Information Security Report

Ref. 2024/2025

Information security is a topic of great relevance for Cemig, as in an increasingly connected world, controlling and protecting the Company's data network becomes essential. Good management of technological resources and ensuring security are fundamental to mitigate risks related to the leakage and misuse of personal data, as well as to prevent unauthorized access to confidential and strategic information. With this objective, Cemig has been continuously investing in its Information Technology (IT) infrastructure, seeking to strengthen the governance and management of IT services, as well as information security.

The topic of governance and information security is 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 advised by the Vice Presidency of Information Technology, which provides monthly reports presenting relevant security actions and the status of implementation. As it is one of the top risks for the Company, this is also monitored by the Risk Committee within the scope of the Board of Directors..

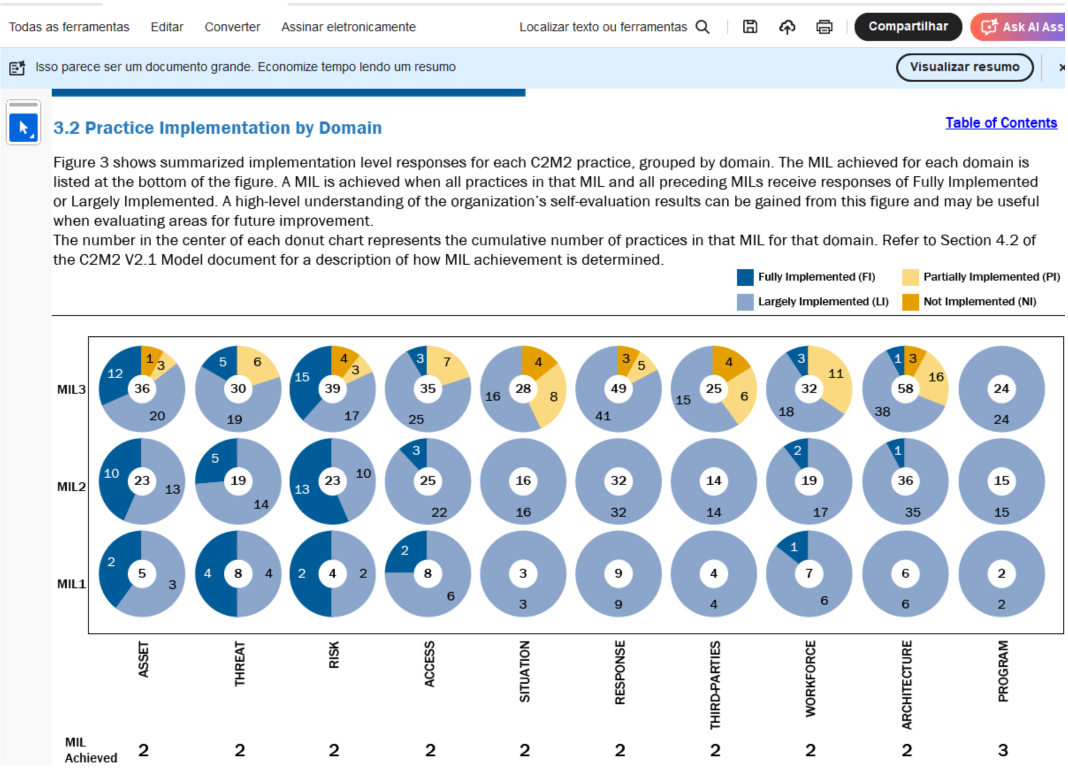
Cemig has an Information Security and Cybersecurity Policy that includes guidelines and principles related to the topic. This policy defines the guidelines, responsibilities, and objectives established to ensure the protection requirements of the Company's information and cyber environment. It can be accessed through the company's website at www.cemig.com.br/politica-de-seguranca-da-informacao-e-seguranca-cibernetica/.

C2M2 –Cybersecurity Capability Maturity Model

Cemig has adopted the C2M2 (Cybersecurity Capability Maturity Model) framework to drive the continuous improvement of its Cybersecurity and Information Security maturity. This initiative also supports alignment with business continuity plans, encompassing architectural solutions, infrastructure, access management, and incident response and management.
The C2M2 is a tool developed by the U.S. Department of Energy to help organizations evaluate and improve their cybersecurity capabilities. It focuses on both information technology (IT) and operations technology (OT) assets and environments.

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

Our company has achieved **Level 2** in the C2M2 framework, indicating that our cybersecurity practices are managed and consistently applied. This achievement demonstrates our commitment to maintaining a robust cybersecurity posture and protecting our assets and operations.



