 2025]. Available from: https://www.fedramp.gov/

[235]LinkedIn. (n.d.). Pete Waterman – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/petewaterman/.

[236]U.S. GENERAL SERVICES ADMINISTRATION (GSA). *Technology Transformation Services*. [n.d.] [Accessed 1 June 2025]. Available from: https://tts.gsa.gov/

[237]MITRE CORPORATION. *National Cybersecurity FFRDC*. [n.d.] [Accessed 2 June 2025]. Available from: https://www.mitre.org/our-impact/rd-centers/national-cybersecurity-ffrdc

[238]LinkedIn. (n.d.). Beth Meinert – LinkedIn profile. LinkedIn. [Accessed May 26, 2025]. Available from: https://www.linkedin.com/in/beth-meinert-95ab832a/.

[239]FEDERAL TRADE COMMISSION (FTC). *About the FTC*. [n.d.] [Accessed 1 June 2025]. Available from: https://www.ftc.gov/about-ftc

[240]LinkedIn. (n.d.). Jake Denton – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/thejakedenton/.

[241]LinkedIn. (n.d.). Harry Coker – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/harry-coker-4263979/.

[242] *Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data.*

[243]FEDERAL CHANCELLERY OF GERMANY. *Federal Chancellors since 1949. Berlin: Press and Information Office of the Federal Government.* [n.d.] [Accessed 1 June 2025]. Available from: https://www.bundeskanzler.de/bk-en/chancellery/federal-chancellors-since-1949

[244]Bundestag. (n.d.). Friedrich Merz – Bundestag profile. Bundestag. [Accessed June 1, 2025]. Available from: https://www.bundestag.de/abgeordnete/biografien/M/merz_friedrich-1046080

Special Tasks: Wolfgang Schmidt[245]

1.2. Federal Ministry of the Interior[246]

1.2.1. Federal Minister of the Interior: Alexander Dobrindt

1.2.1.1. State Secretaries: Hans-Georg Engelke

1.2.1.2. State Secretaries: Bernd Krösser

1.2.1.2.1. Parliamentary State Secretary: Christoph De Vries[247]

1.2.1.2.2. Parliamentary State Secretary: Daniela Ludwig[248]

Legislative Branch

2. Bundestag (Federal Parliament)[249]

2.1. President of the Bundestag: Julia Klöckner (CDU/CSU)[250]

2.1.1. Vice-President of the Bundestag: Andrea Lindholz (CDU/CSU)[251]

2.1.2. Vice-President of the Bundestag: Josephine Ortleb (SPD)[252]

2.1.3. Vice-President of the Bundestag: Omid Nouripour (Alliance 90/The Greens)[253]

2.1.4. Vice-President of the Bundestag: Bodo Ramelow (The Left Party)

3. Bundesrat (Federal Council)[254]

3.1. President of the: Anke Rehlinger

3.1.1. First Vice President of the Federal Council: Manuela Schwesig

3.1.1.1. Second Vice President of the Federal Council: Dr. Andreas

---

[245]LinkedIn. (n.d.). Wolfgang Schmidt – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/wolfgang-schmidt-18213b4/

[246]FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY (BMI). *Leadership. Berlin: Federal Ministry of the Interior and Community.* [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmi.bund.de/DE/ministerium/leitung/leitung-node.html

[247]LinkedIn. (n.d.). Christoph de Vries – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/christoph-de-vries-89684a1b2/

[248]LinkedIn. (n.d.). Daniela Ludwig - LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/daniela-ludwig-400873240/

[249]GERMAN BUNDESTAG. *Wolfgang Schäuble elected new President of the Bundestag*. Berlin: German Bundestag, 24 October 2017 [Accessed 1 June 2025]. Available from: https://www.bundestag.de/en/documents/textarchive/constituent-sitting-529998

[250]LinkedIn. (n.d.). Julia Klöckner – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/julia-kl%C3%B6ckner-0a751923a/

[251]LinkedIn. (n.d.). Andrea Lindholz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/andrea-lindholz-891310250/

[252]LinkedIn. (n.d.). Josephine Ortleb – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/josephineortleb/

[253]LinkedIn. (n.d.). Omid Nouripour – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/nouripour/

[254]GERMAN BUNDESRAT. *President and Presidium*. Berlin: German Bundesrat. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bundesrat.de/DE/bundesrat/praesidium/praesidium-node.html

Bovenschulte[255]

3.2. Chancellery[256]

3.2.1. Federal Chancellor of the Federal Republic of Germany: Friedrich Merz[257]

3.2.1.1. Head of the Federal Chancellery and Federal Minister for Special Tasks: Wolfgang Schmidt[258]

3.3. Federal Ministry of the Interior[259]

3.3.1. Federal Minister of the Interior: Alexander Dobrindt

3.3.1.1. State Secretaries: Hans-Georg Engelke

3.3.1.2. State Secretaries: Bernd Krösser

3.3.1.2.1. Parliamentary State Secretary: Christoph De Vries[260]

3.3.1.2.2. Parliamentary State Secretary: Daniela Ludwig[261]

3.4. **Federal Ministry of Defense[262]**

3.4.1. Federal Minister of Defense: Boris Pistorius

3.4.2. State Secretary in the Federal Ministry of Defense: Benedict Zimmer

3.4.3. State Secretary in the Federal Ministry of Defense: Nils Hilmer[263]

3.4.3.1. Parliamentary State Secretary to the Federal Minister of Defence: Sebastian Hartmann[264]

3.4.3.2. Parliamentary State Secretary to the Federal Minister of Defence: Nils Schmid

---

[255]LinkedIn. (n.d.). Andreas Bovenschulte – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/andreas-bovenschulte-a0b24a65/

[256]FEDERAL CHANCELLERY OF GERMANY. *Federal Chancellors since 1949*. Berlin: Press and Information Office of the Federal Government. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bundeskanzler.de/bk-en/chancellery/federal-chancellors-since-1949

[257]LinkedIn. (n.d.). Friedrich Merz – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/friedrich-merz/

[258]LinkedIn. (n.d.). Wolfgang Schmidt – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/wolfgang-schmidt-18213b4/

[259]FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY (BMI). *Leadership*. Berlin: Federal Ministry of the Interior and Community. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmi.bund.de/DE/ministerium/leitung/leitung-node.html

[260]LinkedIn. (n.d.). Christoph de Vries – LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/christoph-de-vries-89684a1b2/

[261]LinkedIn. (n.d.). Daniela Ludwig – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/daniela-ludwig-400873240/

[262]FEDERAL MINISTRY OF DEFENCE (BMVg). *Federal Ministry of Defence*. Berlin: Federal Ministry of Defence. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmvg.de/de/ministerium

[263]LinkedIn. (n.d.). Nils Hillmer – LinkedIn profile. LinkedIn. [Accessed June 3, 2025]. Available from: https://www.linkedin.com/in/nils-hillmer-061433127/?originalSubdomain=de

[264]LinkedIn. (n.d.). Sebastian Hartmann – LinkedIn profile. LinkedIn. [Accessed May 30, 2025]. Available from: https://www.linkedin.com/in/sebastian-hartmann-b79073bb/

3.5. **Federal Ministry for Economic Affairs and Energy**[265]

3.5.1. Federal Minister for Economic Affairs and Energy: Katherina Reiche

3.5.2. [266]State Secretary: Frank Günter Wetzel

3.5.3. State Secretary: Bernhard Kluttig[267]

3.5.3.1. Parliamentary State Secretary: Gitta Connemann

3.5.3.2. Parliamentary State Secretary: Stefan Rouenhoff[268]

3.6. **Federal Ministry of Research, Technology and Space**[269]

3.6.1. Federal Minister for Research, Technology and Space: Dorothee Bär[270]

3.6.2. Parliamentary State Secretary: Silke Launert[271]

3.6.3. Parliamentary State Secretary Matthias Hauer[272]

3.7. **Federal Ministry of Finance**[273]

3.7.1. Federal Minister of Finance: Lars Klingbeil[274]

3.7.2. State Secretary: Björn Böhning[275]

3.7.3. State Secretary: Rolf Bösinger[276]

3.7.4. State Secretary: Steffen Meyer[277]

3.7.5. State Secretary: Jeanette Schwamberger

---

[265]FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION (BMWK). *Federal Ministry for Economic Affairs and Climate Action*. Berlin: Federal Ministry for Economic Affairs and Climate Action. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmwk.de/Navigation/DE/Home/home.html

[266]LinkedIn. (n.d.). Katharina Reiche – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/katharina-reiche-0aa257163/

[267]LinkedIn. (n.d.). Bernhard Klutting – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/bernhard-kluttig-002802225/

[268]LinkedIn. (n.d.). Stefan Rouenhoff – LinkedIn profile. LinkedIn. [Accessed June 2, 2025]. Available from: https://www.linkedin.com/in/stefan-rouenhoff-82414b18/

[269]FEDERAL MINISTRY OF EDUCATION AND RESEARCH (BMBF). *Leadership*. Berlin: Federal Ministry of Education and Research. [n.d.] [Accessed 1 June 2025]. Available from: https://www.bmbf.de/DE/Ministerium/Hausleitung/hausleitung_node.html

[270]LinkedIn. (n.d.). Dorothee Bär – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/dorobaer/

[271]LinkedIn. (n.d.). Silke Launert – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/silkelaunert/

[272]LinkedIn. (n.d.). Matthias Hauer – LinkedIn profile. LinkedIn. [Accessed June 1, 2025]. Available from: https://www.linkedin.com/in/matthias-hauer-616471172

[273]FEDERAL MINISTRY OF EDUCATION AND RESEARCH (BMBF). *Leadership*. Berlin: Federal Ministry of Education and Research. [Accessed 1 June 2025]. Available from: https://www.bmbf.de/DE/Ministerium/Hausleitung/hausleitung_node.html

[274]LinkedIn. (n.d.). Lars Klingbeil – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/lars-klingbeil/

[275]LinkedIn. (n.d.). Björn Böhning – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/bj%C3%B6rn-b%C3%B6hning-84507a180/

[276]LinkedIn. (n.d.). Rolf Bösinger – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/rolf-b%C3%B6singer-9a1513174/

[277]LinkedIn. (n.d.). Steffen Meyer – LinkedIn profile. LinkedIn. [Accessed 31 May 2025]. Available from: https://www.linkedin.com/in/steffen-meyer-226479157/

3.7.5.1. Parliamentary State Secretary: Dennis Rohde[278]

3.7.5.2. Parliamentary State Secretary: Michael Schrodi[279]

3.8. **Federal Ministry of Justice and Consumer Protection**[280]

3.8.1. Federal Minister of Justice and Consumer Protection: Stefanie Hubig

3.8.2. State Secretary: Eva Schmierer[281]

3.8.2.1. Permanent Representative of the State Secretary: Johannes Dimroth[282]

3.8.2.2. Parliamentary State Secretary: Anette Kramme[283]

3.8.2.3. Parliamentary State Secretary: Frank Schwabe[284]

3.9. **Federal Foreign Office**[285]

3.9.1. Federal Minister of Foreign Affairs: Johann Wadephul[286]

3.9.2. Minister Of State For Europe: Gunther Krichbaum[287]

3.9.3. Minister Of State: Florian Hahn[288]

3.9.4. Minister Of State: Serap Güler[289]

3.9.4.1. State Secretary: Bernhard Kotsch

3.9.4.2. State Secretary: Géza Andreas Von Geyr

[278]LinkedIn. (n.d.). Dennis Rohde – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dennis-rohde-0a6a381b0/

[279]LinkedIn. (n.d.). Michael Schrodi – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/michael-schrodi-b1a64b134/

