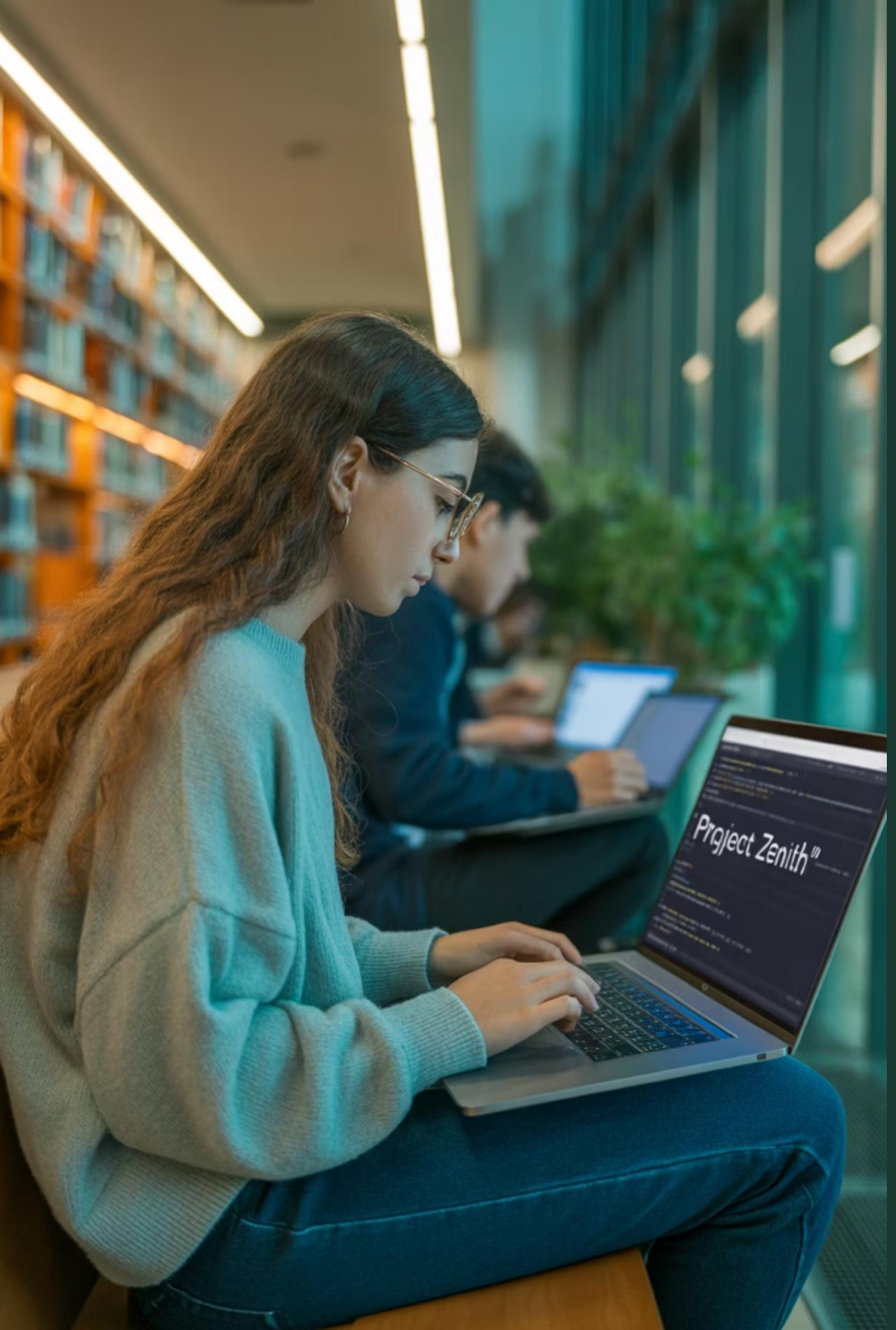
Cybersecurity, IASE 2025 & Educação 5.0

Dominique Fernandes

Seminário ABMES 2025

Agenda

- Cenário atual das IES
- Requisitos de cibersegurança e conformidade
- Indicadores estratégicos (MTTR, RPO, RTO)
- NIST CSF, LGPD e governança
- Roadmap de segurança por fases
- Ferramentas e casos de uso
- Indicadores por fase
- Fornecedores SaaS
- Conclusão



Cenário Atual das IES

Digitalização acelerada

As instituições de ensino superior estão passando por uma transformação digital sem precedentes.