Isso parece ser um documento grande. Economize tempo lendo um resumo

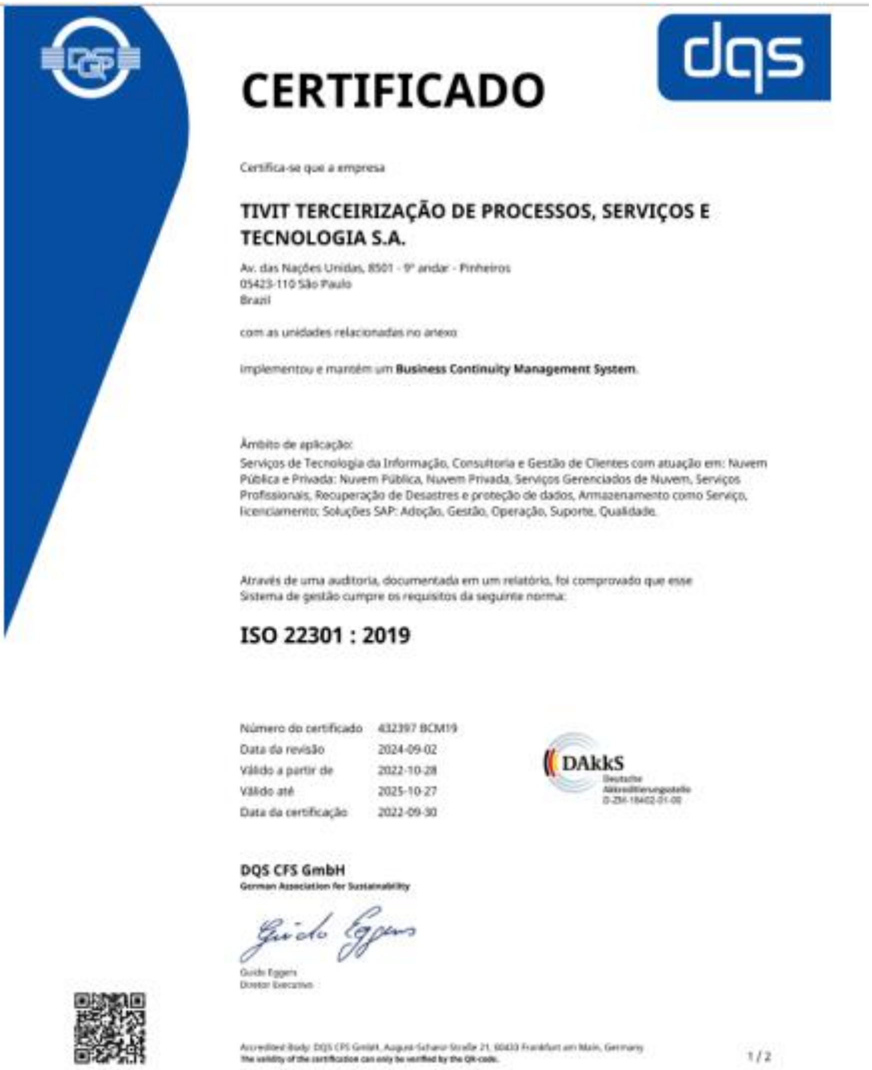
3.2 Practice Implementation by Domain

Figure 3 shows summarized implementation level responses for each C2M2 practice, grouped by domain. The MIL achieved for each domain is listed at the bottom of the figure. A MIL is achieved when all practices in that MIL and all preceding MILs receive responses of Fully Implemented or Largely Implemented. A high-level understanding of the organization's self-evaluation results can be gained from this figure and may be useful when evaluating areas for future improvement.

The number in the center of each donut chart represents the cumulative number of practices in that MIL for that domain. Refer to Section 4.2 of the C2M2 V2.1 Model document for a description of how MIL achievement is determined.

Figure 1 : Screen of the C2M2 (Cybersecurity Capability Maturity Model) framework to drive the continuous improvement of its Cybersecurity and Information Security maturity. This initiative also supports alignment with business continuity plans

Cemig outsources data center infrastructure, managed services, and security operations with TIVIT. TIVIT has a continuity plan and tests it periodically, so much so that it is certified by the international standard ISO 22.301/2019, as per the certificate below.



CERTIFICADO

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-18402-01-00

DQS CFS GmbH
German Association for Sustainability

Guido Eggers

Guido Eggers
Diretor 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 2: Certificate of the ISO 22301/2019 – Business Continuity Management System

Vulnerability analysis

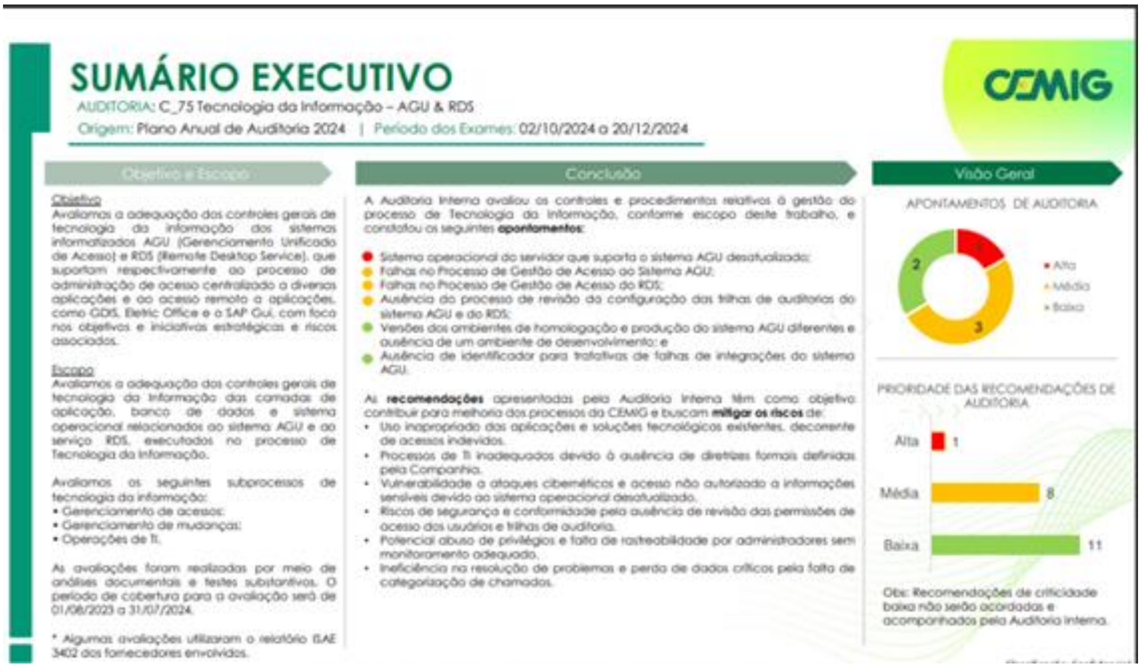
Vulnerability management process:
Cemig has advanced software solutions for vulnerability management and configuration compliance. These tools perform analysis and scanning of assets, web applications, and configuration auditing to ensure robust adherence to cybersecurity best practices and guidelines to eliminate and mitigate information security-related vulnerabilities.

Intrusion tests
With the aim of simulating a cyber-attack and assessing the security of systems and the network, we conduct intrusion tests by an independent external company to evaluate the resilience of the systems against a malicious source attack. The independent company performs an attack simulation to identify vulnerabilities in a system or application. This allows for the identification of possible improvement points and the establishment of preventive actions.

Cyber threat Intelligence
Additionally, complementing the vulnerability management process, we monitor the external environment for threat detection through the Cyber Threat Intelligence process. This involves research and monitoring to identify threats such as fake domains, brand abuse, activities on the deep and dark web, credential leaks, fraud, fake applications, and code leaks. The goal is to detect data leaks, fraud, and other threats.

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

Cemig has an Internal Audit team that periodically conducts audits covering the IT infrastructure. Regarding information security management systems, the associated risks are addressed through controls evaluated within the ISAE 3402 assurance reports issued by service providers as showed in the screens below.



