Information Security Report

Ref. 2025/2026

Information security is a highly relevant topic for Cemig because, in an increasingly connected world, controlling and protecting the company's data network is essential. Sound management of technology resources and assurance of security are fundamental to mitigating risks related to leakage and misuse of personal data, as well as preventing unauthorized access to confidential and strategic information. With this objective, Cemig has continuously invested in its Information Technology (IT) infrastructure, seeking to strengthen IT governance and service management, as well as information security.

Information-security governance and security are managed in the company by the Vice Presidency of Information Technology (VPI), which has a management team dedicated exclusively to the cybersecurity process.

The Board of Directors is supported by the Vice Presidency of Information Technology, which provides monthly reports presenting relevant security actions and implementation status. As one of the Company's main risks, it is also monitored by the Risk Committee within the scope of the Board of Directors.

Cemig has an Information Security and Cybersecurity Policy that includes guidelines and principles related to the topic. This policy defines the guidelines, responsibilities, and objectives established to ensure the protection requirements of the Company's information environment and cybersecurity.

It can be accessed on the company's website at www.cemig.com.br/en/wp-content/uploads/sites/2/2026/06/information-security-policy-cyber-security.pdf.

C2M2 - Cybersecurity Capability Maturity Model

Cemig adopted the C2M2 framework (Cybersecurity Capability Maturity Model) to drive the continuous improvement of its maturity in Cybersecurity and Information Security.

C2M2 is a tool developed by the U.S. Department of Energy to help organizations

assess and improve their cybersecurity capabilities. It focuses on both information technology (IT) assets and environments and operational technology (OT).

Domains: The C2M2 framework is divided into ten domains, each representing a key area of cybersecurity practice:

Our company reached Level 3 in the C2M2 framework in 4 of the 10 domains and level 2 in all domains, indicating that our cybersecurity practices are managed and applied consistently. This achievement demonstrates our commitment to maintaining a robust cybersecurity posture and protecting our assets and operations.

Figure 1: Tracking of t he C2M2 framework (Cybersecurity Capability Maturity Model) to drive the continuous improvement of Cemig's maturity in Cybersecurity and Information Security.

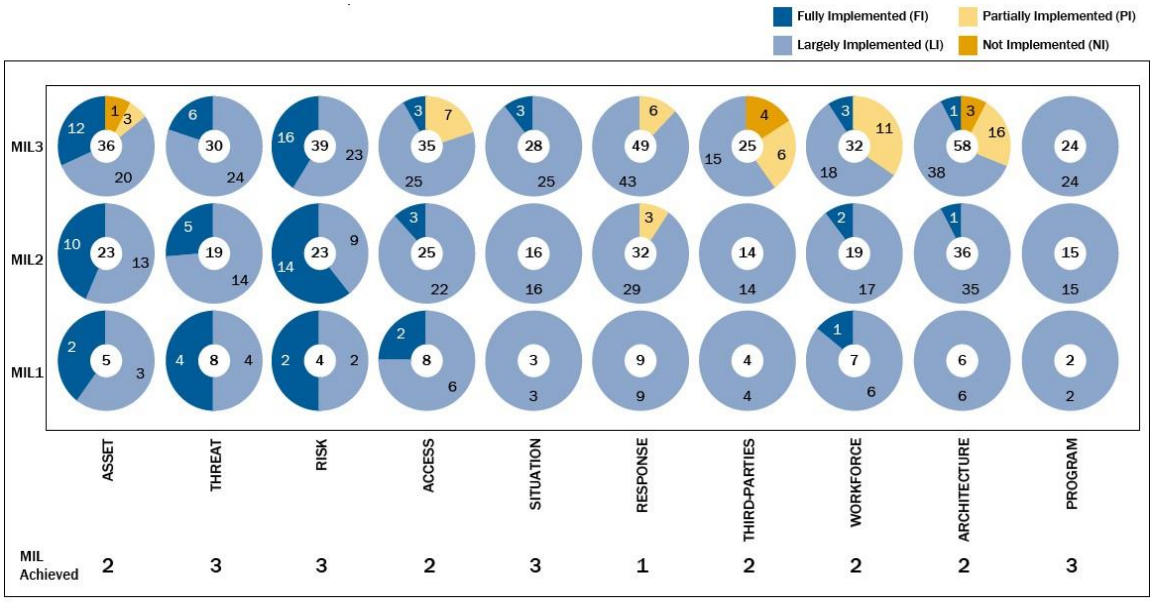

Figure 3: Summary of Responses by MIL and Domain

Cemig outsources data-center infrastructure, managed services, and security operations to TIVIT. TIVIT has a continuity plan and tests it periodically; it is certified under the international ISO 22301:2019 standard, as shown in the certificate below.