[280]FEDERAL MINISTRY OF JUSTICE AND CONSUMER PROTECTION (BMJV). *Leadership*. Berlin: Federal Ministry of Justice and Consumer Protection. [Accessed 1 June 2025]. Available from: https://www.bmj.de/DE/ministerium/hausleitung/hausleitung_node.html

[281]LinkedIn. (n.d.). Eva Schmierer – LinkedIn profile. LinkedIn. [Accessed 31 May 2025]. Available from: https://www.linkedin.com/in/eva-schmierer-abb791186/

[282]LinkedIn. (n.d.). Johannes Dimroth – LinkedIn profile. LinkedIn. [Accessed 28 May 2025]. Available from: https://www.linkedin.com/in/johannes-dimroth-11259a318/

[283]LinkedIn. (n.d.). Anette Kramme – LinkedIn profile. LinkedIn. [Accessed 24 May 2025]. Available from: https://www.linkedin.com/in/anette-kramme-bb428ab6/

[284]LinkedIn. (n.d.). Frank Schwabe – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/frank-schwabe-738b8741

[285]FEDERAL FOREIGN OFFICE. *Leadership*. Berlin: Federal Foreign Office. [Accessed 1 June 2025]. Available from: https://www.auswaertiges-amt.de/en/about-us/leadership-federal-foreign-office

[286]LinkedIn. (n.d.). Johann Wadephul – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/johann-wadephul-a09861a3/

[287]LinkedIn. (n.d.). Gunther Krichbaum – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: https://www.linkedin.com/in/gunther-krichbaum-49a76b345/

[288]LinkedIn. (n.d.). Florian Hahn – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/florian-hahn-3290541a0/

[289]LinkedIn. (n.d.). Serap Güler – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/serap-g%C3%BCler-34a728228/

3.10. **Federal Ministry for Economic Cooperation and Development**[290]

3.10.1. Federal Minister for Economic Cooperation and Development: Reem Alabali-Radovan[291]

3.10.2. State Secretary in the Federal Ministry for Economic Cooperation and Development: Niels Annen

3.10.2.1. Parliamentary State Secretary at the Federal Ministry for Economic Cooperation and Development: Bärbel Kofler[292]

3.10.2.2. Parliamentary State Secretary at the Federal Ministry for Economic Cooperation and Development: Johann Saathoff[293]

3.11. **Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety**[294]

3.11.1. Federal Minister of Environment, Climate Action, Nature Conservation and Nuclear Safety: Carsten Schneider[295]

3.11.2. State Secretary: Jochen Flasbarth[296]

3.11.2.1. Parliamentary State Secretary: Rita Schwarzelühr-Sutter[297]

3.11.2.2. Parliamentary State Secretary: Carsten Träger

3.12. **Federal Ministry of Education, Family, Senior Citizens, Women and Youth**[298]

3.12.1. Federal Minister of Education, Family Affairs, Senior Citizens,

---

[290]FEDERAL MINISTRY FOR ECONOMIC COOPERATION AND DEVELOPMENT (BMZ). *Leadership* [online]. Berlin: Federal Ministry for Economic Cooperation and Development. [Accessed 1 June 2025]. Available from: https://www.bmz.de/en/ministry/leadership-ministry.

[291]LinkedIn. (n.d.). Reem Alabali-Radovan – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/reem-alabali-radovan-6a2776178/

[292]LinkedIn. (n.d.). Bärbel Kofler – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/dr-b%C3%A4rbel-kofler/

[293]LinkedIn. (n.d.). Johann Saathoff – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/johann-saathoff-34ba78123/

[294]FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION, NUCLEAR SAFETY AND CONSUMER PROTECTION (BMUV). *Leadership* [online]. Berlin: BMUV. [Accessed 1 June 2025]. Available from: https://www.bmuv.de/ministerium/hausleitung.

[295]LinkedIn. (n.d.). Carsten Schneider – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/carsten-schneider-482ba6205/

[296]LinkedIn. (n.d.). Jochen Flasbarth – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: http://linkedin.com/in/jochen-flasbarth-886039322/

[297]LinkedIn. (n.d.). Rita Schwarzelühr-Sutter – LinkedIn profile. LinkedIn. [Accessed 30 May 2025]. Available from: http://linkedin.com/in/rita-schwarzel%C3%BChr-sutter-472451132/

[298]FEDERAL MINISTRY FOR EDUCATION, FAMILY AFFAIRS, SENIOR CITIZENS, WOMEN AND YOUTH (BMFSFJ). *Leadership* [online]. Berlin: Federal Ministry for Education, Family Affairs, Senior Citizens, Women and Youth. [Accessed 1 June 2025]. Available from: https://www.bmfsfj.de/bmfsfj/ministerium.

Women and Youth: Karin Prien

3.12.2. State Secretary: Ingo Behnel

3.12.3. State Secretary: Petra Bahr

3.12.3.1. Parliamentary State Secretary: Michael Brand

3.12.3.2. Parliamentary State Secretary: Mareike Wulf[299]

3.13. **Federal Ministry of Labour and Social Affairs**[300]

3.13.1. Federal Minister of Labour and Social Affairs: Bärbel Bas

3.13.2. Permanent State Secretary in the Federal Ministry of Labour and Social Affairs: Leonie Gebers

3.13.3. Permanent State Secretary in the Federal Ministry of Labour and Social Affairs: Lilian Tschan[301]

3.13.3.1. Parliamentary State Secretary to the Federal Minister of Labour and Social Affairs: Kerstin Griese

3.13.3.2. Parliamentary State Secretary to the Federal Minister of Labour and Social Affairs: Katja Mast

Regulatory Entities

3.14. National Regulatory Authorities

3.14.1. The Federal Commissioner for Data Protection and Freedom of Information[302]

3.14.1.1. Federal Commissioner for Data Protection and Freedom of Information: Louisa Specht-Riemenschneider[303]

3.14.1.1.1. Senior Official and Deputy Federal Commissioner for Data Protection and Freedom of Information: Andreas Harlt[304]

[299]LinkedIn. (n.d.). Mareike Wulf – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/mareike-lotte-wulf/?originalSubdomain=d

[300]FEDERAL MINISTRY OF LABOUR AND SOCIAL AFFAIRS (BMAS). *Minister and Senior Officials* [online]. Berlin: Federal Ministry of Labour and Social Affairs. [Accessed 1 June 2025]. Available from: https://www.bmas.de/DE/Ministerium/Ministerin-und-Hausleitung/ministerin-und-hausleitung.html

[301]LinkedIn. (n.d.). Lilian Tschan – LinkedIn profile. LinkedIn. [Accessed 25 May 2025]. Available from: https://www.linkedin.com/in/lilian-tschan-164287105/?originalSubdomain=de

[302]FEDERAL COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION (BFDI). *Organizational Structure* [online]. Bonn: Federal Commissioner for Data Protection and Freedom of Information. [Accessed 1 June 2025]. Available from: https://www.bfdi.bund.de/DE/BfDI/UeberUns/Organisation/organisation-node.html

[303]LinkedIn. (n.d.). Louisa Specht-Riemenschneider – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/louisa-specht-riemenschneider-141617238/ LinkedIn. (n.d.). Andreas Harlt – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/andreashartl/?originalSubdomain=sg

[304]LinkedIn. (n.d.). Andreas Harlt – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/andreashartl/?originalSubdomain=sg

3.14.2. Agency for Innovation in Cybersecurity[305]

3.14.2.1. Commercial Director: Daniel Mayer

3.14.2.2. Research Director: Christian Hummert[306]

3.14.2.2.1. Head of Key Technology Department: Jürgen Freudenberger[307]

3.14.2.2.2. Head of the Safe Society Department: Ariane Wolf[308]

3.14.2.2.3. Head of Secure Systems Department. Matthias Kranz[309]

3.14.2.2.4. Head of Scientific Services: Michael Domberg[310]

3.14.2.2.5. Head of Central Department: Barbara Diederich[311]

3.15. German Institute for Standardization[312]

3.15.1. Chairman of the Executive Board: Christoph Winterhalter[313]

3.15.2. Executive Board Member: Daniel Schmidt[314]

3.16. (BSI) Federal Office for Information Security[315]

3.16.1. President of the Federal Office for Information Security: Claudia Plattner[316]

3.16.1.1. Vice President of the Federal Office for Information Security: Thomas Caspers[317]

---

[305]FEDERAL AGENCY FOR INNOVATION IN CYBERSECURITY (Cyberagentur). *About Us* [online]. Halle (Saale): Federal Agency for Innovation in Cybersecurity. [Accessed 1 June 2025]. Available from: https://www.cyberagentur.de/agentur/ueber-uns/

[306]LinkedIn. (n.d.). Christian Hummert – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/christian-hummert-b60844208/

[307]LinkedIn. (n.d.). Jürgen Freudenberger – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/j%C3%BCrgen-freudenberger-02988520/

[308]LinkedIn. (n.d.). Ariane Wolf – LinkedIn profile. LinkedIn. [Accessed 22 May 2025]. Available from: https://www.linkedin.com/in/ariane-w/

[309]LinkedIn. (n.d.). Matthias Kranz – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/matthiaskranz

[310]LinkedIn. (n.d.). Michael Domberg – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/michael-domberg-885aa1a7/

[311]LinkedIn. (n.d.). Barbara Diederich – LinkedIn profile. LinkedIn. [Accessed 26 May 2025]. Available from: https://www.linkedin.com/in/dr-barbara-diederich-5b0299191/

[312]GERMAN INSTITUTE FOR STANDARDIZATION (DIN). *Executive Board* [online]. Berlin: DIN. [Accessed 1 June 2025]. Available from: https://www.din.de/en/din-and-our-partners/din-e-v/organization/executive-board

[313]LinkedIn. (n.d.). Christoph Winterhalter – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christoph-winterhalter/

[314]LinkedIn. (n.d.). Daniel Schmidt – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/daniel-schmidt-ek/

[315]FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). *Leadership* [online]. Bonn: Federal Office for Information Security. [Accessed 1 June 2025]. Available from: https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/Leitung/leitung_node.html

[316]LinkedIn. (n.d.). Claudia Plattner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/claudiaplattner/

[317]LinkedIn. (n.d.). Thomas Caspers – LinkedIn profile. LinkedIn. [Accessed 27 May 2025]. Available from: https://www.linkedin.com/in/thomascaspers/

3.17. Federal Office for Civil Protection and Disaster Assistance[318]

3.17.1. President of the Federal Office of Civil Protection and Disaster Assistance: Ralph Tiesler[319]

3.17.1.1. Vice President of the Federal Office of Civil Protection and Disaster Assistance: René Funk[320]

3.18. Federal Office for Economic Affairs and Export Control[321]

3.18.1. Head of the Central Department: Holger Beutel[322]

3.18.2. Head of the Export Procedures, Authorisations, International Regime Procedures and Outreach Projects Department: Georg Pietsch[323]

3.18.3. Head of the Export Technology, Technical Opinions and International Regimes Department: Thomas Jennen[324]

3.18.4. Head of the Economic and Small Business Promotion Department: Martina Becker[325]

3.18.5. Head of the Energy Efficiency, Renewable Energies and Special Compensation Scheme Department: Heidi Motsch

3.18.6. Head of the Climate Protection Buildings, Energy Information Center and Adjustment Allowance Department: Venio Piero Quinque[326]

3.19. Central Office for Information Technology in the Security

---

[318]FEDERAL OFFICE OF CIVIL PROTECTION AND DISASTER ASSISTANCE (BBK). *Leadership* [online]. Bonn: Federal Office of Civil Protection and Disaster Assistance. [Accessed 1 June 2025]. Available from: https://www.bbk.bund.de/DE/Das-BBK/Das-BBK-stellt-sich-vor/Leitung/leitung_node.html