SUMÁRIO EXECUTIVO

AUDITORIA: C_75 Tecnologia da Informação – AGU & RDS

Origem: Plano Anual de Auditoria 2024 | Período dos Exames: 02/10/2024 a 20/12/2024

Objetivo e Escopo

Objetivo

Avaliamos a adequação dos controles gerais de tecnologia da informação dos sistemas informatizados AGU (Gerenciamento Unificado de Acesso) e RDS (Remote Desktop Service), que suportam respectivamente ao processo de administração de acesso centralizado a diversas aplicações e ao acesso remoto a aplicações, como GDIS, Eletric Office e o SAP Gui, com foco nos objetivos e iniciativas estratégicas e riscos associados.

Escopo

Avaliamos a adequação dos controles gerais de tecnologia da Informação das camadas de aplicação, banco de dados e sistema operacional relacionados ao sistema AGU e ao serviço RDS, executados no processo de Tecnologia da Informação.

Avaliamos os seguintes subprocessos de tecnologia da informação:
- Gerenciamento de acessos;
- Gerenciamento de mudanças;
- Operações de TI.

As avaliações foram realizadas por meio de análises documentais e testes substantivos. O período de cobertura para a avaliação será de 01/08/2023 a 31/07/2024.

* Algumas avaliações utilizaram o relatório ISAE 3402 dos fornecedores envolvidos.

Conclusão

A Auditoria Interna avaliou os controles e procedimentos relativos à gestão do processo de Tecnologia da Informação, conforme escopo deste trabalho, e constatou os seguintes **apontamentos**:

- 🔴 Sistema operacional do servidor que suporta o sistema AGU desatualizado;
- 🟡 Falhas no Processo de Gestão de Acesso ao Sistema AGU;
- 🟡 Falhas no Processo de Gestão de Acesso do RDS;
- 🟡 Ausência do processo de revisão da configuração das trilhas de auditorias do sistema AGU e do RDS;
- 🟢 Versões dos ambientes de homologação e produção do sistema AGU diferentes e ausência de um ambiente de desenvolvimento; e
- 🟢 Ausência de identificador para tratativas de falhas de integrações do sistema AGU.

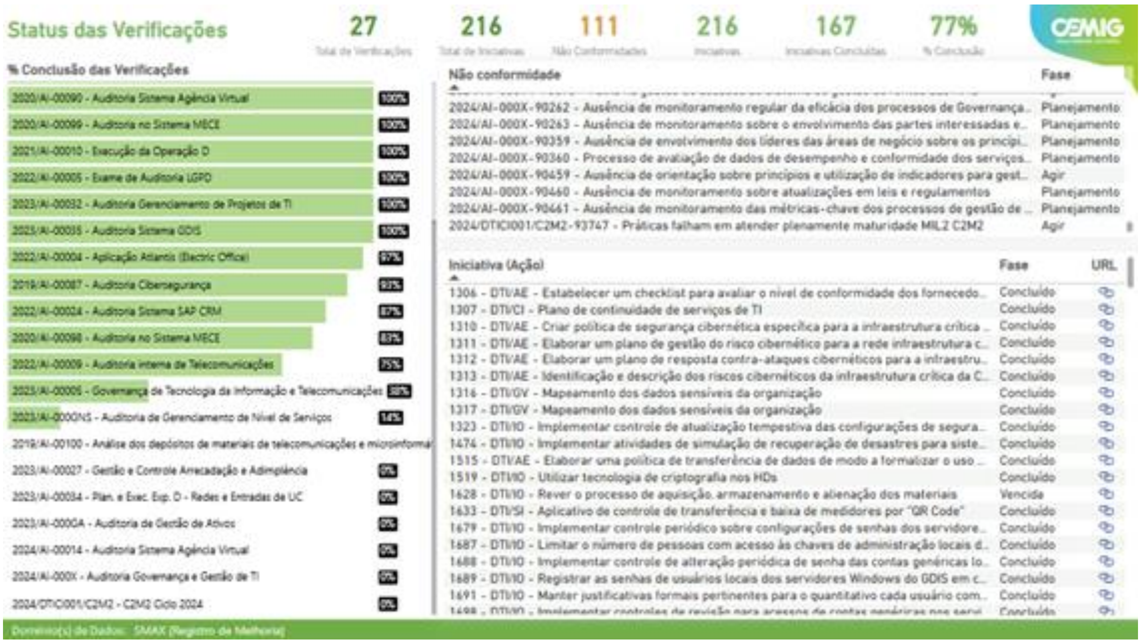
As **recomendações** apresentadas pela Auditoria Interna têm como objetivo contribuir para melhoria dos processos da CEMIG e buscam **mitigar os riscos** de:

- Uso inapropriado das aplicações e soluções tecnológicas existentes, decorrente de acessos indevidos.
- Processos de TI inadequados devido à ausência de diretrizes formais definidas pela Companhia.
- Vulnerabilidade a ataques cibernéticos e acesso não autorizado a informações sensíveis devido ao sistema operacional desatualizado.
- Riscos de segurança e conformidade pela ausência de revisão das permissões de acesso dos usuários e trilhas de auditoria.
- Potencial abuso de privilégios e falta de rastreabilidade por administradores sem monitoramento adequado.
- Ineficiência na resolução de problemas e perda de dados críticos pela falta de categorização de chamados.

Visão Geral

CEMIG
APONTAMENTOS DE AUDITORIA
1
3
2
Alta
Média
Baixa
PRIORIDADE DAS RECOMENDAÇÕES DE AUDITORIA
Alta
1
Média
8
Baixa
11

Obs: Recomendações de criticidade baixa não serão acordadas e acompanhados pela Auditoria Interna.



