Cybersecurity in Computer Science Curricula of Federal Educational Institutions in Southern Brazil

Ricardo de la Rocha Ladeira[1], Gabriel Eduardo Lima[2]

[1]Instituto Federal Catarinense – Campus Blumenau – Blumenau/SC – Brasil
[2]Universidade Federal do Paraná – Curitiba/PR – Brasil

ricardo.ladeira@ifc.edu.br, gelima@inf.ufpr.br

Abstract. *Cybersecurity has grown in formal education in recent years, making its inclusion in Computer Science curricula more important. This paper analyzes Pedagogical Development Programs of federal Computer Science programs in southern Brazil to examine how Cybersecurity is addressed, showing that most curricula cover the topic only to a limited extent.*

1. Introduction

Data generation is growing fast, making it key to ensure the pillars of Information Security — confidentiality, integrity, and availability — for sustained service continuity and protection against cyber threats [Bourgeois *et al*. 2019; Stallings 2024]. Brazil is among the most impacted countries in cyber losses, the hardest hit in South America [Bruce *et al*. 2024], with one-third of companies reporting losses over $1 million [PwC 2025].

It is essential to train people and foster a security culture [Bishop 2025], engaging professionals and users. This need is reinforced by a persistent shortage of Information Security specialists. ISC2 reports 231,927 unfilled cybersecurity positions in Brazil in 2023, and a gap of 328,397 professionals in Latin America in 2024, which limits organizations' capacity to prevent and respond to incidents [ISC2 2023; ISC2 2024].

Formal education promotes cybersecurity culture and expands training for qualified professionals [Kuforiji 2025] by including Information Security content in technical and higher education curricula. It trains professionals and citizens who are more aware of the risks and best practices associated with the use of technology.

Higher education Computer Science programs in Brazil must provide skills and competencies that allow students to identify and manage risks in computing equipment, apply core principles such as abstraction, security, and system evolution, and recognize these as fundamental to Computer Science [Ministério da Educação 2016].

Therefore, this study investigates how Cybersecurity is addressed in Computer Science programs at federal institutions in Southern Brazil, seeking to understand the role the topic plays in undergraduate education. The choice to focus on federal institutions in Southern Brazil is justified by the concentration of long-standing Computer Science programs in this region and their relevance in shaping the local educational landscape. By examining these curricula collectively, this study captures

specific characteristics to this regional context. The contribution of this work is to provide a regional overview of Security-related content within these curricula.

The focus on Computer Science programs is justified because they provide the broadest and most generalist training among Computing degrees in the Brazilian educational system, according to the competencies established in the National Curriculum Guidelines [Ministério da Educação 2016]. Furthermore, this corresponds to the authors' area of expertise, which offers familiarity with institutional structures, curricular documents and the regional educational context.

2. Related Works

Literature on Computer Security in Computer Science education shows interest in how the area is addressed in curricula and pedagogical practices.

Abu-Taieh (2021) consolidates a body of knowledge in Cybersecurity and proposes essential competencies based on 61 master's programs worldwide. He outlines minimum curricular content, supporting this study's focus on Cybersecurity in Southern Brazil's federal Computer Science curricula.

Cristani *et al*. (2020) overview Information Systems Security teaching in Brazil, combining curriculum analysis with surveys of undergraduate and graduate students. Most programs had at least one mandatory discipline, though workload did not correlate with student performance. Their conclusions provide a national framework to contextualize the regional analysis in this study.

De Barros (2023) analyzes cybersecurity education in Brazil and its potential to prevent digital security incidents, highlighting public policies and national awareness. This study, in turn, investigates the extent to which Security topics are integrated into federal Computer Science programs in Southern Brazil.

Meireles & Tomaz (2025) validate the present methodology through a detailed documentary analysis of Pedagogical Development Programs. Focusing on Southeast Brazil, they find strong Information Security coverage in bachelor's and technology degrees, but limited presence in teacher training, highlighting the need for more consistent curricular guidelines and for broadening the national perspective on Computer Security education.

This study differs from previous works by focusing on Computer Science curricula from federal institutions in Southern Brazil. It offers a specific perspective on Computer Security and its subareas and helps identify local particularities, revealing patterns and gaps in Security teaching.

3. Method

The study first identified federal institutions in Southern Brazil offering undergraduate Computer Science degrees, using e-MEC[1] data. The most recent curricula available on

[1]https://emec.mec.gov.br/

institutional websites were downloaded and analyzed in October 2025. When multiple versions existed, the latest was used. Missing matrices or descriptions were supplemented by files like teaching plans. Links to all materials collected are in Appendix A[2].