[319]LinkedIn. (n.d.). Ralph Tiesler – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/ralph-tiesler-35253038/?originalSubdomain=de

[320]LinkedIn. (n.d.). René Funk – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/ren%C3%A9-funk-191a95237/

[321]FEDERAL OFFICE FOR ECONOMIC AFFAIRS AND EXPORT CONTROL (BAFA). *Organizational Structure* [online]. Eschborn: Federal Office for Economic Affairs and Export Control. [Accessed 1 June 2025]. Available from: https://www.bafa.de/DE/Bundesamt/Organisation/Aufbau/aufbau_node.html

[322]LinkedIn. (n.d.). Holger Beutel – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/holger-beutel-26123071/

[323]LinkedIn. (n.d.). Georg Pietsch – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/georg-pietsch-5901b6136/

[324]LinkedIn. (n.d.). Thomas Jennen – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/thomas-jennen-08713614b/

[325]LinkedIn. (n.d.). Martina Becker-Zahn – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/martina-becker-zahn/?locale=es_ES

[326]LinkedIn. (n.d.). Venio Quinque – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/venioquinque/?originalSubdomain=de

Sector (ZITiS)[327]

3.19.1. President of ZiTiS: Wilfried Karl[328]

3.19.1.1. Vice President & CTO: Jens Römer[329]

3.20. The European Union Agency for Cybersecurity (ENISA)[330]

3.20.1. Management Board

3.20.1.1. Chair: Fabienne Tegeler[331]

3.20.1.2. Vice Chair: Tomas Minarik[332]

3.20.1.3. Commission Representatives

3.20.1.4. Member States Representatives

3.20.1.5. EEA-Country Representatives (Observers)

3.20.2. Executive Board:

3.20.2.1. Executive Director of the European Union Agency for Cybersecurity: Juhan Lepassaar[333]

Annex 8: Media - Argentina[334]

Argentina

1.1. Printed Media

1.1.1. National Media

1.1.1.1. Newspapers

1.1.1.1.1. **La Nación**

1.1.1.1.1.1. Editor-in-Chief: Fernán Saguier[335]

[327]CENTRAL OFFICE FOR INFORMATION TECHNOLOGY IN THE SECURITY SECTOR (ZITiS). *Leadership* [online]. Munich: ZITiS. [Accessed 1 June 2025]. Available from: https://www.zitis.bund.de/DE/WerWirSind/werwirsind_node.html#leitung

[328]LinkedIn. (n.d.). Wilfried Karl – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/wilfried-karl-67785571/

[329]LinkedIn. (n.d.). Jens Roemer – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/jens-roemer-82bb57125/?miniProfileUrn=urn%3Ali%3Afs_miniProfile%3AACoAAB713OMBqPmGbXDI6ZbniJ4b5Ho-Za8m4_k

[330]EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *Who We Are* [online]. Athens: European Union Agency for Cybersecurity. [Accessed 1 June 2025]. Available from: https://www.enisa.europa.eu/about-enisa/who-we-are

[331]LinkedIn. (n.d.). Fabienne Tegeler – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: http://linkedin.com/in/fabienne-tegeler-941b37238/?originalSubdomain=de

[332]LinkedIn. (n.d.). Tomáš Minárik – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/tom%C3%A1%C5%A1-min%C3%A1rik-819b1448/?originalSubdomain=cz

[333]LinkedIn. (n.d.). Juhan Lepassaar – LinkedIn profile. LinkedIn. [Accessed 3 June 2025]. Available from: https://www.linkedin.com/in/juhan-lepassaar-961205340/

[334]Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data

[335]LA NACIÓN. *Fernán Saguier es nuevo director de LA NACIÓN* [online]. [Accessed 24 May 2025]. Available from: https://www.lanacion.com.ar/sociedad/fernan-saguier-es-nuevo-director-la-nacion-nid2513760/

1.1.1.1.1.1.1. Executive Editor: José Del Río[336]

1.1.1.1.1.1.1.1. Section Editor: Ricardo Sametband[337] (Technology)

1.1.1.1.1.1.1.1.1. Journalist : Ariel Torres[338] (tech & digital security)

1.1.1.1.1.1.1.1.2. Journalist : Débora Slotnisky[339] (tech & Cybersecurity

1.1.1.1.1.1.1.1.3. Journalist : Victoria Menghini[340] (AI & Cybersecurity)

1.1.1.1.1.1.1.1.4. Journalist : Sebastián Davidovsky[341] (tech & Cybersecurity)

1.1.1.1.2. **Clarín**

1.1.1.1.2.1. Editor-in-Chief: Ricardo Kirschbaum[342]

1.1.1.1.2.2. Deputy Editor-in-Chief: Ricardo Roa[343]

1.1.1.1.2.2.1. Technology Section Editor: Juan Brodersen[344]

1.1.1.1.2.2.1.1. Journalist: Virginia Messi[345] (data security)

1.1.1.1.2.2.1.2. Journalist:Pablo Javier Blanco (tech & cybersecurity)

---

[336]LinkedIn. (n.d.). José Del Rio – LinkedIn profile. LinkedIn. [Accessed 23 May 2025]. Available from: https://www.linkedin.com/in/jos%C3%A9-del-rio-5a413512/

[337]LA NACIÓN. *Ricardo Sametband - LA NACIÓN* [online]. [Accessed 20 May 2025]. Available from: https://www.lanacion.com.ar/autor/ricardo-sametband

[338]LinkedIn. (n.d.). Ariel Torres – LinkedIn profile. LinkedIn. [Accessed 17 May 2025]. Available from: https://www.linkedin.com/in/arieltorres/

[339]LinkedIn. (n.d.). Debora Slotnisky – LinkedIn profile. LinkedIn. [Accessed 20 May 2025]. Available from: https://www.linkedin.com/in/deboraslotnisky/

[340]LA NACIÓN. *Victoria Menghini - LA NACIÓN*. [online] [Accessed 20 May 2025]. Available from: https://www.lanacion.com.ar/autor/victoria-menghini/.

[341]LinkedIn. (n.d.). Sebastián Davidovsky – LinkedIn profile. LinkedIn. [Accessed 20 May 2025]. Available from: https://www.linkedin.com/in/sebasti%C3%A1n-davidovsky/

[342]GRUPO CLARÍN. *Management*. [online] [Accessed 20 May 2025]. Available from: https://ir.grupoclarin.com/management/.

[343]CLARÍN. *Ricardo Roa - Clarín*. [online] [Accessed 20 May 2025]. Available from: https://www.clarin.com/autor/ricardo-roa.html.

[344]LinkedIn. (n.d.). Juan Brodersen – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/juan-brodersen/

[345]GRUPO CLARÍN. *Virginia Messi - Clarín*. [online]. [Accessed 20 May 2025]. Available from: https://www.clarin.com/autor/virginia-messi.html.

1.1.1.1.2.2.1.3. Journalist : Tomás Balmaceda[346] (technology)

1.1.1.1.3. **Perfil**

1.1.1.1.3.1. Editorial Director: Walter Curia[347]

1.1.1.1.3.1.1. Editor-in-Chief: Carlos Piro[348]

1.1.1.1.3.1.2. Executive Editor: Dario silva D'Andrea[349]

1.1.1.1.3.1.2.1. Digital technology manager: Federico Ramato[350]

1.1.1.1.3.1.2.1.1. Journalist: Gabriel Zurdo[351] (Cybersecurity)

1.1.1.1.3.1.2.1.2. Journalist: Claudia Vizcarra[352]

1.1.1.1.3.1.2.1.3. Journalist: Sergio Marin[353] (opinion)

1.1.1.1.3.1.2.1.4. Journalist: Andy Ferreyra[354] (cybersecurity & crime)

1.1.1.1.3.1.2.1.5. Journalist: Francisco Larez[355] (Technology)

1.1.1.1.4. **Página/12**

1.1.1.1.4.1. Editor-in-Chief: Nora Veiras[356]

---

[346]LinkedIn. (n.d.). Tomás Balmaceda – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/tomasbalmacedahuarte/

[347]PERFIL. *Walter Curia – Perfil.* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/waltercuria

[348]LinkedIn. (n.d.). Carlos Piro – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/carlos-piro-795bbb104/

[349]PERFIL. *Darío Silva D'Andrea – Perfil.* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/dsilva.

[350]PERFIL. *Equipo de Editorial Perfil* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/staff

[351]PERFIL. *Gabriel Zurdo – Perfil* [online] [Accessed 20 May 2025]. Available from: https://www.perfil.com/autores/gabrielzurdo.

[352]LinkedIn. (n.d.). Claudia Vizcarra – LinkedIn profile. LinkedIn. [Accessed 15 June 2025]. Available from: https://www.linkedin.com/in/claudiavizcarra/?originalSubdomain=ar

[353]PERFIL. *Sergio Marín – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/Personalidaes/sergio-marin.

[354]PERFIL. *Ciberseguridad oficial vulnerada – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/noticias/cordoba/ciberseguridad-oficial-vulnerada-el-pedido-de-un-experto-tras-el-ataque-a-la-web-del-gobierno.phtml.

[355]PERFIL. *Francisco Larez – Perfil* [online] [Accessed 29 May 2025]. Available from: https://www.perfil.com/autores/franciscolarez.

[356]PÁGINA12. *Nora Veiras – Página 12* [online] [Accessed 29 May 2025]. Available from: https://www.pagina12.com.ar/autores/2333-nora-veiras.

1.1.1.1.4.1.1. Journalist: Mariana Carbajal[357] (Tech & Society)

1.1.1.1.5. **El Cronista**[358]

1.1.1.1.5.1. General director: Christian Findling[359]

1.1.1.1.5.1.1. Editorial Director: Hernán de Goñi[360]

1.1.1.1.5.1.2. Deputy Editorial Director: Horacio Riggi[361]

1.1.1.1.5.1.2.1. Editorial Director: Florencia Pulla[362]

1.1.1.1.5.1.2.1.1. Chief editor: Walter Brown[363]

1.1.1.1.5.1.2.1.2. Journalist: Juana Posbeyikian[364] (Cybersecurity)

1.1.1.2. Magazines[365]

1.1.1.2.1. **Revista Mercado**[366]

1.1.1.2.1.1. Director- Editor: Miguel Angel Diaz[367]

1.1.1.2.1.1.1. Editorial Executive Secretary: Carina Martinez (cybersecurity)[368]

---

[357]PÁGINA12. *Las mujeres tienen mucho que aportar en la ciberseguridad – Mariana Carbajal* [online] [Accessed 29 May 2025]. Available from: https://www.pagina12.com.ar/794250-las-mujeres-tienen-mucho-que-aportar-en-ciberseguridad.

[358] El Cronista does not have a dedicated cybersecurity section but publishes articles about cybersecurity occasionally in sections such as business and technology

[359]EL CRONISTA. *Christian Findling – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/christian-findling/.

[360]EL CRONISTA. *Hernan de Goni – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/hdegoni/.

[361]EL CRONISTA. *Horacio Riggi – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/hriggi/.

[362]EL CRONISTA. *Florencia Pulla – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/florencia-pulla/

[363]EL CRONISTA. *Walter Brown – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/wbrown/.

[364]EL CRONISTA. *Juana Posbeyikian – El Cronista* [online] [Accessed 29 May 2025]. Available from: https://www.cronista.com/autor/juana-posbeyikian/.

[365] The focus was placed on those magazines that are in print format and are specialized in cybersecurity and related topics, or at least have a significant section dedicated to the subject.

[366]REVISTA MERCADO. *Mercado*. Buenos Aires: Mercado [Accessed 29 May 2025]. Available from: https://mercado.com.ar.

A business and corporate analysis outlet with a dedicated cybersecurity section. It regularly publishes content on data protection, cyber risk, and digital security trends.