Status das Verificações

27	216	111	216	167	77%
Total de Verificações	Total de Iniciativas	Não Conformidades	Iniciativas	Iniciativas Concluídas	% Conclusão

% Conclusão das Verificações

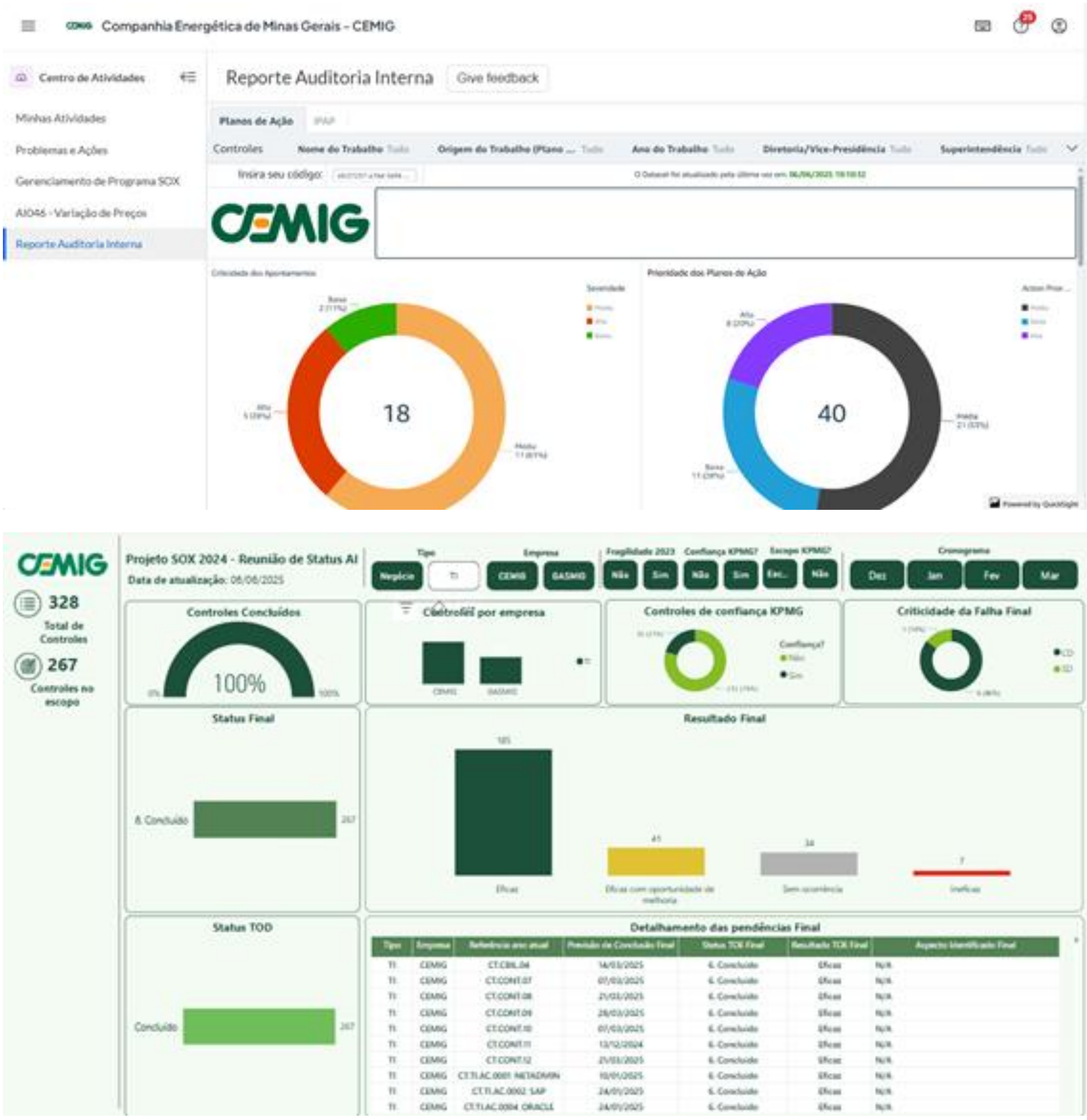
2020/AI-00090 - Auditoria Sistema Agência Virtual	100%
2020/AI-00099 - Auditoria no Sistema MECE	100%
2021/AI-00010 - Execução da Operação D	100%
2022/AI-00005 - Exame de Auditoria LGPD	100%
2023/AI-00032 - Auditoria Gerenciamento de Projetos de TI	100%
2023/AI-00035 - Auditoria Sistema GDIS	100%
2022/AI-00004 - Aplicação Atlantis (Electric Office)	97%
2019/AI-00087 - Auditoria Cibersegurança	93%
2022/AI-00024 - Auditoria Sistema SAP CRM	87%
2020/AI-00098 - Auditoria no Sistema MECE	83%
2022/AI-00009 - Auditoria interna de Telecomunicações	75%
2023/AI-00005 - Governança de Tecnologia da Informação e Telecomunicações	38%
2023/AI-000GNS - Auditoria de Gerenciamento de Nível de Serviços	14%
2019/AI-00100 - Análise dos depósitos de materiais de telecomunicações e microinforma	
2023/AI-00027 - Gestão e Controle Arrecadação e Adimplência	0%
2023/AI-00034 - Plan. e Exec. Exp. D - Redes e Entradas de UC	0%
2023/AI-000GA - Auditoria de Gestão de Ativos	0%
2024/AI-00014 - Auditoria Sistema Agência Virtual	0%
2024/AI-000X - Auditoria Governança e Gestão de TI	0%
2024/DTICI001/C2M2 - C2M2 Ciclo 2024	0%

Não conformidade	Fase
2024/AI-000X-90262 - Ausência de monitoramento regular da eficácia dos processos de Governança...	Planejamento
2024/AI-000X-90263 - Ausência de monitoramento sobre o envolvimento das partes interessadas e...	Planejamento
2024/AI-000X-90359 - Ausência de envolvimento dos líderes das áreas de negócio sobre os princípi...	Planejamento
2024/AI-000X-90360 - Processo de avaliação de dados de desempenho e conformidade dos serviços...	Planejamento
2024/AI-000X-90459 - Ausência de orientação sobre princípios e utilização de indicadores para gest...	Agir
2024/AI-000X-90460 - Ausência de monitoramento sobre atualizações em leis e regulamentos	Planejamento
2024/AI-000X-90461 - Ausência de monitoramento das métricas-chave dos processos de gestão de ...	Planejamento
2024/DTICI001/C2M2-93747 - Práticas falham em atender plenamente maturidade MIL2 C2M2	Agir

