SIC na CAPES

Segurança em camadas. Dados protegidos. Pessoas preparadas.

Francisco Neto | Gestor de SIC

01

SIC na CAPES

A estratégia conecta governança, proteção tecnológica, dados e conscientização.

ESTRATÉGIA

Defesa em profundidade

Nenhuma barreira isolada é suficiente.

- Múltiplas barreiras protegem dados e sistemas.
- Cada camada cumpre uma função específica.
- Firewalls, antivírus, autenticação de dois fatores e criptografia atuam em conjunto.
- Para avançar, um atacante precisa superar várias defesas.



ARQUITETURA

Seis camadas de proteção

Perímetro

Firewalls, gateways e filtros de tráfego.

Rede

Segmentação, IDS/IPS e monitoramento.

Sistemas

Hardening, antivírus, atualizações e vulnerabilidades.

Aplicações

MFA, controle de acesso e código seguro.

Dados

Criptografia, backup e acesso a dados sensíveis.

Usuários

Conscientização, políticas e boas práticas.

NORMAS E RESPOSTA

Governança que orienta a proteção

LGPD

Lei Geral de Proteção de Dados

Protege informações pessoais, reforça o uso seguro, amplia privacidade e dá mais controle aos indivíduos.

NURI

Norma de Uso dos Recursos de Informática

Portaria CAPES nº 179, de 9 de novembro de 2021. Regras para uso seguro, adequado e funcional dos recursos de TI.

POSIC

Política de Segurança da Informação e Comunicação

Portaria CAPES nº 199, de 29 de agosto de 2019. Guia para proteger informações e evitar acessos não autorizados.

RESPOSTA A INCIDENTES

ETIR: prevenção, tratamento e resposta

INVESTIGAR → CONTER → RECUPERAR

- Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.
- Portaria CAPES nº 110, de 21 de junho de 2022.
- Investiga o que aconteceu, como aconteceu e como resolver o problema para proteger sistemas e dados.

csirt@capes.gov.br

Equipe de Incidentes de Segurança - Capes

CANAL DE CONTATO

02

Controles tecnológicos

Barreiras que monitoram, bloqueiam, filtram e recuperam.

CONTROLE TECNOLÓGICO

Firewall



- Uma barreira de segurança digital.
- Monitora e controla o tráfego de rede.
- Bloqueia ameaças e acessos não autorizados.
- Protege contra ataques cibernéticos.
- É essencial para redes e computadores.

CONTROLE TECNOLÓGICO

Sistema de Prevenção de Intrusão



- Um detetive de segurança para o computador ou a rede.
- Observa o tráfego em busca de comportamentos suspeitos.
- Ao detectar algo errado, age imediatamente para bloquear ou deter o ataque.
- É como um guarda que vigia e evita invasões indesejadas.

CONTROLE TECNOLÓGICO

Filtro de Conteúdo



- Filtra e controla o acesso online.
- Bloqueia ou permite tipos específicos de conteúdo.
- Protege os usuários e regula o acesso à web.
- Restringe sites não aderentes às normas.
- Mantém um ambiente online seguro.

CONTROLE TECNOLÓGICO

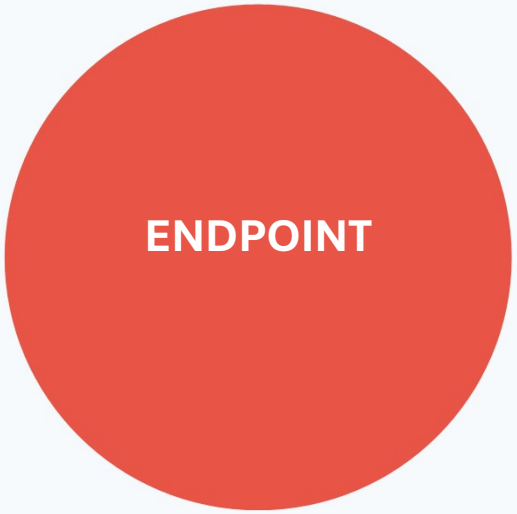
Anti-SPAM



- Filtra e-mails indesejados e separa spam de mensagens legítimas.
- Usa algoritmos e filtros para analisar mensagens.
- Reduz a sobrecarga de e-mails não solicitados.
- Melhora a segurança e a eficiência das comunicações.
- Historicamente, bloqueamos entre 80% e 85% dos e-mails recebidos.