[367]REVISTA MERCADO. *Contenidos*. Buenos Aires: Mercado [Accessed 29 May 2025]. Available from: https://mercado.com.ar/revista/edicion-enero-febrero-n1234/contenidos/.

[368]LinkedIn. (n.d.). Carina Martinez – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/carina-mar/cmartinez/

1.1.1.2.1.1.1.1. Journalist: Juan Martinez[369] (cybersecurity and data protection)

1.2. Digital Media (online)

1.2.1. National Media

1.2.1.1. Newspapers

1.2.1.1.1. **Infobae**[370]

1.2.1.1.1.1. Director & Founder : Daniel Hadad[371]

1.2.1.1.1.1.1. Editor -in-Chief: Mariano Thieberger[372]

1.2.1.1.1.1.2. Commercial Director: Romina Stekar[373]

1.2.1.1.1.2.1. Journalist: Javier Sinay[374]

1.2.1.1.1.2.2. Journalist: Juan Diego Rios[375] (Technology)

1.2.1.1.1.2.3. Journalist: Gabriel Zurdo[376] (Tech & cybersecurity)

1.2.1.1.1.2.4. Journalist: Desiree Jaimovich[377] (Tech & innovation)

---

[369]REVISTA MERCADO. *Juan Martinez*. Buenos Aires: Mercado [Accessed 30 May 2025]. Available from: https://mercado.com.ar/author/juanpmartineznotasgmail-com/.

[370]INFOBAE. Argentina. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com.
Infobae is a major Argentine online news outlet known for fast, broad coverage of national and international news. It occasionally covers cybersecurity topics, especially when related to major incidents, data breaches, or tech trends affecting Latin America.

[371]INFOBAE. *Daniel Hadad*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/daniel-hadad/.

[372]INFOBAE. *Mariano Thieberger*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/mariano-thieberger/.

[373]INFOBAE. *Romina Stekar*. Buenos Aires: Infobae [Accessed 30 May 2025]. Available from: https://www.infobae.com/economia/networking/2021/05/06/el-interactive-advertising-bureau-de-argentina-renovo-autoridades-de-su-consejo-directivo/.

[374]INFOBAE. *Javier Sinay*. Buenos Aires: Infobae, 29 December 2021 [Accessed 30 May 2025]. Available from: https://www.infobae.com/america/soluciones/2021/12/29/desconectarse-es-una-de-las-formas-de-evitar-ciberestafas-en-ano-nuevo-y-vacaciones/.

[375]INFOBAE. *Juan Diego Ríos*. Buenos Aires: Infobae, n.d. [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/juan-diego-r%C3%ADos/

[376]INFOBAE. *Gabriel Zurdo – ataque informático*. Buenos Aires: Infobae, 11 June 2023 [Accessed 30 May 2025]. Available from: https://www.infobae.com/economia/2023/06/11/al-cabo-de-4-dias-la-comision-nacional-de-valores-logro-aislar-y-controlar-un-ataque-informatico-y-manana-lo-denunciara-a-la-justicia/.
He has written articles for Infobae about cybersecurity, including topics such as ransomware, phishing, and the use of artificial intelligence in cybercrime.

[377]INFOBAE. *Desiree Jaimovich – Infobae.* [online]. [Accessed 30 May 2025]. Available from: https://www.infobae.com/autor/desiree-jaimovich/

1.2.1.1.2. **Canal Ar**[378]

1.2.1.1.2.1. Director: Dario Drucaroff[379]

1.2.1.1.2.1.1. Journalist: Matias Nahon[380] (Cybersecurity & AI)

1.2.1.1.2.1.2. Journalist: Federico Tandeter[381] (Cybersecurity)

1.2.1.1.3. **IproUP**[382]

1.2.1.1.3.1. Director: Norberto Zocco[383]

1.2.1.1.3.1.1. Managing Editor: Carlos Altea[384] (finetech)

1.2.1.2. Online Magazines

1.2.1.2.1. **InFo-Cyber** – Cybersecurity and Digital Forensics Journal[385]

1.2.1.2.1.1. Director: Ana Haydée Di Iorio[386]

1.2.1.2.1.1.1. General Editor: Bruno Eduardo Nicolas Constanzo[387] (A.I)

1.2.1.2.1.1.1.1. Cybersecurity editor: Ing. Santiago Trigo[388]

1.2.2. Cybersecurity Websites

---

[378] Canal AR is an Argentine digital media outlet specialized in Information and Communication Technologies (ICT), with a particular focus on cybersecurity, science, and digital culture

[379]CANAL AR. *Darío Drucaroff – Opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=3.

[380]CANAL AR. *Matías Nahón – Opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=1229.

[381]CANAL AR. *Federico Tandeter – Columnas de opinión*. Buenos Aires: Canal Ar [Accessed 30 May 2025]. Available from: https://www.canal-ar.com.ar/opinion.asp?Id=1374.

[382]PROUP. *Sitio web oficial de iProUP*. Buenos Aires: iProUP [Accessed 30 May 2025]. Available from: https://www.iproup.com.

iProUP is an Argentine digital media outlet focused on the digital economy, fintech, innovation, and emerging technologies.

Most cybersecurity articles on iProUP are published under the general byline “Por iProUP” (By iProUP), without individual author attribution.

[383]LinkedIn. (n.d.). Norberto Zocco – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/norbertozocco/

[384]ALTEA, Carlos. *Carlos Altea – iProUP*. Buenos Aires: iProUP [Accessed 30 May 2025]. Available from: https://www.iproup.com/autores/carlos-altea.

[385]INFO-CYBER. *Cybersecurity and Digital Forensics Journal.* Buenos Aires: InFo-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/revista-info-cyber.

[386]DI IORIO, Ana. *Ana Di Iorio – Info-Lab*. Buenos Aires: Info-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/prensa/novedades/181-entrevista-a-ana-di-iorio-

[387]INFO-LAB. *Informe de Gestión 2024*. Buenos Aires: Info-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/images/2022/Papers/2024/Informe_de_Gestion_2024.pdf

[388]INFO-LAB. *Informe de Gestión 2024*. Buenos Aires: Info-Lab [Accessed 30 May 2025]. Available from: https://info-lab.org.ar/images/2022/Papers/2024/Informe_de_Gestion_2024.pdf

1.2.2.1. **Argentina cibersegura**[389]

1.2.2.1.1. President: Federico Perez Acquisto[390]

1.2.2.1.1.1. Vice President: Facundo Malaureille[391]

1.2.2.1.1.1.1. Secretary: Andres Tamburi[392]

1.3. Tv[393]

1.3.1. National Media

1.3.1.1. **TV PÚBLICA**[394]

1.3.1.1.1. Executive Director: Eduardo Gonzales[395]

1.3.1.1.1.1. General Content Manager: Len Cole

1.3.1.1.1.1.1. Host & tech specialist: Lucas Gonzales (cybersecurity)

1.3.1.1.1.1.1.1. Journalist: Julieta Schulkin (technology)

1.3.1.1.1.1.1.2. Journalist: Marcos Mansueti (cybersecurity & ethical hacking)

1.3.1.2. Tec TV

1.3.1.2.1. Executive director: Lucas Turturro[396]

1.3.1.3. TN (Todo Noticias)

1.3.1.3.1. General content manager: Santiago do Regó[397]

1.3.1.3.2. Host & Tech Specialist : Federico Wiemeyer[398](cybersecurity & tech)

1.3.1.3.2.1. Journalist: Julio Lopez[399] (cybersecurity)

1.4. Radio

1.4.1. National Media

1.4.1.1. Radio Nacional AM 870

---

[389]ARGENTINA CIBERSEGURA. *Argentina Cibersegura*. [online] [Accessed 30 May 2025]. Available from: https://www.argentinacibersegura.org
Non-profit organization.

[390]ARGENTINA CIBERSEGURA. *Comisión Directiva*. [online] [Accessed 27 May 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos

[391]LinkedIn. (n.d.). Facundo MP – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: http://linkedin.com/in/facundomp

[392]LinkedIn. (n.d.). Andres Tamburi – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andrestamburi/

[393]Refers to national outlets specialized in cybersecurity or with a strong, regularly updated cybersecurity section.

[394] It currently stands out as the program with the strongest focus on cybersecurity.

[395]QUIÉN ES EDUARDO GONZALEZ - EL DESTAPE. [online] [Accessed 30 May 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos

[396]LinkedIn. (n.d.). Lucas Turturro – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/lucasturturro/?originalSubdomain=ar

[397]LinkedIn. (n.d.). Santiago do Rego – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/santiagodorego/?originalSubdomain=ar

[398]Instagram. (n.d.). Federico Wiemeyer – Instagram profile. Instagram. [Accessed 30 May 2025]. Available from: https://www.instagram.com/wiemeyer/?hl=es

[399]Instagram. (n.d.). Julio Lopez – Instagram profile. Instagram. [Accessed 18 May 2025]. Available from: https://www.instagram.com/julitolopez/?hl=es

1.4.1.1.1. Journalists: Silvia Maruccio[400] (cybersecurity)
1.4.1.1.2. Journalist: Emiliano Piscitelli[401]
1.4.1.2. AM 750 (Grupo Octubre)
1.4.1.2.1. General Director: Eduardo Aliverti[402]
1.5. Podcast
1.5.1.1. National Media
1.5.1.1.1. Secure Podcast[403]
1.5.1.1.1.1. Host: Marcos Garcia[404]
1.5.1.1.1.1.1. Co-Host: Maxi Soler[405]
1.5.1.1.1.1.2. Co- Host : Carlos Garay[406] (cybersecurity)
1.5.1.1.1.1.2.1. Journalist: Marcela Pallero[407] (incidents & response regulations)

Journalist: Cristian Borghello[408] (cybersecurity)

1.5.1.1.2. Meet the hacker[409]
1.5.1.1.2.1. Director: Federico Pacheco[410]

Annex 9: Media - United States[411]

1. U.S.A

1.1. Print Media

1.1.1. National Media

1.1.1.1. Wired Magazine

1.1.1.1.1. Global Editorial Director: Katie Drummond[412]

[400]LinkedIn. (n.d.). Silvia Maruccio – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/silvia-maruccio-7983a81b9/?originalSubdomain=ar
[401]LinkedIn. (n.d.). Emiliano Piscitelli – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/emilianopiscitelli/?originalSubdomain=ar
[402]Instagram. (n.d.). Eduardo Aliverti – Instagram profile. Instagram. [Accessed 18 May 2025]. Available from: https://www.instagram.com/eduardoalivertiok/?hl=es
[403]SECURE PODCAST. [online] [Accessed 18 May 2025]. Available from: https://securepodcast.com
[404]GARCIA, Marcos. *Secure Podcast*. [online] [Accessed 18 May 2025]. Available from: https://securepodcast.com
[405]LinkedIn. (n.d.). Maxi Soler – LinkedIn profile. LinkedIn. [Accessed date unknown]. Available from: https://www.linkedin.com/in/maxisoler/?originalSubdomain=a
[406]LinkedIn. (n.d.). Carlos Garay – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/carlos-garay-4396ba25/?originalSubdomain=a
[407]LinkedIn. (n.d.). Marcela Pallero – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/marcelapallero/
[408]LinkedIn. (n.d.). Cristian Borghello – LinkedIn profile. LinkedIn. [Accessed 18 May 2025]. Available from: https://www.linkedin.com/in/cristianborghello/?locale=es_ES
[409]Meet the hacker. [online] [Accessed 18 May 2025]. Available from: https://podimo.com/shows/meet-the-hacker
[410]Federico Pacheco | LinkedIn. [online]. Available at: https://www.federicopacheco.com [Accessed 18 May2025].
[411]Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data.
[412]LinkedIn. (n.d.). Katie Drummond – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/katie-drummond-75ba6313/