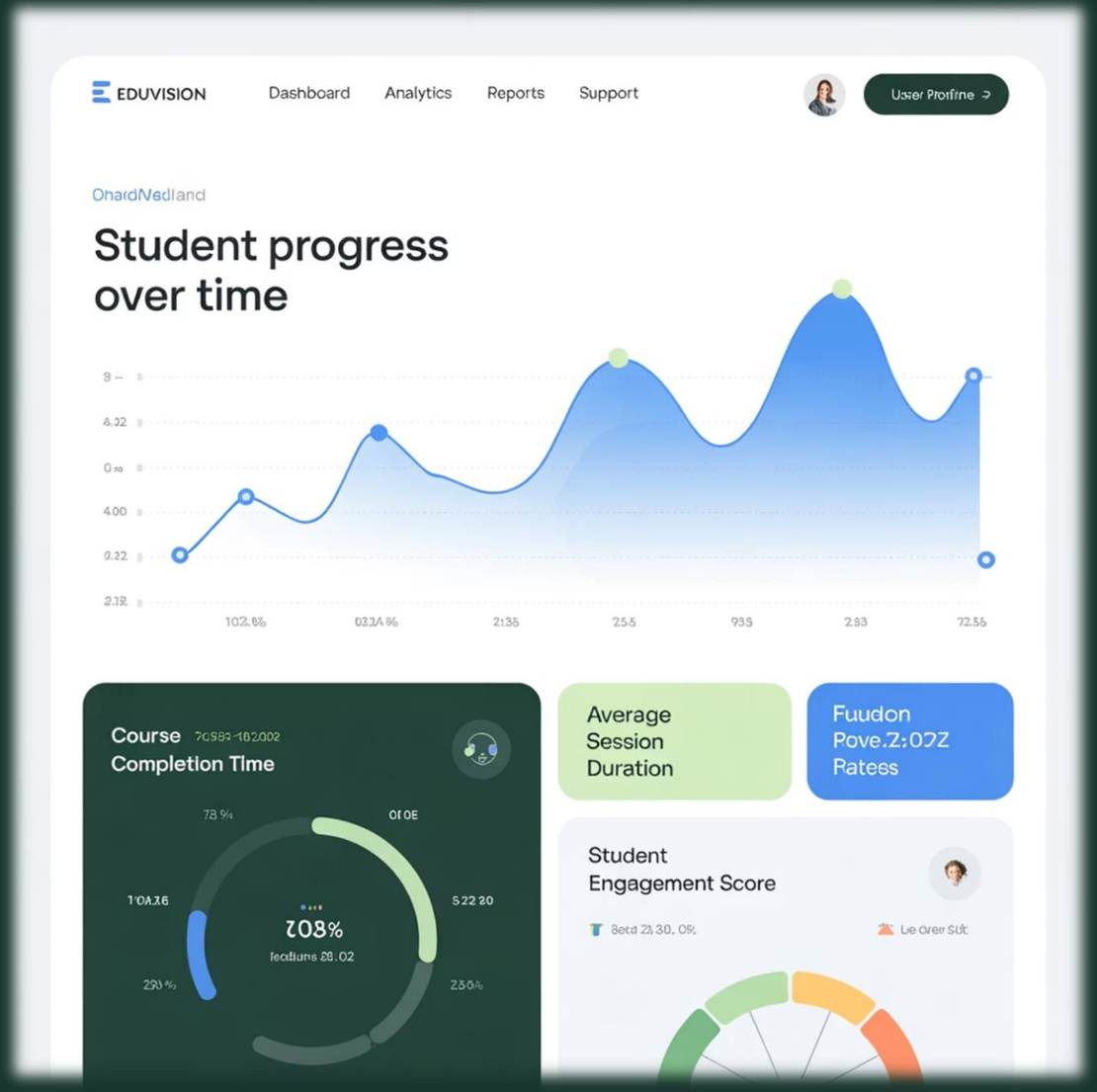
Crescimento do EAD

O ensino à distância tem se expandido rapidamente, criando novos desafios de segurança.

Alunos cada vez mais digitais

A nova geração de estudantes está completamente integrada ao ambiente digital.

Impactos no Planejamento Estratégico



Tecnologia como diferencial competitivo

Instituições que investem em tecnologia segura se destacam no mercado educacional.

Integração TI, compliance e governança

A união dessas três áreas é fundamental para o sucesso estratégico das IES.

Aumento de riscos cibernéticos

Com a digitalização, crescem as ameaças à segurança dos dados institucionais.

ABMES

Ameaças Reais no Setor

Vazamento de dados

Informações sensíveis de alunos e professores expostas publicamente, comprometendo a privacidade e segurança.

Ransomware em universidades

Sequestro de dados críticos com exigência de pagamento para recuperação, paralisando operações acadêmicas.

Fraudes em vestibulares/matrículas

Ataques direcionados aos processos de admissão e matrícula, comprometendo a integridade institucional.

Requisitos Fundamentais

Proteção de dados pessoais (LGPD)

Garantir a conformidade com a Lei Geral de Proteção de Dados é essencial para evitar sanções e proteger informações sensíveis.

Continuidade de serviços críticos

Manter os sistemas educacionais funcionando mesmo em caso de incidenter de segurança.

Governança de riscos

Estabelecer processos claros para identificar, avaliar e mitigar riscos cibernéticos.

Benefícios da Adoção de cibersegurança

Redução de riscos legais e financeiros

Evita multas e processos relacionados a violações de dados e segurança.

Confiança dos alunos e famílias

Fortalece a reputação da instituição como um ambiente digital seguro.

Diferenciação de mercado

Destaca a instituição como referência em segurança e inovação responsável.

Indicadores de Segurança e Continuidade

Tempo médio para responder (MTTR)

Quanto tempo leva para detectar e resolver um incidente de segurança.

Objetivo de ponto de recuperação (RPO)

Quantidade máxima aceitável de perda de dados medida em tempo.

Objetivo de tempo de recuperação (RTO)

Tempo máximo aceitável para restaurar um sistema após um incidente.