Iniciativa (Ação)	Fase	URL
1306 - DTI/AE - Estabelecer um checklist para avaliar o nível de conformidade dos fornecedo...	Concluído	🔗
1307 - DTI/CI - Plano de continuidade de serviços de TI	Concluído	🔗
1310 - DTI/AE - Criar política de segurança cibernética específica para a infraestrutura crítica ...	Concluído	🔗
1311 - DTI/AE - Elaborar um plano de gestão do risco cibernético para a rede infraestrutura c...	Concluído	🔗
1312 - DTI/AE - Elaborar um plano de resposta contra-ataques cibernéticos para a infraestru...	Concluído	🔗
1313 - DTI/AE - Identificação e descrição dos riscos cibernéticos da infraestrutura crítica da C...	Concluído	🔗
1316 - DTI/GV - Mapeamento dos dados sensíveis da organização	Concluído	🔗
1317 - DTI/GV - Mapeamento dos dados sensíveis da organização	Concluído	🔗
1323 - DTI/IO - Implementar controle de atualização tempestiva das configurações de segura...	Concluído	🔗
1474 - DTI/IO - Implementar atividades de simulação de recuperação de desastres para siste...	Concluído	🔗
1515 - DTI/AE - Elaborar uma política de transferência de dados de modo a formalizar o uso ...	Concluído	🔗
1519 - DTI/IO - Utilizar tecnologia de criptografia nos HDs	Concluído	🔗
1628 - DTI/IO - Rever o processo de aquisição, armazenamento e alienação dos materiais	Vencida	🔗
1633 - DTI/SI - Aplicativo de controle de transferência e baixa de medidores por "QR Code"	Concluído	🔗
1679 - DTI/IO - Implementar controle periódico sobre configurações de senhas dos servidore...	Concluído	🔗
1687 - DTI/IO - Limitar o número de pessoas com acesso às chaves de administração locais d...	Concluído	🔗
1688 - DTI/IO - Implementar controle de alteração periódica de senha das contas genéricas lo...	Concluído	🔗
1689 - DTI/IO - Registrar as senhas de usuários locais dos servidores Windows do GDIS em c...	Concluído	🔗
1691 - DTI/IO - Manter justificativas formais pertinentes para o quantitativo cada usuário com...	Concluído	🔗
1698 - DTI/IO - Implementar controles de revisão para acessos de contas genéricas nos servi...	Concluído	🔗

Domínio(s) de Dados: SMAX (Registro de Melhoria)

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



Companhia Energética de Minas Gerais - CEMIG

Centro de Atividades

- Minhas Atividades
- Problemas e Ações
- Gerenciamento de Programa SOX
- AI046 - Variação de Preços
- Reporte Auditoria Interna

Reporte Auditoria Interna

Give feedback

Planos de Ação | IPAP

Controles | Nome do Trabalho Tudo | Origem do Trabalho (Plano ... Tudo | Ano do Trabalho Tudo | Diretoria/Vice-Presidência Tudo | Superintendência Tudo

Insira seu código:

Projeto SOX 2024 - Reunião de Status AI

Data de atualização: 06/06/2025

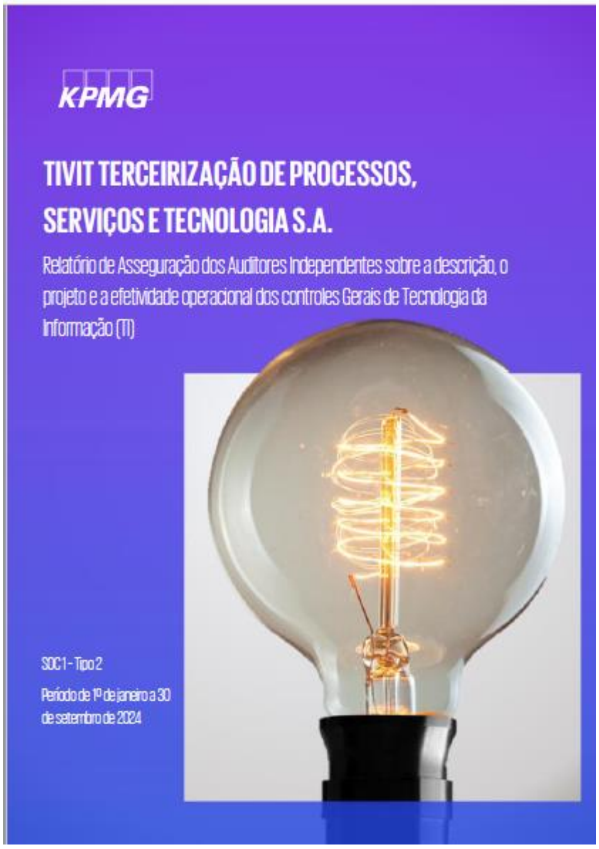
Detalhamento das pendências Final

Tipo	Empresa	Referência ano atual	Previsão de Conclusão Final	Status TOE Final	Resultado TOE Final	Aspecto Identificado Final
TI	CEMIG	CT.CBIL.04	14/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.07	07/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.08	21/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.09	28/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.10	07/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.11	13/12/2024	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.CONT.12	21/03/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.TI.AC.0001 METADMIN	10/01/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.TI.AC.0002 SAP	24/01/2025	6. Concluído	Eficaz	N/A
TI	CEMIG	CT.TI.AC.0004 ORACLE	24/01/2025	6. Concluído	Eficaz	N/A

Figure 4: Internal Audit Report related to information security management systems

❑ Independent external audit of the 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 IT general controls (ITGC), covering both infrastructure and information security aspects. Additionally, since 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 standards for security, quality, and governance.