1.1.1.1.1.1. Senior Editor for Security & Investigations: Andrew Couts[413]

1.1.1.1.1.1.1. Journalist: Andy Greenberg[414]

1.1.1.1.1.1.2. Journalist: Lily Hay Newman[415]

1.1.1.1.1.1.3. Journalist: Matt Burguess[416]

1.1.1.2. Security Today

1.1.1.2.1. Publisher: Ralph C. Jensen[417]

1.1.1.2.1.1. Editor: Brent Dirks[418]

1.1.1.3. **MIT Technology Review**

1.1.1.3.1. Senior Editor: Will Douglas Heaven[419]

1.1.1.4. Fast Company Magazine

1.1.1.4.1. Global Technology Editor: Harry McCracken[420]

1.1.1.4.1.1. Senior Writer: Mark Sullivan[421]

1.1.1.4.1.2. Tech Editor and Writer: Lora Kolodny[422]

1.1.1.4.1.3. Tech Journalist: Daniel Terdiman[423]

1.1.2. Local Media

1.1.2.1. **Miami Herald**

1.1.2.1.1. Executive Editor: Alex Mena[424]

1.1.2.1.1.1. Technology Journalist: Vinod Sreeharsha[425]

1.1.2.2. Global Miami Magazine

---

[413]LinkedIn. (n.d.). Andrew Couts – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andrew-couts-5922412a/

[414]LinkedIn. (n.d.). Andy Greenberg – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/andygreenbergjournalist/

[415]LinkedIn. (n.d.). Lily Hay Newman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lilyhnewman/

[416]WIRED. (n.d.). Matt Burgess – Author profile. Wired. [Accessed 2 June 2025]. Available from: https://www.wired.com/author/matt-burgess/

[417]LinkedIn. (n.d.). Ralph Jensen – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/ralph-jensen-452b353/

[418]LinkedIn. (n.d.). Brent Dirks – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/brentdirks

[419]LinkedIn. (n.d.). Will Douglas Heaven – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/will-douglas-heaven-843358b/

[420]LinkedIn. (n.d.). Harry Mc Cracken – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/harrymccracken/

[421]LinkedIn. (n.d.). Mark Sullivan – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/thesullivan/

[422]LinkedIn. (n.d.). Lora Kolodny – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lorakolodny/

[423]LinkedIn. (n.d.). Daniel Terdiman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/danielterdiman/

[424]LinkedIn. (n.d.). Alex Mena – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/alex-mena-9475856/

[425]LinkedIn. (n.d.). Vinod Sreeharsha – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/vinod-sreeharsha-51317b/

1.1.2.2.1. Editor in Chief: James Faber[426]

1.1.2.2.1.1. Contributing Writer: Doreen Hemlock[427]

1.2. Digital Media

1.2.1. National Media

1.2.1.1. Krebs on Security

1.2.1.1.1. Founder, manager and editor: Bryan Krebs[428]

1.2.1.2. Dark Reading

1.2.1.2.1. Editor in Chief: Kelly Jackson Higgins[429]

1.2.1.2.2. Co-Editor in Chief: Tim Wilson[430]

1.2.1.2.2.1. Senior Editor: Becky Bracken[431]

1.2.1.2.2.2. Associate Writer: Kristina Beek[432]

1.2.1.2.2.3. Contributing Writer: Stephen Lawton[433]

1.2.1.3. Threatpost

1.2.1.3.1. Editor in Chief: Tom Spring[434]

1.2.1.3.2. Editor in Chief: Tara Seals[435]

1.2.1.3.2.1. Managing Editor: Chris Brook[436]

1.2.1.4. The Hacker News

1.2.1.4.1. Editor in Chief: Mohit Kumar[437]

1.2.1.4.2. Cybersecurity and Privacy Reporter: Swati Khandelwal[438]

---

[426]LinkedIn. (n.d.). James Faber – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/james-faber-82052666/

[427]LinkedIn. (n.d.). Doreen Hemlock – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/doreen-hemlock-783953/

[428]LinkedIn. (n.d.). Bryan Krebs – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/bkrebs/

[429]LinkedIn. (n.d.). Kelly Jackson Higgins – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kellyj2/

[430]LinkedIn. (n.d.). Tim Wilson – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/tim-wilson-ba5a082a/

[431]LinkedIn. (n.d.). Becky Bracken – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/becky-bracken-65aa857/

[432]LinkedIn. (n.d.). Kristina Beek – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kristina-beek/

[433]LinkedIn. (n.d.). Stephen Lawton – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/stephenlawton/

[434]LinkedIn. (n.d.). Tom Spring – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/zpring/

[435]LinkedIn. (n.d.). Tara Seals – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/tara-seals-763a2155/

[436]LinkedIn. (n.d.). Chris Brook – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/chris-brook-91223712/

[437]LinkedIn. (n.d.). Mohit Kumar – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mohitkumar09/

[438]LinkedIn. (n.d.). Swati Khandelwal – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/swati-khandelwal-4566b78a/

1.2.1.4.2.1. Cybersecurity Researcher and Analyst: Mayank Grover[439]

1.3. TV

1.3.1. National Media

1.3.1.1. **Bloomberg TV**

1.3.1.1.1. Executive Producer: Christine Baratta[440]

1.3.1.2. **CNBC**

1.3.1.2.1. Senior Executive Producer: Lisa Villalobos[441]

1.3.1.2.2. Executive Producer: Kevin Flynn[442]

1.3.1.3. Cheddar News

1.3.1.3.1. Executive Producer: Kathy Cherpelis[443]

1.3.1.3.1.1. Senior Producer: Chris Castellino[444]

1.3.2. Local Media

1.3.2.1. NBC 6 South Florida

1.3.2.1.1. Executive Producer of Content: Christina Fiumefreddo[445]

1.4. Multiplatform (Stream, Podcast)

1.4.1. National Media

1.4.1.1. CISA Live (Stream)

1.4.1.1.1. Department of Homeland Security

1.4.1.2. Storm Watch (Stream)

1.4.1.2.1. Data Scientist: Bob Rudis[446]

1.4.1.2.2. Security Researcher: Himaja Motheram[447]

1.4.1.3. **Fortinet TV** (Stream and Podcast)

1.4.1.3.1. Brass Tacks – Talking Cybersecurity (Podcast)

---

[439]LinkedIn. (n.d.). Mayank Grover – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mayank-grover/

[440]LinkedIn. (n.d.). Christine Baratta – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christine-baratta-1a2a13a/

[441]LinkedIn. (n.d.). Lisa Villalobos – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lisavillalobos

[442]LinkedIn. (n.d.). Kevin Flynn – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kevin-flynn-5b603660/

[443]LinkedIn. (n.d.). Kathy Cherpelis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/kathy-cherpelis-b5850aa/

[444]LinkedIn. (n.d.). Chris Castellino – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/chriscastellino/

[445]LinkedIn. (n.d.). Christine Fiumefreddo – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/christina-fiumefreddo/

[446]LinkedIn. (n.d.). Bob Rudis – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/hrbrmstr/

[447]LinkedIn. (n.d.). Himaja Motheram – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/himaja-m/

1.4.1.3.1.1. Content Strategist : Joe Robertson[448]

1.4.1.4. **TWiT.tv** (Stream and Podcast)

1.4.1.4.1. CEO & Executive Producer: Lisa Laporte[449]

1.4.1.4.1.1. Editor and Producer: John Ashley[450]

1.4.1.5. **TechCrunch Live** (Stream)

1.4.1.5.1. Senior Editor: Matt Burns[451]

1.4.1.6. **Cyber Wire** (Podcast)

1.4.1.6.1. Executive Producer: Jennifer Eiben[452]

1.4.1.6.2. Host and Producer: Dave Bittner[453]

1.4.1.7. **Secure World Radio** (Podcast)

1.4.1.7.1. Host: Bruce Sussman[454]

1.5. Radio

1.5.1. National Media

1.5.1.1. National Cyber Security Radio Show

1.5.1.1.1. Executive Producer: Gregory D. Evans[455]

Annex 10: Media - Germany[456]

1. Germany

1.1. Print Media

1.1.1. National Media

1.1.1.1. **Süddeutsche Zeitung**

[448]LinkedIn. (n.d.). Joe Robertson – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/joerobertson1/

[449]LinkedIn. (n.d.). Lisa Laporte – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lisadlaporte/

[450]LinkedIn. (n.d.). John Ashley – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/johnhashley/

[451]LinkedIn. (n.d.). Matt Burns – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/mjburnsy/

[452]LinkedIn. (n.d.). Jennifer Eiben – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jennifer-eiben/

[453]LinkedIn. (n.d.). Dave Bittner – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/dave-bittner-27231a4/

[454]LinkedIn. (n.d.). Bruce Sussman – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/brucesussman/

[455]LinkedIn. (n.d.). Gregory D Evans – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/gregorydevans/

[456]*Please note that any details not explicitly attached or referenced herein may be subject to change, may contain outdated information, or may be incomplete due to a lack of available data*

1.1.1.1.1. Chairman: Dr. Christian Wegner[457] [458]

1.1.1.1.1.1. Management: Johannes Hauner[459]

1.1.1.1.1.2. Management: Dr. Karl Ulrich[460]

1.1.1.1.1.2.1. Chief Editor: Wolfgang Krach[461]

1.1.1.1.1.2.2. Chief Editor: Judith Wittwer[462]

1.1.1.1.1.2.2.1. Newsroom Head: Dr. Alexandra Föderl

1.1.1.1.1.2.2.2. Newsroom Head: Jens Schneider

1.1.1.2. **iX (Heise Verlag Magazine)**

1.1.1.2.1. Editor in Chief: Dr. Oliver Diedrich[463]

1.1.1.2.2. Deputy Editor in Chief: Ulrich Wolf[464]

1.1.1.2.3. Senior Editor: Susanne Nolte[465]

1.1.1.2.3.1. Editor: Wolf Hosbach[466]

1.1.1.2.3.2. Editor: Kersten Auel[467]

1.1.1.2.3.3. Editor: Alexander Neumann

1.2. Digital Media

1.2.1. National Media

1.2.1.1. **Heise Medien**

1.2.1.1.1. Founder: Ansgar Heise[468]

---

[457]LinkedIn. (n.d.). Christian Wegner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christian-wegner-89852541/

[458]SÜDDEUTSCHE ZEITUNG. *Verlag: Impressum – Geschäftsführung.* [online] [Accessed 30 May 2025]. Available from: https://www.sueddeutsche.de/projekte/artikel/verlag/artikel-e287935/#:~:text=Gesch%C3%A4ftsf%C3%BChrung%20Dr.Karl%20Ulrich

[459]LinkedIn. (n.d.). Johannes Hauner – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/haunerjo/

[460]LinkedIn. (n.d.). Karl Ulrich – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/karl-ulrich-07b135197/

[461]SUEDDEUTSCHE.DE. *Wolfgang Krach.* [n.d.] [Accessed 1 June 2025]. Available from: https://www.sueddeutsche.de/autoren/wolfgang-krach-1.1143286.

[462]SUEDDEUTSCHE.DE. *Verlag: Impressum – Chefredaktion*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.sueddeutsche.de/projekte/artikel/verlag/artikel-e287935/#:~:text=Chefredaktion.

[463]LinkedIn. (n.d.). Oliver Diedrich – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/oliverdiedrich/

[464]HEISE GRUPPE. *Über uns.* [n.d.] [Accessed 30 May 2025]. Available from: https://www.heisegroup.de/ueber-uns.html#:~:text=match%20at%20L259%20Karsten%20Marquardsen%2C,Verlag%20Dumrath%20%26%20Fassnacht%20übernommen.