Impacto no Negócio

MTTR alto

→ perda de confiança e receita

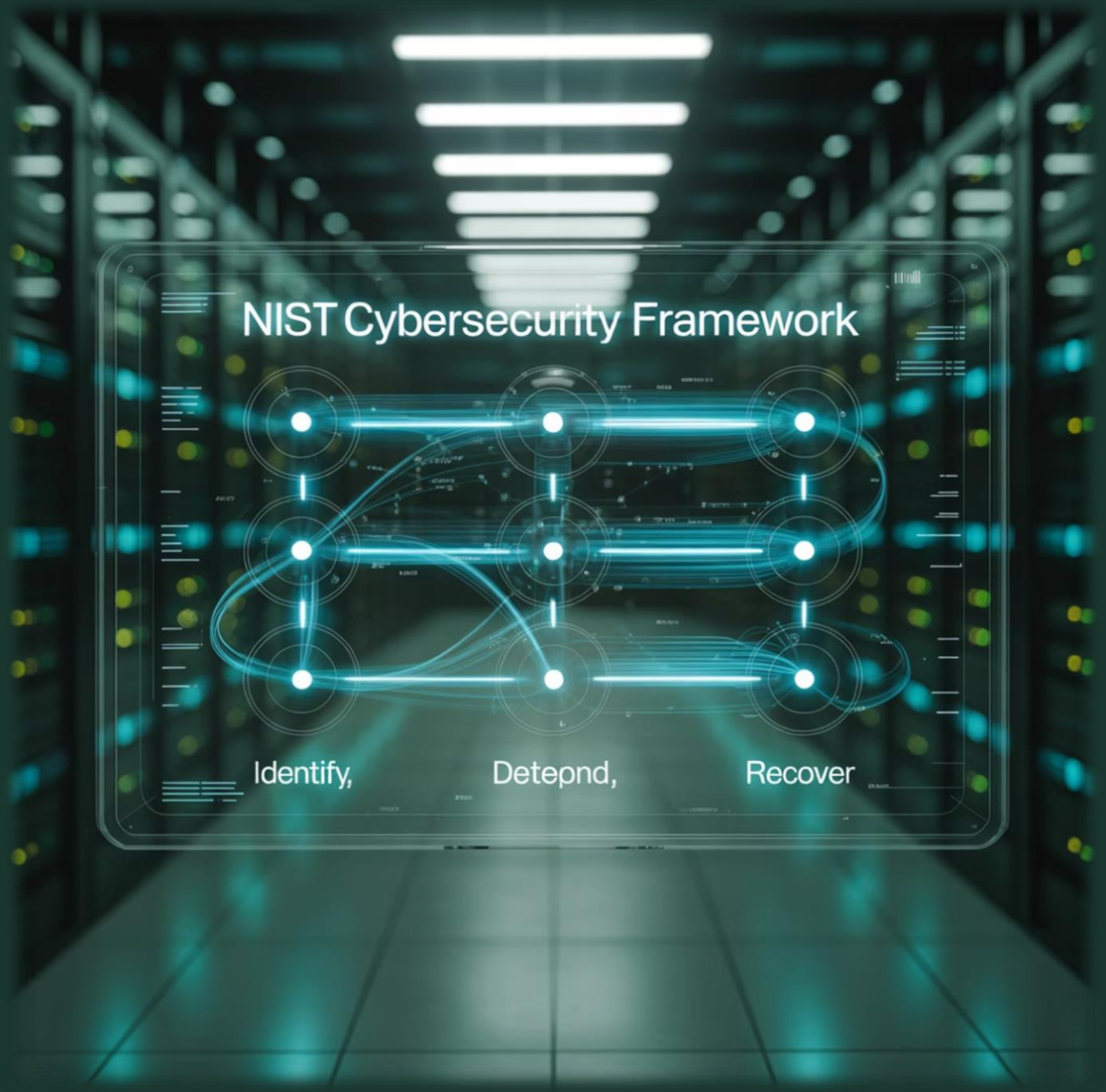
RPO não atendido

→ perda de dados e retrabalho

RTO elevado

→ interrupção das atividades e perda de receita e confiança

O que é o NIST Cybersecurity Framework (CSF)



- Framework global de segurança
- Estrutura em 5 funções: Identify, Protect, Detect, Respond, Recover
- Atividades, resultados desejados e padrões de referência
- Ajudar organizações a compreender, gerenciar e reduzir riscos de segurança cibernética

LGPD e Requisitos Legais

Papéis de controlador e operador

Definição clara das responsabilidades de cada agente no tratamento de dados pessoais.

Prevenção, prestação de contas

Obrigação de implementar medidas preventivas e demonstrar conformidade.

Segurança por design

Incorporação da proteção de dados desde a concepção dos sistemas e processos.

ABMES

Integração NIST CSF + LGPD + RPO/RTO

Alinhamento de frameworks e leis

Integração das melhores práticas internacionais com requisitos legais brasileiros.

Segurança como pilar estratégico

Elevação da cibersegurança ao nível de decisão executiva nas instituições de ensino.

Roadmap de Segurança por Fases

Fase 1: Fundamentos

Estabelecimento das bases essenciais de segurança.

Fase 2: Monitoramento

Implementação de sistemas de vigilância contínua.

Fase 3: Inteligência

Adoção de soluções avançadas de análise e resposta.