CONTROLE TECNOLÓGICO

Antimalware



- Software de segurança contra malware, vírus e spyware.
- Detecta e remove ameaças.
- Ajuda a manter dispositivos seguros.
- Previne danos e perda de dados por infecções.

CONTROLE TECNOLÓGICO

Backup & Recuperação

CONTINUIDADE

- Portaria CAPES nº 239, de 31 de outubro de 2022.
- Cópias de segurança dos arquivos importantes em outro local seguro, como disco externo ou nuvem.
- É o plano B para não perder informações preciosas.

03

Segurança orientada por dados

Monitorar o ambiente transforma volume em prioridade de proteção.

VISIBILIDADE

Plataforma de Segurança e Análise de Dados

Proteger

Ajuda a proteger informações confidenciais e gerenciar acessos.

Monitorar

Acompanha atividades de usuários e detecta ameaças internas.

Conformidade

Contribui para cumprir regulamentações de privacidade.

Decidir

Apoia decisões informadas sobre dados e segurança.

ESCALA

O ambiente monitorado em números

56,5 TB
de dados

2,8 M
pastas

49,2 M
arquivos

25,8 M
permissões

30,2 TB
no OneDrive

29,9 M
arquivos no OneDrive

875 mil
pastas no OneDrive

34.444
contas

3.271
contas de computador

5.818
grupos de usuários

04

IPSA

Índice de Proteção Sobre os Ativos: uma medida da segurança das estações de trabalho.

ÍNDICE DE PROTEÇÃO SOBRE OS ATIVOS

IPSA: inovação aplicada à proteção

- Resultado de um Concurso de Inovação interno na DTI.
- Atribui uma nota de segurança às estações de trabalho.
- O conceito Adequado, adquirido em 2024, foi mantido em 2025, porém foi reduzido para Regular em 2026, evidenciando a necessidade de fortalecer as políticas de atualização.



2025 2026

ADEQUADO

05

Campanha de phishing

Simulações transformam comportamento em uma camada ativa de defesa.

CONSCIENTIZAÇÃO

O que é phishing?

Uma fraude online criada para obter informações pessoais.

1. Finge ser uma entidade confiável
2. Usa e-mails, mensagens ou links falsos
3. Busca roubar informações, como senhas
4. Exige verificar fontes e evitar links suspeitos