Figure 2: ISO 22301:2019 Certificate - Business Continuity Management System

CERTIFICATE

dqs

This is to certify that

TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A.
Site Eldorado

Av. das Nações Unidas, 8501 - 9º andar - Pinheiros
05425-110 São Paulo
Brazil

with the organizational units/sites as listed in the annex

has implemented and maintains a **Business Continuity Management System**.

Scope:
Business continuity management system for information technology, cybersecurity, consulting, and customer management services, operating in public clouds, private clouds, and SAP solutions, in accordance with the "DQS-LMR-004 Planning, Monitoring, and Control - GCN TIVIT" declaration.

Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:

ISO 22301 : 2019

Certificate registration no.	432397 BCM19
Valid from	2025-10-28
Valid until	2028-10-27
Date of certification	2025-09-21

DAkkS Deutsche Akkreditierungsstelle D-ZM-16402-01-00

DQS CFS GmbH
German Association for Sustainability

Guido Eggers
Managing Director

DQS IS A MEMBER OF IQNET

Accredited Body: DQS CFS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
The validity of the certification can only be verified by the QR-code.

1 / 2

Vulnerability Analysis

Vulnerability management process:

Cemig has advanced software solutions for vulnerability management and configuration compliance. These tools perform analysis and scanning of assets and web applications, as well as configuration audits, to ensure robust adherence to cybersecurity best practices and guidelines, with the aim of eliminating and mitigating vulnerabilities related to information security.

Penetration Testing

To simulate a cyberattack and assess the security of systems and the network, we conduct penetration tests through an independent external company to evaluate system resilience against an attack of malicious origin. The independent company performs an attack simulation to identify vulnerabilities in a system or application. This enables the identification of possible improvement points and the establishment of preventive actions.

Cyber Threat Intelligence

In addition, complementing the vulnerability-management process, we monitor the external environment to detect threats through the Cyber Threat Intelligence process. This involves research and monitoring to identify threats such as fake domains, brand abuse, deep-web and dark-web activity, credential leaks, fraud, fake applications, and source-code leaks. The objective is to detect data leaks, fraud, and other threats.

Internal audits of IT infrastructure and/or information-security management systems

Cemig has an Internal Audit team that periodically performs audits covering IT infrastructure. Regarding information-security management systems, the associated risks are addressed through controls assessed in ISAE 3402 assurance reports issued by service providers, as shown in the screenshots below.

Figure 3: Executive Summary of the Internal Audit Result for information-security management systems. 02/10/2024

Figure 4: Internal Audit report related to information-security management systems

Independent external audit of IT infrastructure and/or information-security management systems: please provide the names and standards used (such as ISO 27001)

Cemig has an external auditor (KPMG) that periodically assesses the company's general IT controls (ITGC), covering both infrastructure and information-security aspects. In addition, because Cemig outsources data-center infrastructure, managed services, and security operations, the respective providers deliver ISAE 3402 reports and hold certifications such as ISO 27001, TIER III, CMMI, and PCI DSS, ensuring compliance with international security, quality, and governance standards.

Figure 5: KPMG Assurance Report on Information Technology controls and process

Tivit, the data-center infrastructure provider, also has an integrated Quality Management system that includes several certifications, among which the following stand out:

a) ISO 9001:2015

Figure 6 - ISO 9001:2015 Certificate

b) ISO/IEC 20000-1:2018 - Service Management and ITIL

CERTIFICADO

dqs

Certifica que a empresa

TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A.

TIVIT

Av. das Nações Unidas, 8501 • 9º andar • Pinheiros
05423-110 São Paulo, SP
Brazil

com as unidades relacionadas no anexo

implementou e mantém um **Sistema de Gestão de Serviços.**

Escopo:
Serviços gerenciados de suporte, monitoramento, manutenção e otimização, com atuação em: Sustentação de aplicações, Serviços Gerenciados de Nuvem, Soluções SAP, Serviços Gerenciados de Segurança, Serviços Gerenciados de Mainframe, Detecção e Resposta Gerenciadas, Gerenciamento de Ameaças e Vulnerabilidades, Gerenciamento de Crises e Armazenamento como Serviço.