Fase 4: Resiliência

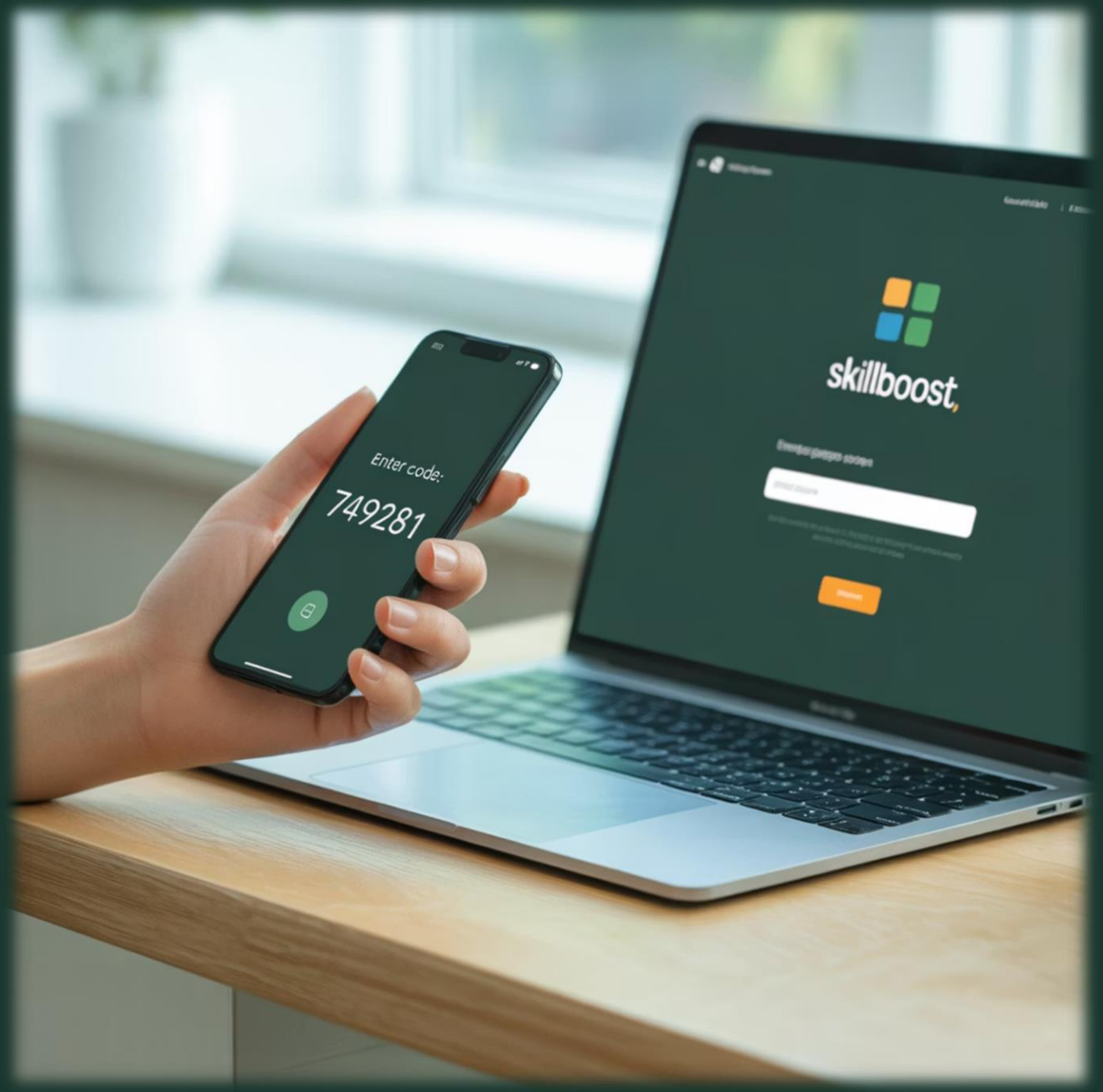
Capacidade de manter operações mesmo sob ataques.

Fase 1 – Fundamentos

Firewall de próxima geração - NGFW:

- O que faz: protege rede contra ataques externos
- NIST: Protect | LGPD: prevenção
- Benefício: evita indisponibilidade
- Caso de uso: portal de matrículas

Fase 1 – Fundamentos



Múltiplo Fator de autenticação - MFA:

- O que faz: exige múltiplas etapas de login
- NIST: Protect | LGPD: segurança por design
- Benefício: impede invasões
- Caso de uso: LMS/ERP

Fase 1 – Fundamentos

Backup & Disaster Recovery:

- O que faz: restauração rápida
- NIST: Recover | LGPD: disponibilidade
- Benefício: RPO<1h, RTO<4h
- Caso de uso: banco acadêmico

Fase 1 – Fundamentos

Antivírus:

- O que faz: bloqueia malware
- NIST: Protect
- Benefício: protege endpoints
- Caso de uso: secretaria/labs

Fase 2 – Monitoramento

Endpoint Detection & Respond:

- Detecta e responde a ameaças
- NIST: Detect + Respond
- Benefício: reduz MTTR
- Caso de uso: servidores de pesquisa

Fase 2 – Monitoramento

Centro de Operações de Segurança - SOC 24x7:

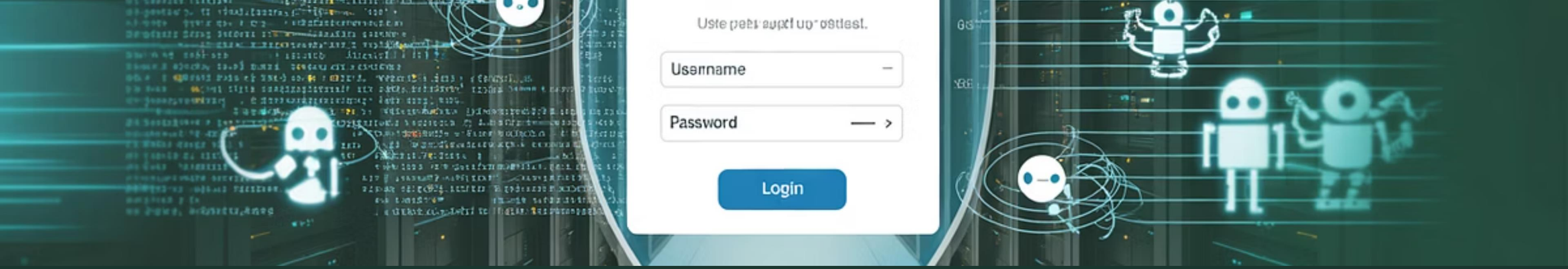
- Monitoramento contínuo
- NIST: Detect
- Benefício: defesa em tempo real
- Caso de uso: vestibulares online