The analysis focused on Security-related courses, such as Network Security and Information Security. In addition, related sub-areas, such as Cryptography and Systems Auditing, were considered. The course descriptions were also analyzed to confirm whether the content effectively addressed security topics. Courses mentioning *segurança* (security, in Portuguese) or related terms were also included.

This work does not claim to be a comprehensive guide to Computer Security disciplines, as topics may appear transversally or in components not explicitly labeled as Security. The analysis is limited to syllabi, acknowledging some content may be addressed elsewhere.

As no standard glossary or universally accepted list of terms exists, the expressions analyzed were defined by the authors and include: authenticity, authorization, access control, confidentiality, cryptography, availability, integrity, privacy, cryptographic protocols, and security. The context matters: *Cybersecurity* and *Information Security* are relevant, while *Occupational Safety* is not. In addition, although security topics may appear in courses like *Computer Networks*, *Operating Systems* or *Database*, only disciplines explicitly labeled with security-related terms were counted.

For each identified course component, its workload, the stage in which it is offered and whether it is mandatory or optional were recorded. The stage was noted as a range when an elective could appear in different stages of the program, and marked as undefined when no stage was indicated.

4. Results & Discussion

Twenty undergraduate Computer Science programs were found in federal higher education institutions in Southern Brazil. The cities where these programs are offered are marked with a red dot on the map of the Southern region of Brazil, as shown in Figure 1.

[2]Available at `https://github.com/ricardodelarocha/Research/blob/main/Computer-Science-Curricula/Appendix-A-v2-en.pdf`.

Figure 1. Map of the Southern region of Brazil showing the location of municipalities where Computer Science is offered at federal educational institutions.

Table 1 lists the institutions, cities where the programs are offered, and the year of the most recent curriculum, grouped by state. The IFFarr curriculum could not be accessed due to the institution's website being unavailable during the research period.

It is observed that 20 programs are offered in different cities and the distribution among the states is uniform (six programs in Paraná, seven in Rio Grande do Sul and seven in Santa Catarina). It was observed that UTFPR and IFC offer the most programs (four each). They are also the only ones that offer the program on more than one campus.

Table 1. Institutions offering Computer Science programs and their respective campuses.

State	**Educational Institution**	***Campus***	**Most recent Pedagogical Development Program found**
Paraná	IFPR	Pinhais	2025
	UFPR	Curitiba	2023
	UTFPR	Campo Mourão	2011
		Medianeira	2023
		Ponta Grossa	2022
		Santa Helena	2023
Rio Grande do Sul	IFFarr	Frederico Westphalen	Unavailable
	IFRS	Ibirubá	2019
	IFSul	Passo Fundo	2025
	UFPel	Pelotas	2015
	UFRGS	Porto Alegre	2025
	UFSM	Santa Maria	2024

	UNIPAMPA	Alegrete	2023
Santa Catarina	IFC	Blumenau	2023
		Concórdia	2024
		Rio do Sul	2022
		Videira	2022
	IFSC	Lages	2025
	UFFS	Chapecó	2025
	UFSC	Florianópolis	2007

The analysis of the 19 pedagogical programs indicates their structure is reasonably up-to-date; 15 (78.95%) were published in the last five years. This update suggests adaptation to regulations, faculty profiles, and local productive arrangements.

It is worth noting that the program offerings are balanced between Federal Institutes and Federal Universities: nine out of the 20 (45%) programs are offered by Federal Institutes and eleven (55%) are offered by Federal Universities.

From 19 curricula, 22 Security-focused courses were identified by title. There is a wide diversity of names (16), often with distinct syllabi addressing different security aspects. Table 2 lists the subjects containing the term *segurança* (security) in the title.

Table 2. Courses explicitly about Cybersecurity and the institutions that offer them.

Course Component	**Institution(s)**
Computer Network Security	IFSul
Computer Security (*Segurança de Computadores* in portuguese)	UFPel
Computer Security (*Segurança Computacional* in portuguese)	IFC Blumenau, IFSC, UFPR
Cybersecurity	UTFPR Santa Helena
Data Science for Security	UFPR
Information Security	IFC Concórdia, IFPR, Unipampa
Information Security in Open Source Environments	UTFPR Campo Mourão
Information Technology Security	IFRS
Security in Computing	UFSC
Security in Computer Network	UTFPR Medianeira
Security in Computer Systems	UFRGS
Special Topics in Systems Security	IFC Videira
Systems and Information Security Topics	UNIPAMPA
Systems Security	IFC Videira
Systems Security and Auditing	UFFS, UTFPR Campo Mourão, UTFPR Ponta Grossa
Topics in Computer Security	UFPR

Among these 22 disciplines, nine are mandatory and 13 optional. In some cases, students may choose courses from other Computing areas, and elective status does not guarantee that the course will be offered.