KPMG

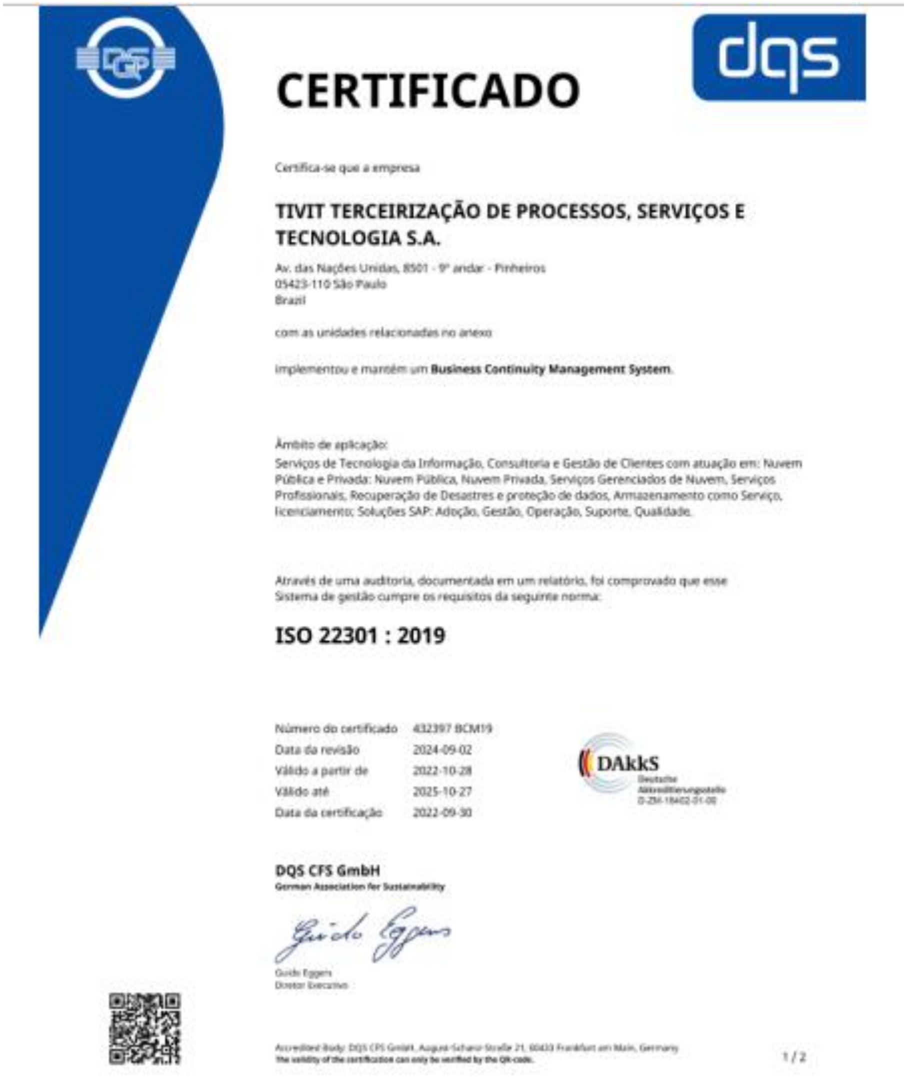
TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A.

Relatório de Asseguração dos Auditores Independentes sobre a descrição, o projeto e a efetividade operacional dos controles Gerais de Tecnologia da Informação (TI)

SOC 1 - Tipo 2

Período de 1º de janeiro a 30 de setembro de 2024

Figure 5: KPMG Assurance Report of control and process of Information Tecnology



CERTIFICADO

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-18402-01-00

DQS CFS GmbH
German Association for Sustainability

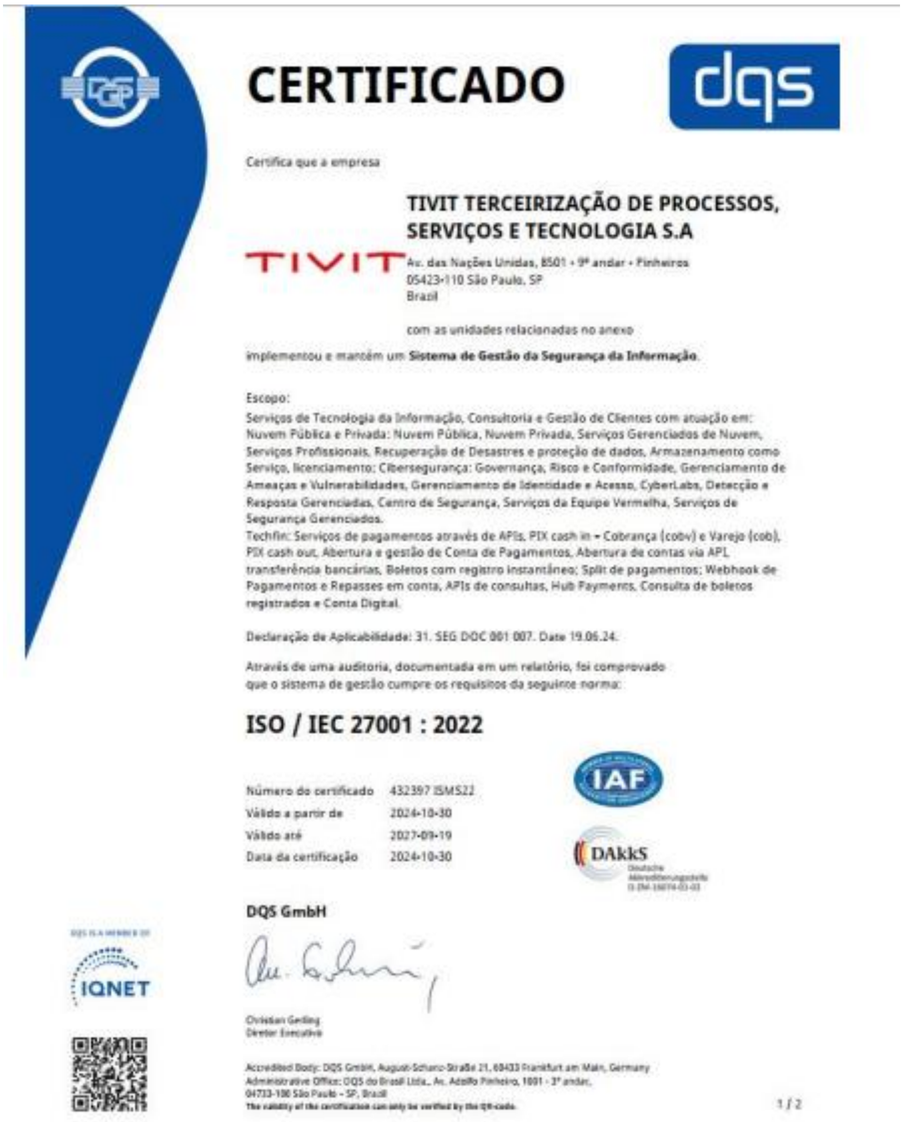
Guido Eggers

Guido Eggers
Diretor 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 5: KPMG Assurance Report of control and process of Information Tecnology (TIVIT – our datacenter)



CERTIFICADO

Certifica que a empresa

TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A

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 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 Payments, 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

DAkkS Deutsche Akkreditierungsstelle D-ZM-16074-03-03

DQS IS A MEMBER OF IQNET

DQS GmbH

Christian Gerling
Diretor 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, Brasil
The validity of the certification can only be verified by the QR-code.