ABMES

Fase 2 – Monitoramento

Gestão de Vulnerabilidades:

- Identifica e corrige falhas
- NIST: Identify + Protect
- Benefício: reduz riscos
- Caso de uso: ERP/biblioteca digital



Fase 2 – Monitoramento

Firewall de proteção Web - WAF:

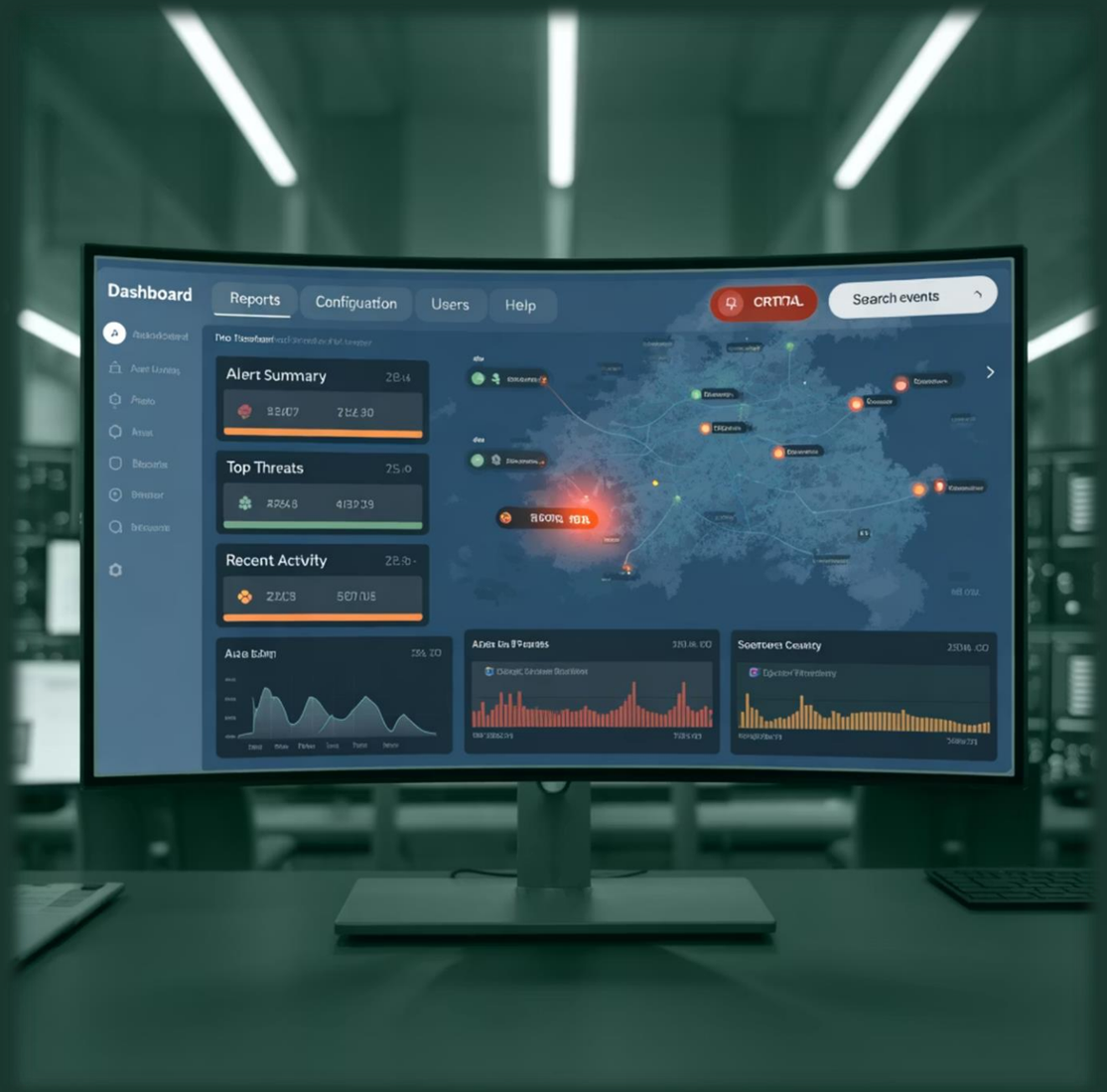
- Protege aplicações web
- NIST: Protect | LGPD: integridade
- Benefício: preserva dados
- Caso de uso: portal do aluno