[465]LinkedIn. (n.d.). Susanne Nolte – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/susanne-nolte-9b0b1b268/

[466]LinkedIn. (n.d.). Wolf Hosbach – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/wolfhos/

[467]LinkedIn. (n.d.). Kersten Auel – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/kersten-auel-57a6b68b/

[468]LinkedIn. (n.d.). Ansgar Heise – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/ansgar-heise-0a958019/

1.2.1.1.1.1. Managing Director: Karsten Marquardsen[469]

1.2.1.1.1.1.1. Editor in Chief: Dr. Volker Zota[470]

1.2.1.2. **Golem (Computec Media / Marquard Group)**

1.2.1.2.1. Director: Jens Ihlenfeld[471]

1.2.1.2.1.1. Editor in Chief: Benjamin Sterbenz[472]

1.2.1.3. **Computerwoche**

1.2.1.3.1. CEO: Maria Savvidou[473]

1.2.1.3.2. Editor in Chief: Martin Bayer[474]

1.3. Radio

1.3.1. National Media

1.3.1.1. **Deutschlandfunk[475]**

1.3.1.1.1. Director General: Stefan Raue[476]

1.3.1.1.2. Chief Editor: Birgit Wentzien[477]

1.4. TV

1.4.1. 3.4.1 National Media

1.4.1.1. **ARD Tagesschau**

1.4.1.1.1. Editor in Chief: Marcus Bornheim[478]

1.4.1.1.1.1. Digital Expert Journalist: Jörg Schieb[479]

1.4.2. Local Media

1.4.2.1. **ProSieben**

1.4.2.1.1. CEO: Bert Habets[480]

---

[469]LinkedIn. (n.d.). Karsten Marquardsen – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/karsten-marquardsen/

[470]HEISE GRUPPE. *Dr. Volker Zota wird Chefredakteur von heise online*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.heisegroup.de/presse/Personalien-Heise-Medien-6522370.html#:~:text=Dr.Leitmedium%20ausbauen.

[471]LinkedIn. (n.d.). Jens Ihlenfeld – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/ihlenfeld/

[472]GOLEM.DE GMBH. *Impressum*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.golem.de/sonstiges/impressum.html

[473]IDG COMMUNICATIONS MEDIA AG. *Impressum*. [n.d.] [Accessed 30 May 2025]. Available from: https://www.computerwoche.de/impressum

[474]LinkedIn. (n.d.). Martin Bayer – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/martin-bayer-7664881/

[475]DEUTSCHLANDRADIO. *Presseteam*. Cologne: Deutschlandradio, n.d. [Accessed 30 May 2025]. Available from: https://www.deutschlandradio.de/presseteam-100.html

[476]LinkedIn. (n.d.). Stefan Raue – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/stefanrau/

[477]LinkedIn. (n.d.). Birgit Wentzien – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/birgit-wentzien-93151372/

[478]ARD. *Speaker Marcus Bornheim. Munich: ARD, n.d.* [Accessed 31 May 2025]. Available from: https://www.ard.de/die-ard/presse-und-kontakt/speaker/Speaker-Marcus-Bornheim-100/

[479]LinkedIn. (n.d.). Jörg Schieb – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/schiebde/

[480]LinkedIn. (n.d.). Bert Habets – LinkedIn profile. LinkedIn. [Accessed 3, June 2025]. Available from: https://www.linkedin.com/in/berthabets1/

1.4.2.1.1.1. Presenter (Technology): Stefan Gödde[481]

1.4.2.1.1.2. Presenter (Technology): Aiman Abdallah

1.5. Multiplatform (Podcast, Streaming)

1.5.1. National Media

1.5.1.1. **Myra Minds**

1.5.1.1.1. Author: Nicolas Armer[482]

1.5.1.1.2. Host: Christof Klaus[483]

1.5.1.2. **Cybersecurity entschlüsselt**

1.5.1.2.1. Host: Johannes Bauer[484]

1.5.1.2.2. Host: Reinhold Bentele[485]

Annex 11: Analysis of previous Communication Campaign

"Good Practices in Cybersecurity – Part 3[486]: Groundhog Day Security"

Launched on February 2 in 2023, the campaign focuses on an educational and awareness-driven initiative aimed at promoting cybersecurity best practices. Using the metaphor of "Groundhog Day", it emphasizes the need for continuous improvement and iteration in security strategies. The objective was to raise awareness about proactive cybersecurity measures, targeting organizations seeking to enhance their security posture. The campaign was distributed through blog posts, articles, and social media platforms.

In Argentina, where Faraday was founded and has its main operational headquarters, the campaign adopted an educational and approachable tone. Cultural metaphors like "Groundhog Day" were used to make technical concepts easier to grasp. The core message emphasized the importance of integrating cybersecurity from the early stages of development and maintaining continuous vigilance. Distribution channels included Faraday's official blog on Medium, social media platforms such as LinkedIn and Twitter, and participation in local technology events. The target audience was mainly IT

[481]WIKIPEDIA CONTRIBUTORS. *Stefan Gödde*. Wikipedia, n.d. [Accessed 31 May 2025]. Available from: https://en.wikipedia.org/wiki/Stefan_Gödde

[482]MYRA SECURITY GMBH. *Myra Minds.* [online]. [Accessed 31 May 2025]. Available from: https://www.myrasecurity.com/en/news/myra-minds/

[483]LinkedIn. (n.d.). Christof Klaus – LinkedIn profile. LinkedIn. [Accessed 1 June 2025]. Available from: https://www.linkedin.com/in/christof-klaus-4b2286a6/

[484]LinkedIn. (n.d.). Johannes Bauer – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/johannes-bauer-6b0267198/

[485]PODCASTAI. *Cybersecurity entschlüsselt.* [online]. [Accessed 31 May 2025]. Available from: https://podcastai.com/shows/fpvwxj-cybersecurity-entschluesselt

[486]FARADAY. *Good practices in cybersecurity – Part 3: Groundhog Day security*. [online]. 29 May 2024 [Accessed 15 April 2025]. Available from: https://faradaysec.com/good-practices-in-cybersecurity-part-3/

professionals, developers, and small to medium-sized businesses seeking to strengthen their security posture.

In the United States, where Faraday holds its largest market share, the tone of the campaign was more professional and results-oriented, with a strong emphasis on metrics and regulatory compliance. The message focused on the need for a proactive and adaptable security strategy to face increasingly sophisticated threats. The campaign was disseminated through publications in cybersecurity-focused platforms, webinars, and collaborations with industry experts. The audience was composed primarily of large corporations, internal security teams, and compliance officers.

In Mexico, where Faraday has an expanding commercial presence in Latin America, the campaign adopted a hybrid tone that balanced technical accuracy with accessibility. The message centered around empowering businesses to adopt continuous improvement in cybersecurity processes. The primary distribution channels included LinkedIn, local IT forums, and regional cybersecurity webinars, often in collaboration with local tech communities. The target audience consisted of growing tech companies and mid-sized enterprises looking to scale their security posture.

Finally, in Germany, as a representative of the European market, the campaign maintained a formal and technical tone, particularly emphasizing compliance with regulations such as GDPR[487]and other international standards. The message underscored the importance of having an integrated security strategy that covers the entire software lifecycle, from development to production. Faraday used specialized media publications, participated in European cybersecurity conferences, and partnered with industry associations to reach its target audience, which consisted mainly of medium to large enterprises, especially those operating in highly regulated sectors like finance and healthcare.

[487]GENERAL DATA PROTECTION REGULATION (GDPR). *Subject-matter and objectives*. [online]. 2025 [Accessed 25 May 2025]. Available from: https://gdpr-info.eu/art-1-gdpr/.
The GDPR is a data privacy law from the European Union that took effect on May 25, 2018. It sets strict rules for how organizations collect, use, store, and protect the personal data of individuals in the European Union.

Annex 12: Variables Crossing - Media

PUBLIC / VARIABLE	GENERAL			SPECIFIC	
	Awareness Level	**Engagement Frequency**	**Potential Influence**	**Focus in Cybersecurity Issues**	**Amount of Mentions of Cybersecurity Companies**
PRINT MEDIA					
La Nación	Low	Occasional	Medium	Medium	Medium
Clarín	Médium	Consistent	Medium	Medium	Medium
Perfil	Low	Absent	Low	Low	Low
Página/12	Low	Absent	Low	Low	Medium
El Cronista	Low	Absent	Low	Low	Low
Revista Mercado	Null	Absent	Low	Low	Low
Wired Magazine	Low	Absent	High	High	Medium
Security Today	Medium	Absent	High	High	High
MIT Technology Review	Low	Absent	High	High	Medium
Fast Company Magazine	Low	Absent	High	High	Medium
Miami Herald	Null	Absent	Medium	Low	Low
Global Miami Magazine	Null	Absent	Low	Low	Low
Süddeutsche Zeitung	Null	Absent	High	Medium	Low
iX (Heise Verlag Magazine)	Null	Absent	High	High	High
DIGITAL MEDIA					
Infobae	Low	Occasional	High	High	Medium
Canal Ar	Null	Absent	Medium	Medium	Low

Ipro Up	Null	Absent	Low	Medium	Low
InFo- Cyber	Null	Occasional	Low	Medium	Medium
Argentina Cibersegura	Medium	Occasional	Medium	High	Medium
TV Pública	Low	Occasional	Medium	Low	Low
Krebs On Security	Null	Absent	High	High	High
Dark Reading	High	Occasional	High	High	High
Threatpost	Medium	Absent	High	High	High
The Hacker News	High	Consistent	High	High	High
Heise Meiden	Null	Absent	High	High	High
Golem	Null	Absent	High	High	Medium
Computerwoch e	Null	Absent	High	High	High
TV					
TV Pública	Low	Occasional	Medium	Low	Low
Tec TV	Low	Absent	Low	Medium	Low
TN	Low	Occasional	High	Medium	Low
Bloomberg TV	Null	Absent	Medium	Medium	Medium
CNBC	Null	Absent	Medium	Medium	Medium
Cheddar News	Null	Absent	Medium	High	Low
NBC 6 South Florida	Null	Absent	Low	Null	Null
ARD Tagesschau	High	Absent	High	Medium	Low
ProSieben	Medium	Absent	High	Low	Low
MULTIPLATFORM					
Secure Podcast	Medium	Consistent	Medium	High	Low
Meet the	High	Consisten	Medium	High	Low

hacker					
HmanOS	Low	Absent	Low	High	Low
CISA Live	Low	Absent	High	High	High
Storm Watch	Low	Absent	High	High	High
Fortinet TV	Low	Absent	High	High	High
TWIT.tv	Low	Absent	High	High	High
TechCrunch Live	Low	Absent	High	Medium	Medium
Cyber Wire	High	Occasional	High	High	High
Secure World Radio	Null	Absent	Medium	High	High
Myra Minds	Low	Absent	Medium	High	High
Cybersecurity Entschlüsselt	Low	Absent	Medium	High	Medium

Annex 13: Variables Crossing - Government

Segment	Awareness Level	Engagement Frequency	Potential Influence	Compliance with Local Cybersecurity Laws and policies	Contribution to National Talent Development
Argentina					
Executive branch (AFC, DNSC, Ministry of Security)	Null	Absent	Medium	Full	Partial
Legislative (Senate & Deputies Commissions)	Null	Absent	Medium	Full	Null
Regulatory (AAIP, IRAM)	Low	Occasional	High	Full	Partial