1 / 2

Figure 6: ISO 27001 Certified provide byKPMG Assurance Report of control and process of Information Tecnology DQS Audit Conpany (TIVIT)

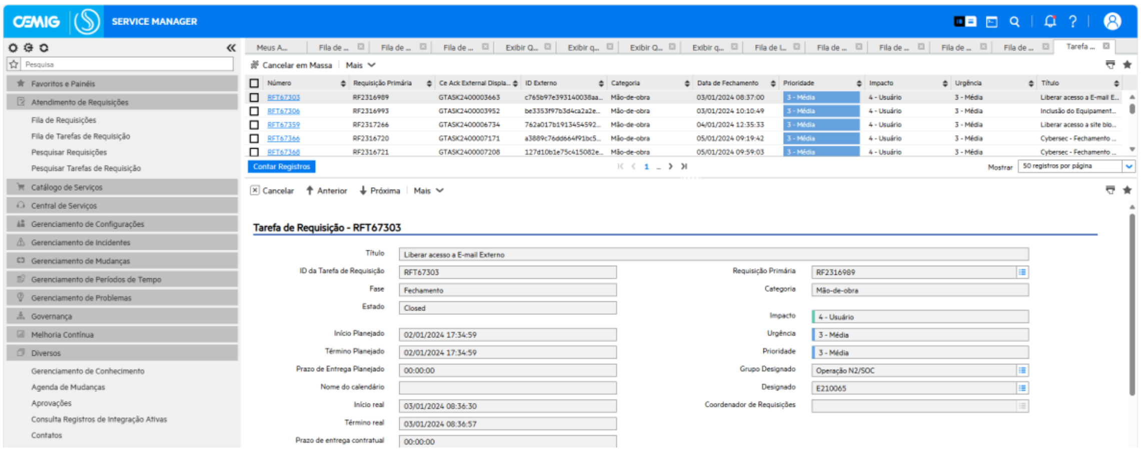
Figure 5: KPMG Assurance Report of control and process of Information Tecnology

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

Monitoring and Incident Response:
Cemig conducts continuous monitoring of its IT environment through a specialized team at the SOC (Security Operation Center), responsible for monitoring, detecting, investigating, and responding to threats.
This team, along 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 suspected phishing attempts or any security incident.

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



Número	Requisição Primária	Ce Ack External Displa...	ID Externo	Categoria	Data de Fechamento	Prioridade	Impacto	Urgência	Título
RFT67303	RF2316989	GTASK2400003663	c765b97e393140038aa...	Mão-de-obra	03/01/2024 08:37:00	3 - Média	4 - Usuário	3 - Média	Liberar acesso a E-mail E...
RFT67306	RF2316993	GTASK2400003952	be3353f97b3d4ca2a2e...	Mão-de-obra	03/01/2024 10:10:49	3 - Média	4 - Usuário	3 - Média	Inclusão do Equipament...
RFT67359	RF2317266	GTASK2400006734	762a017b1913454592...	Mão-de-obra	04/01/2024 12:35:33	3 - Média	4 - Usuário	3 - Média	Liberar acesso a site blo...
RFT67366	RF2316720	GTASK2400007171	a3889c76dd664f91bc5...	Mão-de-obra	05/01/2024 09:19:42	3 - Média	4 - Usuário	3 - Média	Cybersec - Fechamento ...
RFT67368	RF2316721	GTASK2400007208	127d10b1e75c415082e...	Mão-de-obra	05/01/2024 09:59:03	3 - Média	4 - Usuário	3 - Média	Cybersec - Fechamento ...

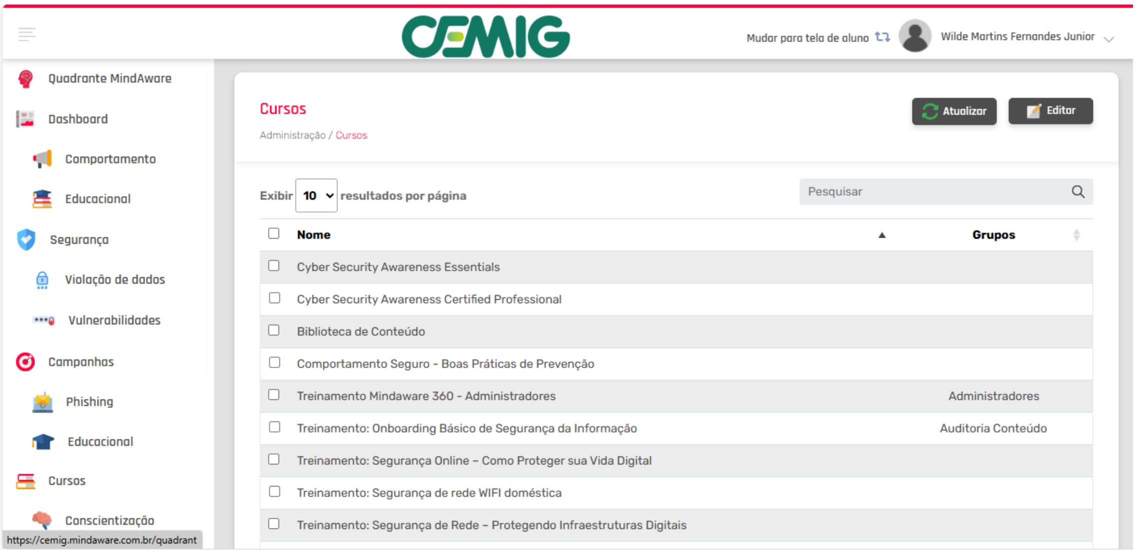
Tarefa de Requisição - RFT67303

Título: Liberar acesso a E-mail Externo
ID da Tarefa de Requisição: RFT67303
Fase: Fechamento
Estado: Closed
Início Planejado: 02/01/2024 17:34:59
Término Planejado: 02/01/2024 17:34:59
Prazo de Entrega Planejado: 00:00:00
Nome do calendário:
Início real: 03/01/2024 08:36:30
Término real: 03/01/2024 08:36:57
Prazo de entrega contratual: 00:00:00
Requisição Primária: RF2316989
Categoria: Mão-de-obra
Impacto: 4 - Usuário
Urgência: 3 - Média
Prioridade: 3 - Média
Grupo Designado: Operação N2/SOC
Designado: E210065
Coordenador de Requisições:

Figure 7: Example of escalation process for employees to report incidents

❑ Information security awareness training

<u>Security Awareness and Training Platform</u>
Cemig has implemented a security awareness platform. The platform increases employees' resilience to phishing attacks through simulations of real threats. Beyond the phishing simulations, there is educational and training content that promotes a cybersecurity culture throughout the company.



