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
[2]Universidade Federal do Paraná

December 9, 2025

Table of Contents

Motivation

- Data generation is growing rapidly, increasing risks (Bourgeois *et al.*, 2019).
- Brazil is heavily impacted by cyber losses (Bruce *et al.*, 2024), with 1/3 of its companies losing over US$1 million in 2025 (PwC, 2025).
- A Lack of specialists weakens prevention and response (ISC2, 2023, 2024).

Figure: Amount of Data Created Daily. Source (Duarte, 2025).

Problem & Justification

- A **cybersecurity culture** depends on **continuous training** (Bishop, 2025).
- **Formal education** broadens **awareness** and promotes **good** digital **practices** (Kuforiji, 2025).
- **Curriculum guidelines** require **competencies** to **identify and mitigate risks** (Ministério da Educação, 2016).
- It is not yet known **how cybersecurity is addressed in curricula** in the South.
    - **Traditional programs** and a wide range of federal offerings.
- **Focus on Computer Science** – CS due to its more generalist background.

- **Map the Cybersecurity courses** in the curricula of federal CS programs in the South.
- Verify **mandatory/elective status**, **offering semester**, and **workloads**.
- **Identify patterns**, **gaps**, and regional **particularities**.

Related Works

- Abu-Taieh (2017) proposes an essential body of knowledge in Cybersecurity.
- Jesus Cristani *et al.* (2020) analyze Information Systems Programs in Brazil; most have at least one mandatory course on the topic.
- Meireles and Tomaz (2025): validate the method and find solid Security coverage in Southeast degrees, but it is limited in teacher training.

- A focused view of Southern Brazil is lacking; this work offers an **initial step** toward filling that gap.

Method

- Identification of federal institutions in the Southern region via e-MEC.
- Collection of the most recent available curriculum (October 2025).
- Analysis of syllabi to verify Cybersecurity-related content.
  - Searched terms: *segurança* (security) , *criptografia* (cryptography), *confidencialidade* (confidentiality), *integridade* (integrity), etc.

- This is an exploratory analysis; it does not aim to provide a comprehensive mapping, but rather to establish an **initial basis** for broader future studies.

Limitations

- Dependence on available syllabi.
- Course titles do not always reflect the actual content.
- Searched terms may not be exhaustive.
- Lack of information on whether courses are actually offered every year.
- Lack of information on workload hours (class hours vs. clock hours).

Sample Programs

- 20 programs identified; 19 Development Programs analyzed.
- Balanced distribution: PR (6), SC (7), RS (7).

- Balanced network: 9 Federal Institutes and 11 Universities.
- Pedagogical Programs indicate that their structure is reasonably up-to-date: 78.95% have been updated in the last 5 years.

Cybersecurity Courses (overview)

- 22 courses with "*segurança*" (security) in the title.
- 9 mandatory / 13 optional: electives predominate.
- Strong diversity of names (16): suggests distinct approaches among institutions.
- Some course names:
  - *Cibersegurança* (Cybersecurity)
  - *Ciência de Dados para Segurança* (Data Science for Security)
  - *Segurança em Redes de Computadores* (Security in Computer Networks)
  - *Segurança de Sistemas* (Systems Security)
  - *Tópicos em Segurança Computacional* (Topics in Computer Security)

Related Disciplines (partial content)

- 99 curricular components partially address cybersecurity topics.

  Table: 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

- Cybersecurity **is present**, but in **non-uniform** ways.

Related Disciplines (partial content)

- Distributed systems (from Pedagogical Development Program, in portuguese):
    1. *Transações distribuídas, interoperabilidade, consciência de contexto, **segurança e privacidade**, adaptabilidade, metamodelo de ambientes e descoberta de recursos aplicados à computação em grade, computação em nuvem, computação ubíqua e computação móvel.*
    2. *Problemas Básicos em Computação Distribuída: comunicação, coordenação e sincronização de processos. Exclusão Mútua, Difusão de Mensagens. Transações Distribuídas. **Tolerância a Faltas**. Exemplos de Sistemas Distribuídos. Memória Compartilhada. Computação ubíqua. Middleware para a concepção de sistemas distribuídos.*

Mandatory Offer, Course Workload and phase

- 55 mandatory courses and 44 electives in total.
- All programs include at least one mandatory course covering security (fully or partially).
  - Electives may reveal curricular priorities and dependence on specialized faculty who may not always be available.