Some programs address Security indirectly through other disciplines. Analyzing the 19 curriculum plans, 99 disciplines were found covering Security or its sub-areas, fully or partially. The five most frequently appearing components are listed in Table 3.

Table 3. Most frequently offered Security-related course components.

Rank	Course Component	Appearances
#1	Database II, Database 2 or Advanced Database	10
#2	Computer Networks II or Computer Networks 2	9
#3	Operating Systems, Operating Systems I, or Operating Systems “A”	6
#4	Internet of Things	5
#5	Web Development II	4

Curricular analysis revealed Security content variations: in some programs it appears as mandatory subjects, in others only as electives. Among the 99 identified disciplines, 55 are mandatory and 44 are elective, showing a slight predominance of mandatory courses. The distribution of mandatory and elective courses varies across institutions. Only one curriculum (UNIPAMPA) lists all Security subjects as elective.

Course workloads ranged from 30 to 80 hours, generally concentrated in the final stages. Two complementary hypotheses arise: (i) the topic is addressed only after students gain fundamentals in Networks, Operating Systems, and Programming; and (ii) curricular structures suggest that Cybersecurity remains largely peripheral, treated as a specialization rather than a core component of Computing education. Differences among institutions may also reflect faculty availability, as the offer of Security courses often depends on having specialists in the area.

The subjects offered, their workloads, the stages of the course in which they are taught, and whether the components are mandatory are available in Appendix B[3].

5. Conclusion

This work analyzed Computer Science programs in Southern Brazil’s Federal Education Network, focusing on disciplines addressing Computer Security, using the most recent curricula from official institutional websites. The presence of Cybersecurity is notable but varies among institutions. Twenty-two courses directly focus on Security, nine mandatory and 13 elective, and 99 courses address the topic explicitly, fully or partially.

Most of the specific subjects are offered in final stages, demonstrating that students engage with Cybersecurity after mastering the fundamentals. Furthermore, 13 of the 22 subjects are mandatory, which is not ideal and suggests that the discipline remains peripheral and supplementary, needing greater integration as an essential skill.

This analysis is a starting point for Computer Security investigations in Computer Science curricula. Future research can (i) analyze guidelines (CESeg/SBC,

[3]Available at `https://github.com/ricardodelarocha/Research/blob/main/Computer-Science-Curricula/Appendix-B-v2-en.pdf`.

NICE and ACM/IEEE) to compare institutional practices with recommended competency structures, (ii) analyze all Southern region programs (including uncovered public and private institutions) and (iii) survey Brazil's Federal Network to examine Security discipline inclusion, revealing patterns, differences and trends, and (iv) investigate faculty qualification profiles and research areas within federal institutions to understand how teaching staff expertise relates to the Security courses offered.

References

Abu-Taieh, E. M. (2017). Cyber security body of knowledge. In 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2), 104-111.

de Barros, J. A. A. (2023). Segurança cibernética nas escolas e universidades brasileiras: avaliando a inserção da educação cibernética no sistema educacional brasileiro e seus efeitos na prevenção de incidentes cibernéticos.

Bishop, G. (2025). Cybersecurity Culture. CRC Press.

Bourgeois, D. T., Smith, J. L., Wang, S., & Mortati, J. (2019). Information systems for business and beyond. Saylor Academy. Open Textbooks. 1.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one, 19(4).

Cristani, M., Alves, W., Pereira, G., and Lazarin, N. (2020). Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no Brasil. In Simpósio Brasileiro de Sistemas de Informação 2020.

ISC2 (2024). Cybersecurity Workforce Study 2023.

ISC2 (2024). Cybersecurity Workforce Study 2024.

Kuforiji, J. (2025). The Importance of Integrating Security Education into University Curricula and Professional Certifications. IJTMH, 11(03), 1-10.

Meireles, B. R. A. V., & Tomaz, L. B. P. (2025). Segurança da Informação em Foco: Análise Curricular dos Cursos de Computação da Rede Federal no Sudeste do Brasil. In Simpósio Brasileiro de Cibersegurança 2025.

Ministério da Educação (2016). Resolução CNE/CES nº 5, de 16 de novembro de 2016.

PwC, PricewaterhouseCoopers Brasil (2025). Resiliência cibernética: Como superar os desafios diante da expansão dos ataques. Pesquisa Global Digital Trust Insights 2025.

Stallings, W. (2024). Computer Security: Principles and Practice. 5th ed. Pearson.