Indirect interaction (Ekoparty, USUARIA)	High	Consistent	High	Full	Full
United States					
Executive (ONCD, CISA)	Low	Absent	High	Full	Partial
Legislative (Senate, House Committees)	Low	Absent	High	Partial	Null
Regulatory (NIST, FedRAMP, FTC)	Medium	Occasional	High	Full	Partial
Indirect interaction (DEF CON, SANS Forum)	High	Consistent	High	Partial	Full
Germany					
Executive (BMI, BMVg, BMBF)	Low	Absent	Medium	Partial	Null
Legislative (Bundestag, Bundesrat)	Low	Absent	Medium	Partial	Null
Regulatory (BSI, BfDI, ENISA)	Medium	Occasional	High	Full	Partial
Indirect interaction (Potsdam Conf., HPI)	High	Consistent	High	Partial	Null

Annex 14: Non - Governmental Forums and Associations - Argentina

1. **International Strategic Forums**

1.1. Black Hat USA (Las Vegas, USA)[488]
1.1.1. Jeff Moss[489]: Founder
1.2. DEF CON (Las Vegas, USA)[490]
1.2.1. Jeff Moss[491]: Conference Chair President
1.3. Disobey Cybersecurity (Helsinki, Finland) [492][493]
1.4. H2H – Hackers to Hackers Conference (Brazil)[494]
1.5. Cyber Summit[495] - The Premier Cybersecurity Conference (Latin America)[496]
1.5.1. Flavia Mendez: Founder and CEO[497]

2. **National Industry Conferences & Forums**
2.1. Ekoparty Security Conference[498] - Hack the Talent Summit[499]
2.1.1. Founder: Juan Pablo Daniel Borgna[500]
2.1.2. Founder: Leonardo Pigner[501]

---

[488] FARADAY SECURITY. BlackHat & Car Hacking at DEFCON [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_blackhat-carhacking-defcon-activity-7360770644894007296-y8kJ

[489] MOSS, Jeff. LinkedIn profile [online]. Washington, D.C.: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/jeffmoss/

[490] FARADAY SECURITY. BizzTech Retail Ciberseguridad [online]. Linkedin, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_bizztech-retail-ciberseguridad-activity-7361417337725419520-Pifw

[491] MOSS, Jeff. LinkedIn profile [online]. Washington, D.C.: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/jeffmoss/

[492] Disobey. About – Organising hacker culture events since 2015 [online]. Disobey, [Accessed 18 August 2025]. Available from: https://disobey.fi/2026/about A major cybersecurity and hacker culture event held annually in Helsinki, Finland at Kaapelitehdas. The event brings together a vibrant community of cybersecurity professionals, ethical hackers, researchers, and enthusiasts.

[493] FARADAY SECURITY. CEO Federico Kirschbaum in Uruguay [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_last-week-our-ceo-and-cofounder-federico-activity-7298341543705210881-4DV6

[494] FARADAY SECURITY. H2H [online]. Linkedin, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_h2h-activity-7274431098703540227-5zIK. H2H is a Brazilian information security conference organized by individuals actively involved in information security research and development. It's a platform for sharing knowledge about information security through training and lectures presented by researchers and experts from the corporate, research, and underground communities.

[495] CYBERSUMMIT. Ciberseguridad Industrial [online]. Linkedin, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/thecybersummit_ciberseguridadindustrial-thepremierconference-activity-7336394329323716608-VKsX

[496] CYBERSUMMIT. CyberSummit [online]. Buenos Aires: CyberSummit, [Accessed 16 August 2025]. Available from: https://cybersummit.io/

[497] MÉNDEZ, Flavia. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/flaviamendez/?originalSubdomain=ar

[498] EKOPARTY. *Official website of Ekoparty* [online]. [Accessed 1 June 2025]. Available from: https://ekoparty.org/. It is one of the most prominent cybersecurity events in Latin America, attracts participants from both the private and public sectors, including officials from the Ministry of Security, AFIP, Gendarmería, and the National Directorate of Cybersecurity. Faraday's role as sponsor, workshop leader, and speaker enables informal yet strategic exposure to decision-makers in the public sector.

[499] FARADAY SECURITY. Participamos del evento Ekoparty Hack the Signal [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_participamos-del-evento-ekoparty-hack-the-activity-7345871519589236737-k8l7

[500] LinkedIn. (n.d.). J. P. D. Borgna – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jpdborgna/

[501] LinkedIn. (n.d.). L. Pigñer – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/lpigner/

2.1.3. Founder: Federico Kirschbaum[502]
2.1.4. Founder: Jerónimo Basaldúa[503]
2.1.5. Founder: Francisco Amato[504]
2.2. BizzTech Summit[505] [506]
2.2.1. Vertex Business Connections[507]
2.3. Security BSides Annual Conference (Cordoba) [508] [509]
2.4. Segurinfo Conference[510]

3. **Professional Associations & Networks**
3.1. Argentine Association of Computer and Communications Users (USUARIA)[511]
3.1.1. President: Silvio Szostak[512]
3.1.2. Argentine Chamber of the Software Industry (CESSI)[513]
3.2. Open Worldwide Application Security Project (OWASP)[514] [515]

4. **Academic-Industry Collaborations**

---

[502] LinkedIn. (n.d.). F. K. – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/fedek/
[503] LinkedIn. (n.d.). J. Basaldúa – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/jbasaldua
[504] LinkedIn. (n.d.). F. Müller Amato – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/franamatok/
[505] FARADAY SECURITY. BizzTech Retail Ciberseguridad [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/feed/update/urn:li:activity:7361417337725419520/
[506] BizzTech Summit 2025 – Organization. 2025. [online]. [Accessed 16 Aug. 2025]. Available at: https://2025.bizztechsummit.com/#organizacion
[507] Multisectoral business and technology networking event connecting startups, SMEs, corporations, and institutional representatives
[508] BSides Córdoba. Official website [online]. BSides Córdoba, [Accessed 16 August 2025]. Available from: https://bsidescordoba.org/. BSides Córdoba is a community-driven cybersecurity conference held annually in Córdoba, Argentina that promotes open, inclusive, and technically rich events focused on information security.
[509] FARADAY SECURITY. Participamos en BSides Córdoba [online]. LinkedIn, [Accessed 18 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_bsidescaejrdoba-bsidescaejrdoba-activity-7337914544368893952-AWOK[2](https://www.linkedin.com/embeds/publishingEmbed.html?articleId=7079208955850672993)
[510] Argentine Association of Informatics and Communications Users (USUARIA). *Official website of the Argentine Association of Informatics and Communications Users* [online]. [Accessed 1 June 2025]. Available from: https://www.usuaria.org.ar/. This is a high-level event focused on information security, data protection, and compliance. It convenes a wide array of stakeholders—government entities, multilateral organizations, industry leaders, and academics—providing Faraday with opportunities to position itself among regulators and policy influencers
[511] USUARIA. *Asociación Argentina de Usuarios de la Informática y las Comunicaciones* [online]. [Accessed 2 June 2025]. Available from: https://www.usuaria.org.ar/
[512]LinkedIn. (n.d.). Silvio Szostak – LinkedIn profile. LinkedIn. [Accessed 2 June 2025]. Available from: https://www.linkedin.com/in/silvio-szostak-1a62016/
[513] FARADAY SECURITY. Estuvimos presentes en el Encuentro Empresarial de Ciberseguridad [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_estuvimos-presentes-en-el-encuentro-empresarial-activity-7332789865647910914-LO1v
[514] FARADAY SECURITY. Our COO Martín D. Tartarelli is also a professor at Universidad Austral [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_our-coo-martin-d-tartarelli-is-also-activity-7275166591883902978-3hHX
[515] A globally recognized non-profit organization dedicated to improving software security. Faraday's COO, Martín D. Tartarelli, serves as the Chapter Leader of OWASP Buenos Aires

4.1. Universidad Austral
  4.1.1. Faculty of Engineering – Center for Cybersecurity and Data Studies, Universidad Austral
    4.1.1.1. Platinum Sponsorship of Degree in Cybersecurity Management and Strategy
      4.1.1.1.1. Pedro Adamovic[516]: Director
      4.1.1.1.2. Webinar[517] [518]
4.2. Information Security Lab (LASI) of UADER University and the Municipality of Paraná - Hacking Day 2025[519]
4.3. Universidad Siglo 21: Córdoba Cybersecurity Conference Reloaded[520] [521]
4.4. Universidad Nacional del Comahue - Hack del Valle[522]

Annex 15: Community - Argentina

1. **Local Awareness & Engagement Initiatives:**
  1.1. BA-CSIRT[523] Community Talks [524] [525]
    1.1.1. Gustavo Linares[526]: Director General of Information Security of the Government of the City of Buenos Aires

[516] Universidad Austral – Facultad de Ingeniería. Diplomatura en Gestión y Estrategia en Ciberseguridad [online]. Universidad Austral, [Accessed 16 August 2025]. Available from: https://www.austral.edu.ar/ingenieria/ingenieria-posgrados/ciberseguridad/diplomatura-en-gestion-y-estrategia-en-ciberseguridad/

[517] Hosted a webinar presented by Martín D. Tartarelli on strategies and best practices in cybersecurity, targeting academic and professional audiences.

[518] FARADAY SECURITY. Se viene agosto en Faraday: desde conferencias hasta capacitaciones [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_se-viene-agosto-en-faraday-desde-conferencias-activity-7355987264188887041-MRCY

[519] Facultad de Ciencia y Tecnología – UADER. El LASI y la Municipalidad de Paraná organizan el Hacking Day 2025 [online]. FCyT UADER, [Accessed 16 August 2025]. Available from: https://fcyt.uader.edu.ar/el-lasi-y-la-municipalidad-de-parana-organizan-el-hacking-day-2025/

[520] Collaboration through a full-day cybersecurity session where Faraday experts engaged with students and faculty, discussing security challenges and industry practices.

[521] FARADAY SECURITY. Hablar de seguridad todo el día en el Encuentro Empresarial [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/faradaysec_hablar-de-seguridad-todo-el-d%C3%ADa-en-el-activity-7338925852644040706-4A0L

[522] Hack El Valle. Hack El Valle official website [online]. [Accessed 16 August 2025]. Available from: https://hackelvalle.org/

[523] BA-CSIRT. BA-CSIRT [online]. Buenos Aires: BA-CSIRT, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/ba-csirt/

[524] Organized by the Buenos Aires City Government, these free cybersecurity talks are held in local community centers across the city. Topics include: Online scams and fraud, Identity theft, Safe internet practices

[525] GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. La Ciudad ofrece charlas gratuitas de ciberseguridad en las comunas para prevenir engaños [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, 1 March 2024 [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/noticias/la-ciudad-ofrece-charlas-gratuitas-de-ciberseguridad-en-las-comunas-para-prevenir-enganos

[526] LINARES, Gustavo. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/gustavo-linares-705713b/?originalSubdomain=ar

1.1.1.1. César Torres: Secretary of Government and Citizen Liaison of the Buenos Aires Government[527]

1.2. BA-CSIRT's Cybersecurity Alerts & Resources[528]

1.3. CyberCity V[529] – Citizen Cybersecurity Day[530]

1.3.1. Gustavo Linares[531]: Director General of Information Security of the Government of the City of Buenos Aires

1.4. After Cyber[532] 2025 – ZULA Ciberseguridad[533]

1.5. "Con Vos en la Web"[534]

1.6. Cibersecurity LATAM LinkedIn Group[535] [536]

1.7. Internet Society Argentina Chapter (ISOC)[537]

1.7.1. Olga Cavalli[538]: President

2. **Educational Outreach** – High schools, public workshops, hackathons targeting non-professional audiences.