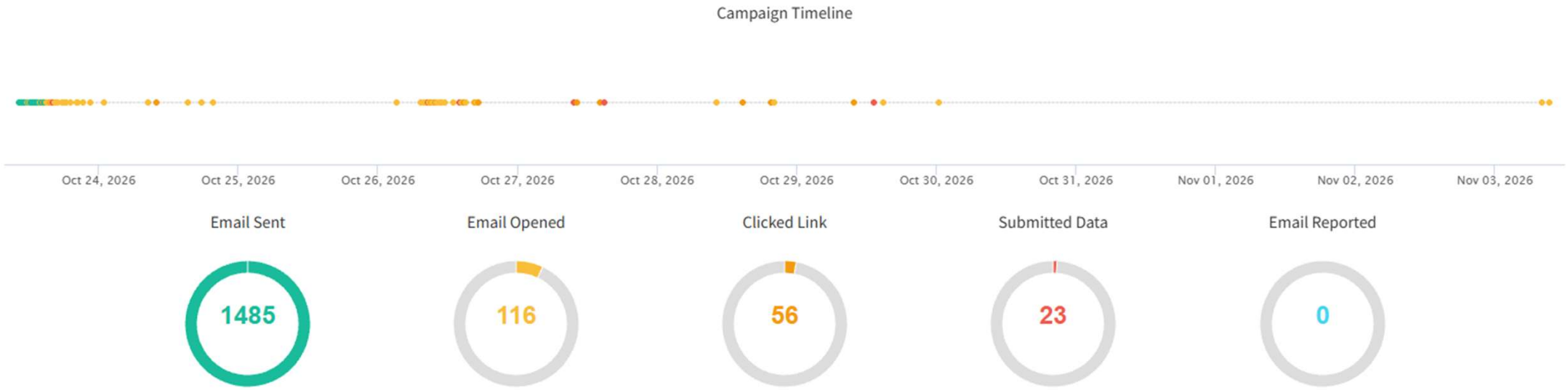
PARE

VERIFIQUE

PROTEJA-SE

Results for Migração da Caixa de E-mail Institucional para Nova Plataforma

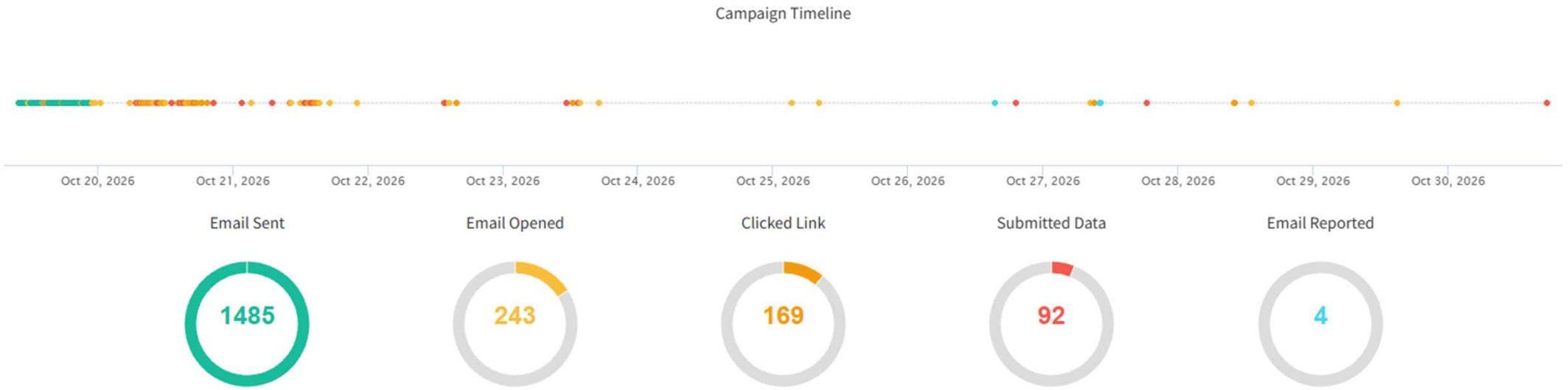
Back | Export CSV | Complete | Delete | Refresh



CAMPANHA 1

Results for Cadastro obrigatório da autenticação facial nas estações de trabalho

Back | Export CSV | Complete | Delete | Refresh



CHECKLIST PRÁTICO

O que olhar no e-mail?

- ✓ Remetente e domínio
- ✓ Tom de urgência ou pressão
- ✓ Pedido de senha ou dado sensível
- ✓ Destino real do link
- ✓ Anexos inesperados
- ✓ Erros, inconsistências e contexto

Assista ao exemplo da campanha

06

Um incidente e um plano de ação

Uma resposta estruturada para acelerar controles, atribuir responsabilidades e medir a evolução em 180 dias.

CONTEXTO RESERVADO

O incidente que motivou o plano

RELATO DO INCIDENTE

O que aconteceu

Impacto e resposta

Aprendizados

ID948 - Exfiltração de Dados na Aplicação Meus Dados

RESUMO EXECUTIVO

Plano de Ação SIC

Elevar o nível mínimo de segurança das aplicações hospedadas, desenvolvidas ou publicadas pela CAPES.

Prioridade

Aplicações expostas à Internet, dados pessoais e correção das fragilidades relacionadas ao incidente.

Execução

Controles progressivos, automação de bloqueios, evidências técnicas e foco inicial nas aplicações de maior risco.

Governança

Patrocínio do Diretor da DTI, coordenação da CGSII e responsabilidades distribuídas entre Infraestrutura, Segurança e Desenvolvimento.

CRONOGRAMA

Três ondas de execução

IMEDIATO

Inventário, requisito para deploy, varredura emergencial, fluxo de exceção e acompanhamento semanal.

CURTO PRAZO

Quality Gate, capacitação, logs conforme a Portaria nº 116/2023 e migração para o F5.

MÉDIO PRAZO

Centralização de logs, alertas, WAF, gestão contínua de vulnerabilidades, SCA e painel executivo.

MUDANÇA DE PADRÃO

Controles que passam a condicionar a implantação

Sistema Gestão

Fonte oficial do inventário e requisito para deploy.

Qualidade do Código Fonte

Quality Gate bloqueante no código novo ou alterado.

Portaria nº 116/2023

Logs mínimos gerados, centralizados e disponíveis.

Balanceador e Firewall de Aplicação

Tráfego protegido e políticas progressivamente bloqueantes.

Vulnerabilidades

Varredura, priorização, reteste e prazos por severidade.

Segredos e dependências

Proteção institucional de segredos e análise SCA na pipeline.

Segurança é uma responsabilidade compartilhada.

Muito obrigado

seguranca.ti@capes.gov.br

CAPES | Semana SIC 2026