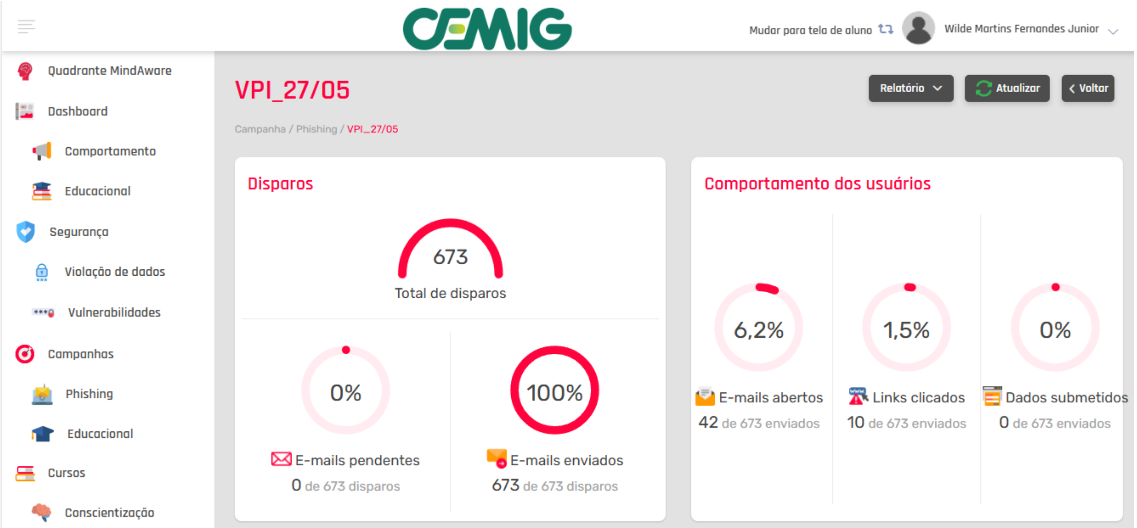
Cursos

Administração / Cursos

Nome	Grupos
□ Cyber Security Awareness Essentials	
□ Cyber Security Awareness Certified Professional	
□ Biblioteca de Conteúdo	
□ Comportamento Seguro - Boas Práticas de Prevenção	
□ Treinamento Mindaware 360 - Administradores	Administradores
□ Treinamento: Onboarding Básico de Segurança da Informação	Auditoria Conteúdo
□ Treinamento: Segurança Online – Como Proteger sua Vida Digital	
□ Treinamento: Segurança de rede WIFI doméstica	
□ Treinamento: Segurança de Rede – Protegendo Infraestruturas Digitais	

Figure 8: Corporate University training courses. The screen shows the following training: Cyber Security Awareness

Essentials, Cyber Security Awareness Certified Professional among others



VPI_27/05

Campanha / Phishing / VPI_27/05

Disparos

673 Total de disparos

0% E-mails pendentes 0 de 673 disparos

100% E-mails enviados 673 de 673 disparos

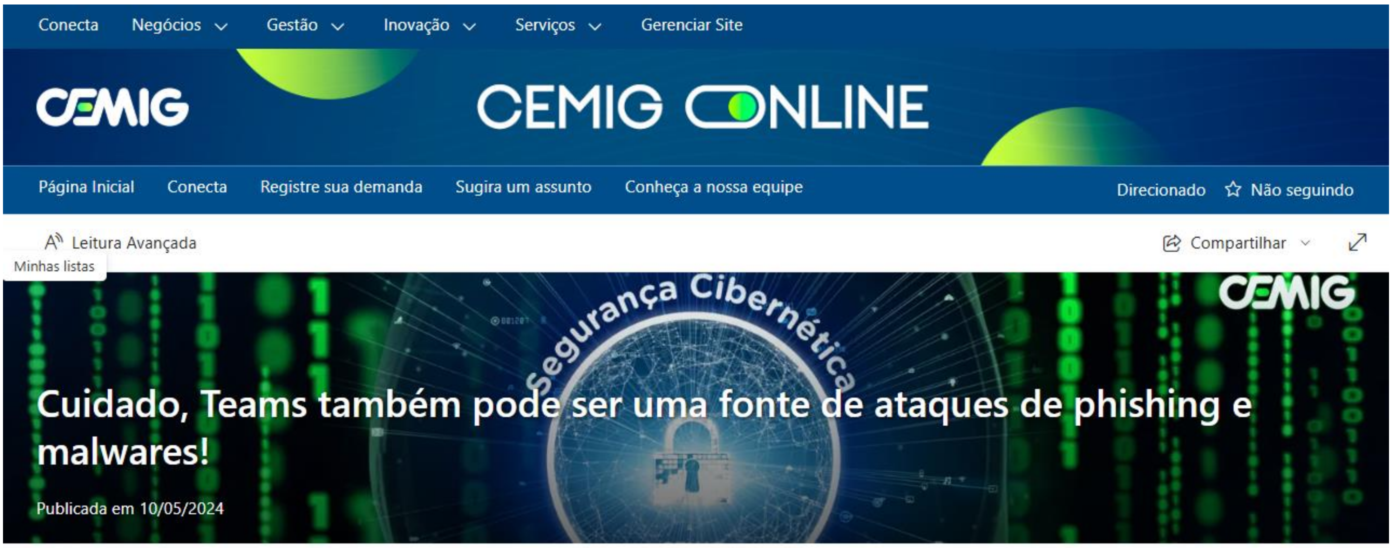
Comportamento dos usuários

6,2% E-mails abertos 42 de 673 enviados

1,5% Links clicados 10 de 673 enviados

0% Dados submetidos 0 de 673 enviados

Figure 9: Screen of the system with to phishing attacks through simulations of real threats



Cuidado, Teams também pode ser uma fonte de ataques de phishing e malwares!

Publicada em 10/05/2024

Figure 10: Intranet screen – "take Care with fishing"

As a result of our practices no breaches occurred in last year.