Através de uma auditoria, documentada em um relatório, foi comprovado que o sistema de gestão cumpre os requisitos da seguinte norma:

ISO / IEC 20000-1 : 2018

Número do certificado	432397 SMS18
Válido a partir de	2024-10-30
Válido até	2027-08-04
Data da certificação	2024-10-30

DAkkS Deutsche Akkreditierungsstelle D-ZM-16074-01-00

DQS IS A MEMBER OF IQNET

DQS GmbH

Christian Gerling
Director Executivo

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
Administrative Office: DQS do Brasil Ltda., Av. Adolfo Pinheiro, 1001 - 3º andar, 04733-100 São Paulo - SP, Brazil
The validity of the certification can only be verified by the QR-code.

1 / 2

c) ISO 22301:2019 Business Continuity Management System

CERTIFICADO

dqs

Certifica-se que a empresa

TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A.

Av. das Nações Unidas, 8501 - 9º andar - Pinheiros
05423-110 São Paulo
Brazil

com as unidades relacionadas no anexo

implementou e mantém um **Business Continuity Management System.**

Âmbito de aplicação:
Serviços de Tecnologia da Informação, Consultoria e Gestão de Clientes com atuação em: Nuvem Pública e Privada: Nuvem Pública, Nuvem Privada, Serviços Gerenciados de Nuvem, Serviços Profissionais, Recuperação de Desastres e proteção de dados, Armazenamento como Serviço, licenciamento; Soluções SAP: Adoção, Gestão, Operação, Suporte, Qualidade.

Através de uma auditoria, documentada em um relatório, foi comprovado que esse Sistema de gestão cumpre os requisitos da seguinte norma:

ISO 22301 : 2019

Número do certificado	432397 BCM19
Data da revisão	2024-09-02
Válido a partir de	2022-10-28
Válido até	2025-10-27
Data da certificação	2022-09-30

DAkkS Deutsche Akkreditierungsstelle D-ZM-19402-01-00

DQS CFS GmbH
German Association for Sustainability

Guido Eggers
Director Executivo

Accredited Body: DQS CFS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
The validity of the certification can only be verified by the QR-code.

1 / 2

Figure 7: Business continuity plan certification report

ISO 27001:2022 Information Security Management System Certificate

CERTIFICADO

dqs

Certifica que a empresa

TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A

TIVIT

Av. das Nações Unidas, 8501 - 9º andar - Pinheiros
05423-110 São Paulo, SP
Brasil

com as unidades relacionadas no anexo

implementou e mantém um **Sistema de Gestão da Segurança da Informação**

Escopo:
Serviços de Tecnologia da Informação, Consultoria e Gestão de Clientes com atuação em: Nuvem Pública e Privada: Nuvem Pública, Nuvem Privada, Serviços Gerenciados de Nuvem, Serviços Profissionais, Recuperação de Desastres e proteção de dados, Armazenamento como Serviço, licenciamento; Cibersegurança: Governança, Risco e Conformidade, Gerenciamento de Ameaças e Vulnerabilidades, Gerenciamento de Identidade e Acesso, CyberLabs, Detecção e Resposta Gerenciadas, Centro de Segurança, Serviços da Equipe Vermelha, Serviços de Segurança Gerenciados.
Techfin: Serviços de pagamentos através de APIs, PIX cash in - Cobrança (cobv) e Varejo (cob), PIX cash out, Abertura e gestão de Conta de Pagamentos, Abertura de contas via API, transferência bancárias, Boletos com registro instantâneo; Split de pagamentos; Webhook de Pagamentos e Repasses em conta; APIs de consultas, Hub Paymenrs, Consulta de boletos registrados e Conta Digital.

Declaração de Aplicabilidade: 31. SEG DOC 001 007. Date 19.06.24.

Através de uma auditoria, documentada em um relatório, foi comprovado que o sistema de gestão cumpre os requisitos da seguinte norma:

ISO / IEC 27001 : 2022

Número do certificado	432397 ISMS22
Válido a partir de	2024-10-30
Válido até	2027-09-19
Data da certificação	2024-10-30

IAF

DAkkS

DQS GmbH

IQNET

Christian Gerling
Director Executive

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
Administrative Office: DQS do Brasil Ltda., Av. Adolfo Pinheiro, 1001 - 3º andar,
04733-100 São Paulo – SP, Brazil
The validity of the certification can only be verified by the QR-code.

1 / 2

Figure 8: ISO 27001 Certificate - Information Security Management System Certificate.

Escalation process for employees to report incidents, vulnerabilities, or suspicious activities

Cemig continuously monitors its IT environment through a specialized SOC (Security Operations Center) team, responsible for monitoring, detecting, investigating, and responding to threats.

This team, together with members of the Cybersecurity and Information Management department, forms the CSIRT (Computer Security Incident Response Team). They work together to respond to incidents, perform analyses, and develop preventive actions to ensure the confidentiality, availability, and integrity of services.