ABMES

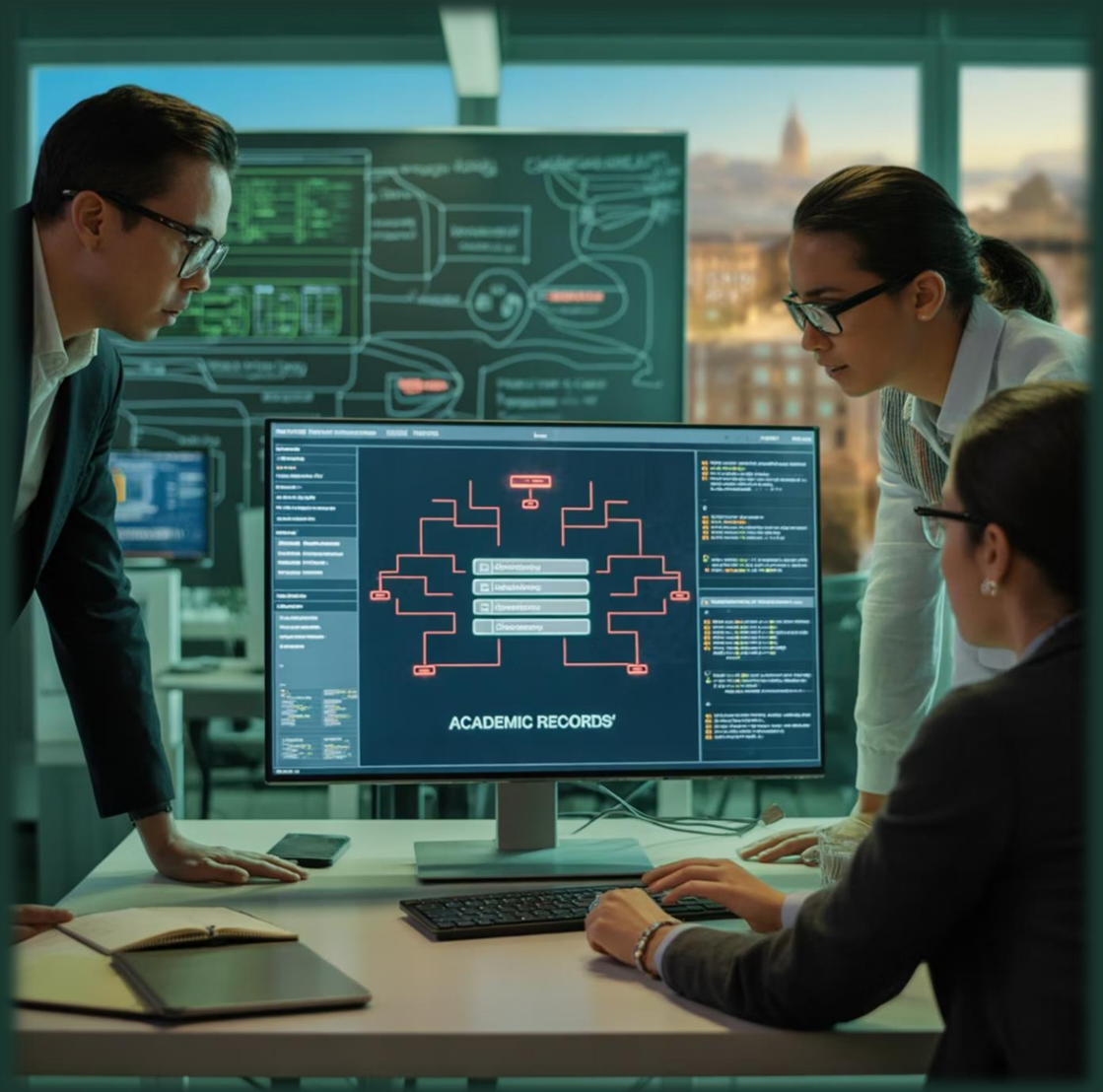
Fase 3 – Inteligência

Sistema de correlação de eventos - SIEM:

- Correlaciona logs e gera alertas
- NIST: Detect
- Benefício: visão executiva
- Caso de uso: ERP+LMS



Fase 3 – Inteligência



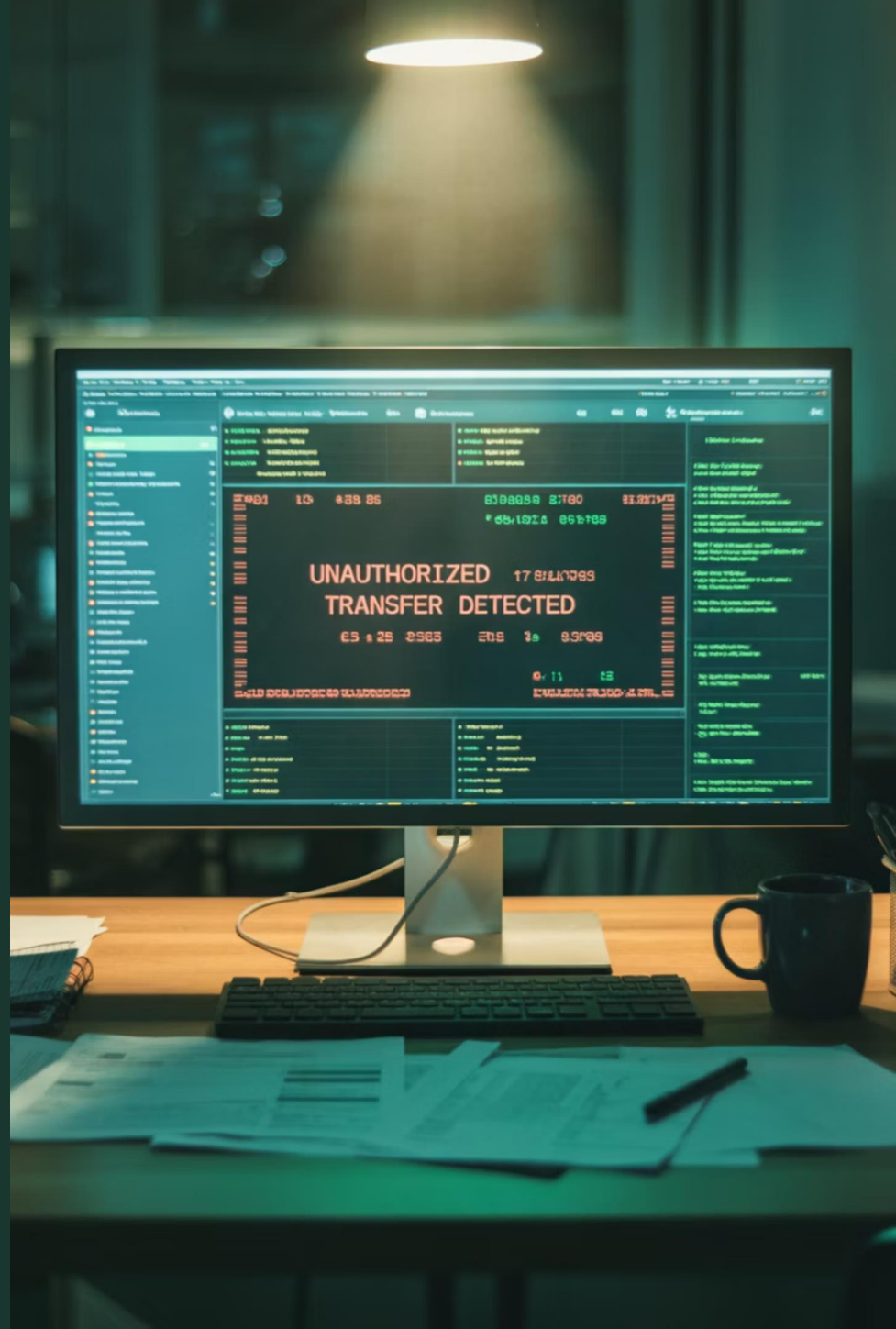
Sistema de automação de resposta - SOAR:

- Automatiza resposta
- NIST: Respond
- Benefício: reduz tempo de contenção
- Caso de uso: fraudes em vestibulares

Fase 3 – Inteligência

Prevenção de vazamento/perda de dados - DLP:

- Bloqueia movimentação de dados sensíveis
- NIST: Protect | LGPD: prevenção
- Benefício: evita vazamentos
- Caso de uso: dados de secretaria



Fase 3 – Inteligência

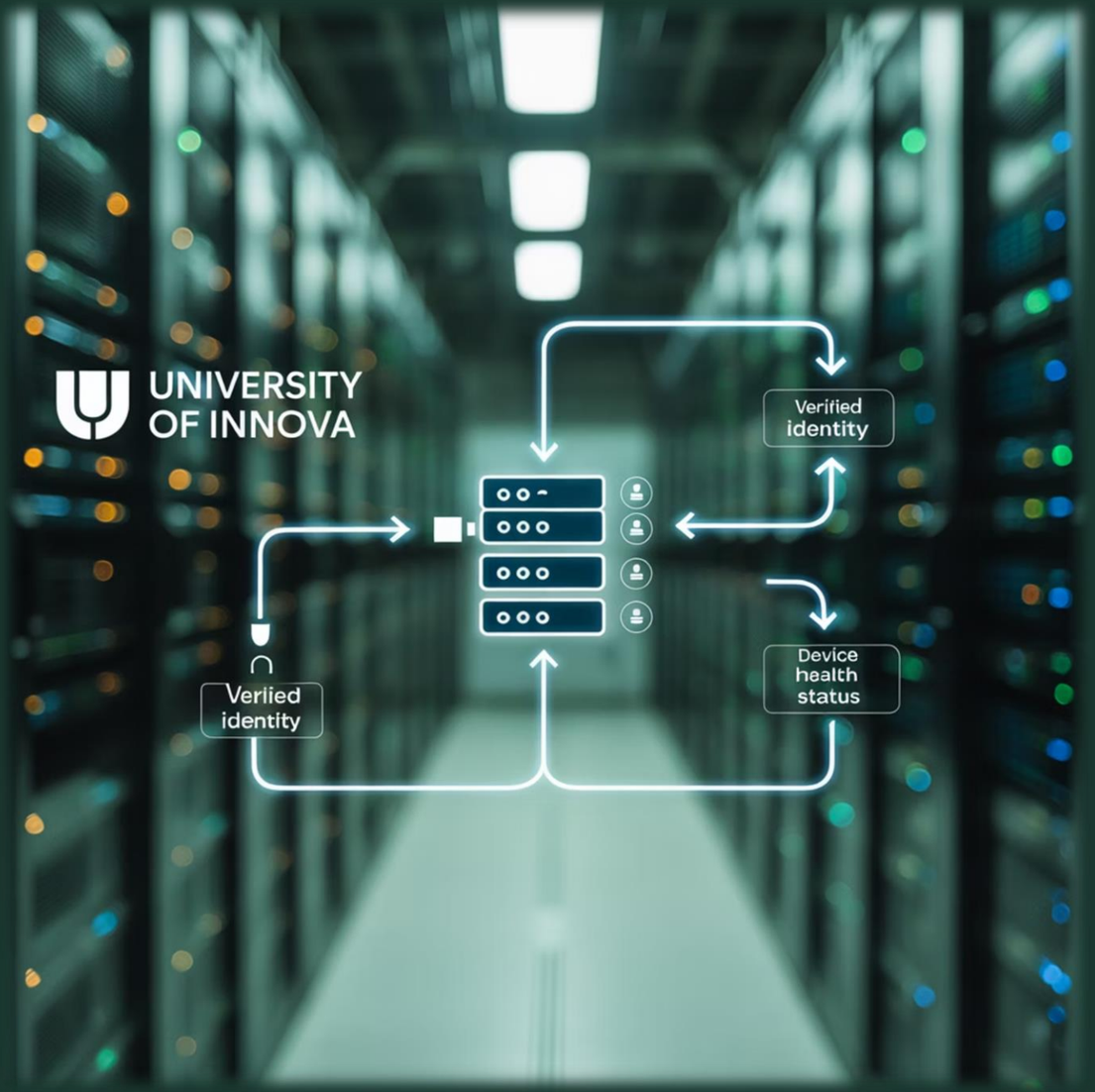
Monitoramento de Dark Web:

- Detecta credenciais expostas
- NIST: Identify + Detect
- Benefício: ação preventiva
- Caso de uso: credenciais de alunos

Fase 4 – Resiliência

Soluções de confiança Zero - Zero Trust:

- Valida identidades e contexto
- NIST: Protect
- Benefício: reduz riscos
- Caso de uso: acessos remotos



Fase 4 – Resiliência

Inteligência de Ameaças - Threat Intelligence:

- Antecipação de ataques globais
- NIST: Identify + Detect
- Benefício: preparar antes do ataque
- Caso de uso: universidades internacionais

Fase 4 – Resiliência

Red/Blue Team:

- Simulações de ataque/defesa
- NIST: Respond + Identify
- Benefício: valida defesas
- Caso de uso: portal de matrícula

Fase 4 – Resiliência

Proteção de acesso a aplicações de nuvem - CASB:

- Controle de SaaS e nuvem
- NIST: Protect + Detect | LGPD: segurança em cloud
- Benefício: evita compartilhamento indevido
- Caso de uso: Google Workspace/Office 365

ABMES

Ferramentas x NIST CSF

Protect

NGFW, MFA, Antivírus, WAF, DLP, Zero Trust, CASB

Identify

Gestão de Vulnerabilidades, Threat Intel, Dark Web, Red Team

Detect

SOC, SIEM, EDR, Dark Web, CASB

Respond

SOAR, Red Team, EDR

Recover

Backup & DR

Casos de Uso Acadêmicos

Portal de matrículas

Protegido por NGFW e WAF

Secretarias

Protegidas com Antivírus e EDR

LMS

Acesso com MFA e DLP

ERP

Integrado a Backup & DR + SIEM

Vestibulares online

Monitorados pelo SOC

Indicadores de Adoção por Fase

% endpoints protegidos

Medição da cobertura de proteção nos dispositivos finais.

% vulnerabilidades corrigidas em SLA

Eficiência na remediação de falhas identificadas.

Conformidade LGPD

Nível de adequação às exigências legais.

RPO/RTO atingidos

Sucesso nos testes de recuperação de desastres.

MTTR médio

Tempo médio de resposta a incidentes.

Fornecedores SaaS – Desafios

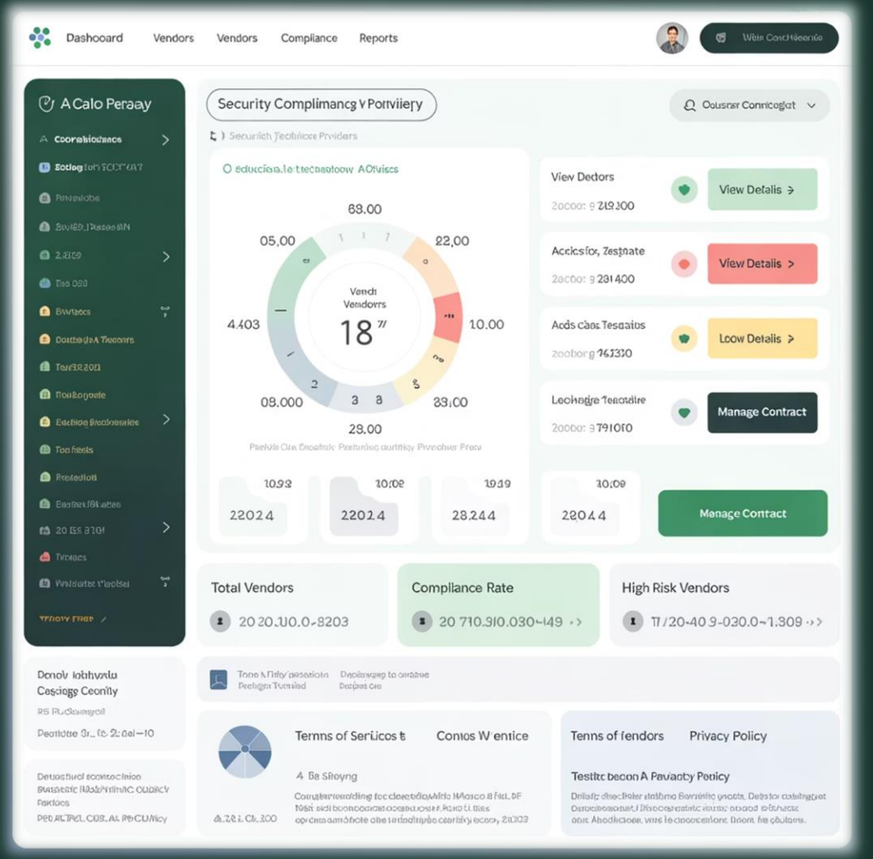
- Dependência tecnológica
- Vazamentos em terceiros
- Continuidade de serviços

Alinhamento de Requisitos com Fornecedores

- SLA de RPO/RTO
- Certificações ISO 27001 / SOC 2
- Criptografia e segregação de dados
- Integração com SIEM/SOC da IES
- Contrato com requisitos de LGPD
- Auditoria e evidências de testes de continuidade e segurança

Benefícios Esperados

- Redução de riscos legais e operacionais
- Confiança institucional
- Continuidade e inovação
- Diferenciação competitiva



Segurança é pauta de conselho

Não é custo: é investimento estratégico

Educação 5.0 exige confiança digital