- Workloads ranging from 30 to 80 hours: high variability.

- Most courses are offered in the final phases.
  - This may reflect a dependency on technical prerequisites (networks, operating systems, programming).

Key Findings, Interpretation & Implications

- Security-related content is distributed inconsistently across curricula.
  - Course titles and descriptions vary widely, showing little standardization.

- Security courses typically appear only in the final stages of the degree.
  - Security remains peripheral, not a core part of most programs.

- The number of instructors in Security may limit how consistently and how deeply the topic is taught.

- **Risk**: students may graduate with a superficial understanding of the area.
- **Opportunity**: treat Security as a required component integrated across all stages of the program.
  - May already be happening!

Conclusion

- There is an institutional effort, but with great variability.

- 22 specific courses and 99 Cybersecurity-related courses show reasonable interest.
  - Only one program does not have security (fully or partially) covered in a mandatory course.

- Cybersecurity needs to be more central in the curriculum.
  - It certainly depends on specialized teachers!

Future Work

- Compare curricula with NICE, CESeg/SBC, and ACM/IEEE guidelines.
- Expand the analysis to include public and private institutions in the South.
- Study of the national Federal Network to map trends.
- Investigate teacher profiles and their influence on course offerings.
- Investigate sub-areas covered by the Development Programs (cryptography, authentication, etc.).

ABU-TAIEH, Evon MO. **Cyber security body of knowledge**. *In:* IEEE. 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2). [*S. l.: s. n.*], 2017. p. 104–111.

BISHOP, Gulsebnem. **Cybersecurity Culture**. [*S. l.*]: CRC Press, 2025.

BOURGEOIS, David T *et al.* **Information systems for business and beyond**. [*S. l.*]: Saylor Academy, 2019.

BRUCE, Miranda *et al.* Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one, Public Library of Science, v. 19, n. 4, e0297312, 2024.

DUARTE, Fabio. **Amount of Data Created Daily (2025)**. [*S. l.: s. n.*], 2025. https://explodingtopics.com/blog/data-generated-per-day. Visited on: 7 Dec. 2025.

ISC2. **Cybersecurity Workforce Study 2023**. [*S. l.*], 2023.

ISC2. **Cybersecurity Workforce Study 2024**. [*S. l.*], 2024.

JESUS CRISTANI, Matheus de *et al*. Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no brasil. *In:* SBC. SIMPÓSIO Brasileiro de Sistemas de Informação (SBSI). [*S. l.: s. n.*], 2020. p. 1–4.

KUFORIJI, John. The importance of integrating security education into university curricula and professional certifications. International Journal of Technology, Management and Humanities, v. 11, n. 03, p. 1–10, 2025.

MEIRELES, Bruno Raphael Andrade Varjao; TOMAZ, Lídia Bononi Paiva. Segurança da Informação em Foco: Análise Curricular dos Cursos de Computação da Rede Federal no Sudeste do Brasil. *In:* SBC. SIMPÓSIO Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg). [*S. l.: s. n.*], 2025. p. 273–282.

MINISTÉRIO DA EDUCAÇÃO. Resolução CNE/CES nº 5, de 16 de novembro de 2016. [*S. l.: s. n.*], 2016. Conselho Nacional de Educação. Disponível em: http://portal.mec.gov.br.

PWC. Resiliência cibernética: Como superar os desafios diante da expansão dos ataques. [*S. l.*], 2025. Pesquisa Global Digital Trust Insights 2025.

Thank you!

https://github.com/ricardodelarocha/Research/blob/main/Computer-Science-Curricula/

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
[2]Universidade Federal do Paraná

December 9, 2025

Search by sub-areas (cryptography)

- No results for courses offered in a foreign language.

- Data on the **cryptography** subfield:
    - 21 courses were found across 16 programs.
        - PR: 7 courses; 5 programs;
        - RS: 8 courses; 5 programs; and
        - SC: 6 courses; 6 programs.
    - 11 mandatory and 10 optional
        - Uniform distribution among the states.
        - In only ten courses the topic is covered in a mandatory way.
        - Again, the topic can be approached in a cross-cutting manner.
    - Workload between 60 and 72 hours
        - **outlier**: 40 hours (IFSC)
    - Courses between 4th and 10th semesters; most of them taught in 7th and 8th.

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
[2]Universidade Federal do Paraná

December 9, 2025