Cemig periodically issues communications about cyber risks and encourages employees to report suspicious phishing attempts or any security incident.

Any employee may directly register a request through a service ticket in the ITSM software, or direct inquiries to the Cybersecurity and Information Security teams. The response team will investigate, analyze, and conduct the appropriate handling.

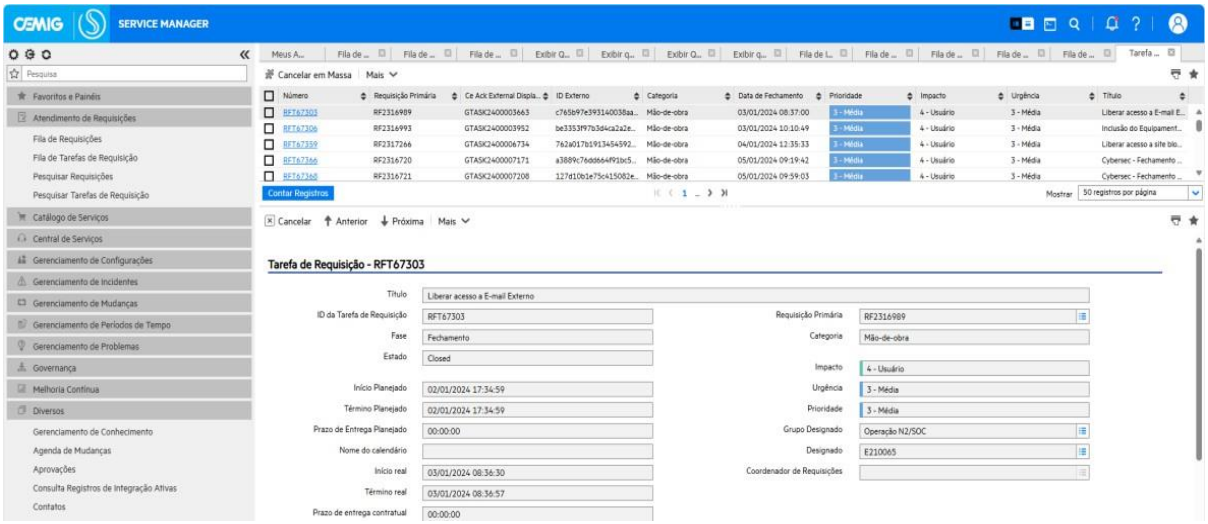

Figure 9: Example of the escalation process for employees to report incidents

Information-security awareness training

Security Awareness and Training Platform

Cemig implemented a security-awareness platform. The platform increases employees' resilience against phishing attacks through simulations of real threats. In addition to phishing simulations, it includes educational and training content that promotes a cybersecurity culture throughout the company.

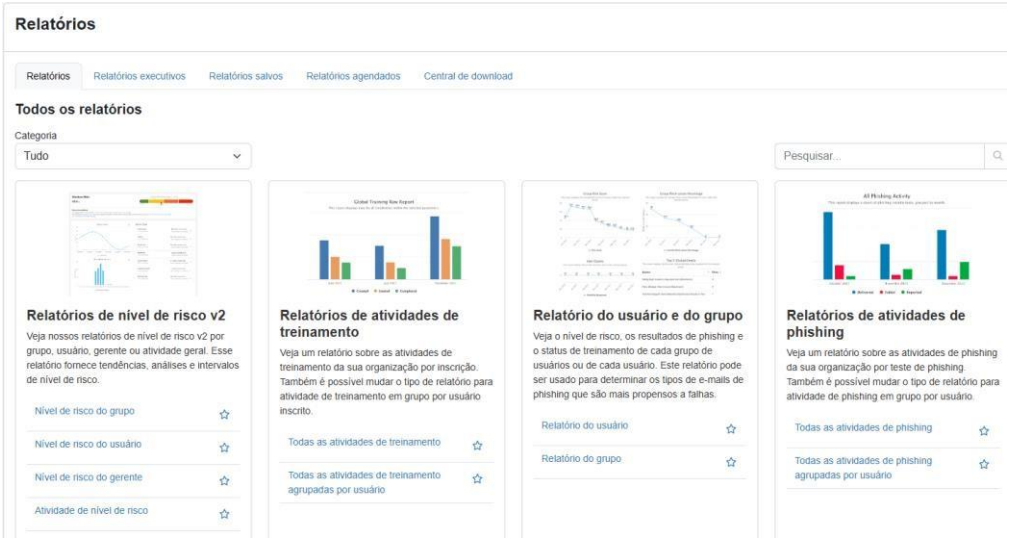

Figure 10: Training, awareness, and phishing-simulation platform.
The screen shows follow-up reports for training activities and phishing simulations.