2.1. Argentina Cibersegura[539]

2.1.1. Federico Perez Acquisto: President[540]

---

[527] TORRES, César. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/c%C3%A9sar-torres-748b78103/?originalSubdomain=ar

[528] GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. ¿Quiénes somos y qué hacemos? [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/jefaturadegabinete/centro-de-ciberseguridad/quienes-somos-y-que-hacemos

[529] A full-day event organized by the Buenos Aires government to promote cybersecurity awareness among residents. Includes workshops, interactive activities, and expert talks

[530] GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. Cybercity: V Jornada de Ciberseguridad Ciudadana [online]. Buenos Aires: Gobierno de la Ciudad Autónoma de Buenos Aires, 30 April 2025 [Accessed 16 August 2025]. Available from: https://buenosaires.gob.ar/noticias/cybercity-v-jornada-de-ciberseguridad-ciudadana

[531] LINARES, Gustavo. LinkedIn profile [online]. Buenos Aires: LinkedIn Corporation, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/gustavo-linares-705713b/?originalSubdomain=ar

[532] Community talks & networking in Puerto Madero

[533] BURASTERO, Alan. Ciberseguridad awareness: concientización [online]. LinkedIn, 2025 [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/alanburastero_ciberseguridad-awareness-concientizaciaejn-activity-7334252196475072513-qtFQ

[534] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN. Con Vos en la Web [online]. Buenos Aires: Argentina.gob.ar, [Accessed 16 August 2025]. Available from: https://www.argentina.gob.ar/justicia/convosenlaweb

[535] CIBERSEGURIDAD LATAM. ¡Hola a todos! Queremos invitarlos a participar... [online]. LinkedIn, 2025 [Accessed 16 August 2025]. Available from: https://www.linkedin.com/posts/ciberseguridadlatam_hola-a-todos-queremos-invitarlos-a-participar-activity-7361424893252370433-3sWH

[536] A growing professional and semi-professional community sharing awareness content

[537] ISOC Argentina. Internet Society – Argentina Chapter official website [online]. ISOC Argentina, [Accessed 19 August 2025]. Available from: https://isoc.org.ar/. Is a nonprofit organization that promotes the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

[538] CILLO, Vanesa. LinkedIn profile [online]. LinkedIn, [Accessed 18 August 2025]. Available from: https://www.linkedin.com/in/vanesacillo/

[539] ARGENTINA CIBERSEGURA. Charlas en escuelas [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/charlas-en-escuelas. Established initiative that offers in-person and online talks for students ages 7 and up, covering topics such as: identity and digital footprint, online safety, digital violence and digital citizenship

[540] ARGENTINA CIBERSEGURA. Quiénes somos [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/quienes-somos

2.1.1.1. “My Secure Network” Course[541]

2.2. Salta CyberSecurity Club[542] [543]

2.3. Sadosky Foundation[544] [545]

3. **Social & Inclusion Programs** – NGOs or initiatives that promote tech inclusion for underrepresented groups (e.g., women in tech, low-income youth).

3.1. NGO Securances[546]

3.1.1.1. Jorge Abanto: President[547]

3.2. Chicas en Tecnología[548] [549]

3.2.1. PUMM | Programando un Mundo Mejor[550]

3.2.1.1. Vanesa Cillo[551]: Board Member

3.2.1.2. Lucia Mauritzen: Executive Director[552]

---

[541] ARGENTINA CIBERSEGURA. Mi Red Segura – Guillermo Brea [online]. Buenos Aires: Argentina Cibersegura, [Accessed 16 August 2025]. Available from: https://www.argentinacibersegura.org/mi-red-segura/#:~:text=Guillermo%20Brea-,Guillermo%20Brea,e%20instituciones%20p%C3%BAblicas%20y%20privadas.&text=Guillermo%20Brea%20es%20uno%20de,en%20media%20docena%20de%20pa%C3%ADses.

[542] SALTA CYBERSECURITY CLUB. Salta Cybersecurity Club [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/salta-cybersecurity-club/

[543] SALTA CYBERSECURITY CLUB. Salta Cybersecurity Club [online]. Salta: Salta Cybersecurity Club, [Accessed 16 August 2025]. Available from: https://saltacybersecurity.club/. A community of students, professionals, and enthusiasts passionate about cybersecurity that aims to create a shared space where people can discuss, learn, and share knowledge.

[544] ARGENTINA.GOB.AR. Becas de formación en seguridad informática para agentes del Estado [online]. Buenos Aires: Secretaría de Innovación Pública, [Accessed 16 August 2025]. Available from: https://www.argentina.gob.ar/noticias/becas-de-formacion-en-seguridad-informatica-para-agentes-del-estado

[545] FUNDACIÓN SADOSKY. Fundación Sadosky [online]. Buenos Aires: Fundación Sadosky, [Accessed 16 August 2025]. Available from: https://fundacionsadosky.org.ar/. A public-private foundation that promotes science and technology education in Argentina. Through its Cybersecurity Program, it offers webinars, school outreach, and training for public sector employees. It also collaborates with universities and government agencies to strengthen cybersecurity capabilities.

[546] SECURANCES. Awareness [online]. Buenos Aires: Securances, [Accessed 16 August 2025]. Available from: https://securances.org/web/awareness/

[547] LinkedIn. (n.d.). Jorge Abanto – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/jorge-abanto-peru/

[548] CHICAS EN TECNOLOGÍA. Chicas en Tecnología [online]. Buenos Aires: Chicas en Tecnología, [Accessed 16 August 2025]. Available from: https://chicasentecnologia.org/. Nonprofit organization that seeks to reduce the gender gap in the technology sector. It is dedicated to motivating, training, and supporting young women to engage in technology careers and ventures, providing free programs and resources to develop their digital skills and encourage their participation in the sector.

[549] CHICAS EN TECNOLOGÍA. Chicas en Tecnología [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/company/chicasentecnologia/

[550] Evento PUMM [online]. Buenos Aires: Chicas en Tecnología, [Accessed 16 August 2025]. Available from: https://chicasentecnologia.org/eventopumm/

[551] CILLO, Vanesa. LinkedIn profile [online]. LinkedIn, [Accessed 16 August 2025]. Available from: https://www.linkedin.com/in/vanesacillo/

[552] LinkedIn. (n.d.). Lucía Mauritzen – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/luciamauritzen/

3.3. Cybercirujas[553] [554]

Annex 16: Internal - Argentina

1. **Executive Leadership & Management:**
   - 1.1. Francisco Müller Amato: Co-Founder & Chairman[555]
   - 1.2. Federico Kirschbaum: CEO & Co-Founder[556]
   - 1.3. Martin D. Tartarelli: COO[557]
   - 1.4. Santiago Fernandez Boccacci: CFO[558]
   - 1.5. Joshua Mador: VP of Business Development and International Sales[559]

2. **Sales, Marketing & Client Relations:**
   - 2.1. Marcos Carabajal: (CRO) Chief Revenue Officer[560]
   - 2.2. Cecilia Garmendia: Marketing and Communication Leader[561]
   - 2.3. María Florencia Migliorisi: Strategic Storyteller | Content, Community, Culture[562]
   - 2.4. Nicolás Bunader: Key Account Manager[563]
   - 2.5. Octavio Boggiano: Enterprise Solutions Specialist[564]

3. **Technical & Development Teams:**

[553] OTERO, Mariana. Los 'cybercirujas', el movimiento que desafía el 'usar y tirar' de la tecnología en Argentina [online]. Madrid: El País, [Accessed 16 August 2025]. Available from: https://elpais.com/america-futura/2024-09-02/los-cybercirujas-el-movimiento-que-desafia-el-usar-y-tirar-de-la-tecnologia-en-argentina.html

[554] CYBERCIRUJAS CLUB. Cybercirujas [online]. Buenos Aires: Cybercirujas Club, [Accessed 16 August 2025]. Available from: https://linktr.ee/cybercirujas. A grassroots movement that refurbishes discarded tech and promotes digital inclusion in underserved communities across Argentina. They host repair workshops, donation campaigns, and digital self-defense talks, often using free software and recycled devices.

[555] LinkedIn. (n.d.). Francisco Müller Amato – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/famato

[556] LinkedIn. (n.d.). Federico Kreplak – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/fedek/

[557] LinkedIn. (n.d.). Martín D. Tartarelli – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/tartamar/

[558] LinkedIn. (n.d.). Santiago Fernández Boccacci – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/santiago-fernandez-boccacci-16522854/

[559] LinkedIn. (n.d.). Joshua Amador – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/joshuamador/

[560] LinkedIn. (n.d.). Marcos Carabajal – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/marcos-carabajal-87119137/

[561] LinkedIn. (n.d.). *Cecilia Garmendia* – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/ceciliagarmendia/

[562] LinkedIn. (n.d.). Florencia Migliorisi – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/flormigliorisi/

[563] LinkedIn. (n.d.). Nicolás Bunader – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/nicolasbunader/

[564] LinkedIn. (n.d.). Octavio Boggiano – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/octavioboggiano/

3.1. Matias Massut: UI Designer[565]

3.1.1. Merlin Müller Amato Espert Pucheu: Senior Researcher[566]

3.1.2. David Alejandro Kraus: Sr Back-End Developer[567]

3.1.3. Octavio Gianatiempo: Security Researcher[568]

3.1.4. Gaston Aznarez: Security Researcher[569]

3.1.5. Agustin Baranowski: Security Analyst[570]

3.1.6. Juan Mamani: Security Analyst | Pentester[571]

3.1.7. Roberto Focke: Computer Scientist[572]

4. **Administrative & Support Staff:**

4.1. Mariana Echeverría: People & Culture at Faraday[573]

Annex 17: Variables Crossing - Indirect / Non Governmental Forums and Associations

Segment	Awareness Level	Engagement Frequency	Potential Influence	Sectoral Visibility Contribution	Knowledge Exchange & Networking
Argentina					
International Strategic Forums	High	Consistent	High	High	Partial
National Industry Conferences & Forums	High	Consistent	High	High	Full
Professional	Medium	Occasional	HIgh	Medium	Full

[565] LinkedIn. (n.d.). Matías Massut – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/matias-massut-a7453914a/

[566] LinkedIn. (n.d.). Merlin Müller Amato Espert Pucheu – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/merlin-m%C3%BCller-amato-espert-pucheu-4a2044218/

[567] LinkedIn. (n.d.). David Alejandro Kraus – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/david-alejandro-kraus-a3893b56/

[568]LinkedIn. (n.d.). Octavio Gianatiempo – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/octavio-gianatiempo/

[569] LinkedIn. (n.d.). Gastón Aznárez – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/gastonaznarez/

[570] LinkedIn. (n.d.). Agustín Baranowski – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/agustinbaranowski/

[571] LinkedIn. (n.d.). Juan Mamani (Aka. z1ro) – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/z1ro/

[572] LinkedIn. (n.d.). Roberto Focke – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/roberto-focke-305043332/

[573] LinkedIn. (n.d.). Mariana Echeverría – LinkedIn profile. LinkedIn. [Accessed 17 August 2025]. Available from: https://www.linkedin.com/in/marianaecheverria/

Associations & Networks					
Academic - Industry Collaborations	Medium	Consistent	Medium	Medium	Full

Annex 18: Variables Crossing - Community

Segment	Awareness Level	Engagement Frequency	Potential Influence	Contribution for Local Awareness	Inclusivity & Social Impact
Argentina					
Local Awareness & Engagement Initiatives	Low	Consistent	Medium	Medium	Partial
Educational Outreach Programs and activities	Low	Occasional	Medium	Full	Partial
Social Inclusion Programs	Medium	Occasional	Medium	Partial	Full

Annex 19: Variables Crossing - Internal

Segment	Awareness Level	Engagement Frequency	Potential Influence	Visibility of Contributions	Talent Retention Signals
Argentina					
Executive Leadership & Management	High	Consistent	High	High	Medium
Sales, Marketing & Client Relations	Medium	Occasional	Medium	Medium	Medium

Technical, Development & Operations Teams	High	Consistent	High	Medium	High
Support & Administrative Staff	Low	Occasional	Low	Low	Medium