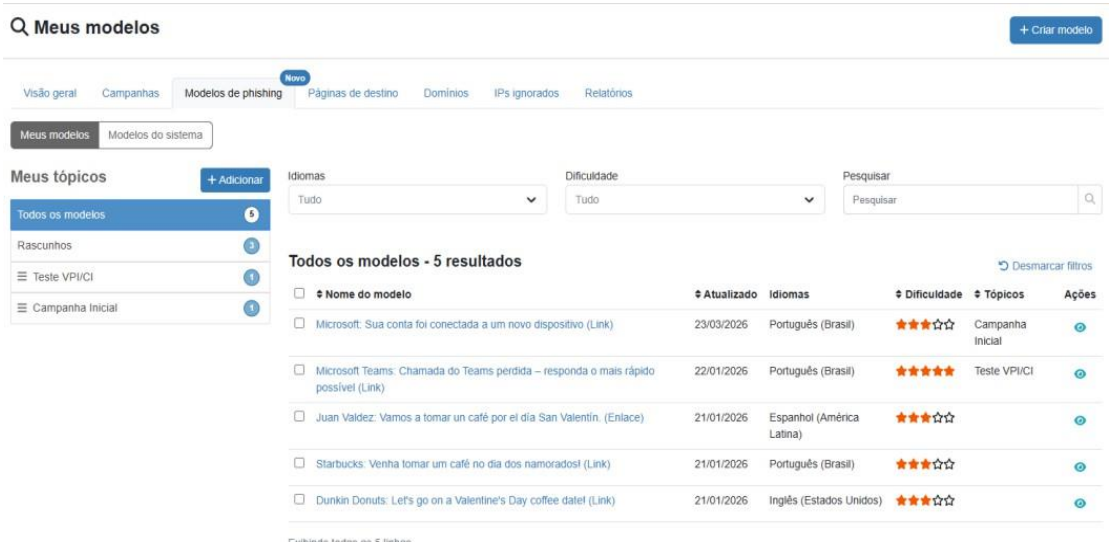

Figure 11: System screen with phishing-simulation templates that simulate real attacks.

Figure 12: Screen of the mandatory training course "Basic Information Security Onboarding" held at Univercemig, the corporate university.

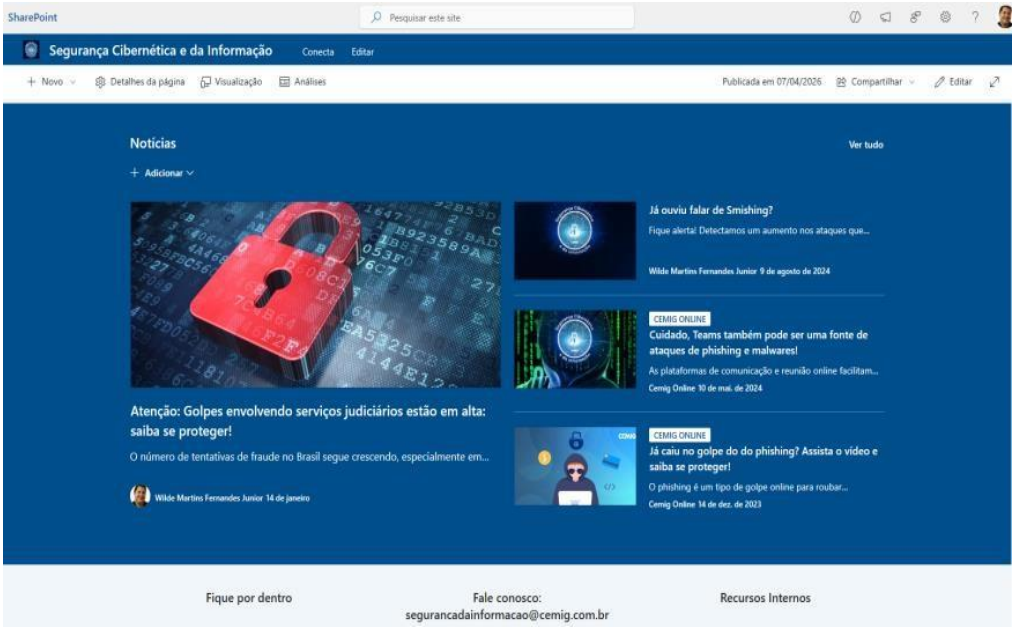

Figure 13: Intranet screen - "security communications"

As a result of our practices, no breach occurred last year.