MATRIZ DE CONFORMIDADE · 01 · FRAMEWORKS UNIVERSAIS

Mapeamento direto · controle CSURFACE × cláusula regulatória

Sete controles entregues pela plataforma CSURFACE, com a cláusula específica de cada framework que cada um atende — NIST CSF, ISO 27001:2022, CIS Controls v8, PCI DSS 4.0 e NIS2. Brasil e setoriais na próxima página.

Datasheet 2026
CSURFACE

Por que esta matriz importa. O auditor não pergunta "vocês têm ASM?". O auditor pergunta "como vocês atendem ao requisito X da norma Y?". Esta matriz responde diretamente — cada controle entregue pela CSURFACE com a cláusula específica que ele atende, em sete frameworks que aparecem em RFP e em parecer regulatório.

CONTROLE CSURFACE	NIST CSF v1.1 / v2.0	ISO 27001:2022 Anexo A	CIS CONTROLS V8 Center for Internet Sec.	PCI DSS 4.0 PCI SSC	NIS2 Diretiva UE 2022/2555
Descoberta contínua da superfície externa Inventário automático e contínuo dos ativos externos, sem agente.	**ID.AM-2** inventário de software	**A.5.9 · A.8.16** inventário · monitoramento	**1.1 · 1.5** asset inventory · descoberta	**11.3.2** scan externo trimestral+	**Art. 21.2(a)** política de risco
Inventário de ativos com classificação e proprietário Atribuição automática de propriedade, setor, categoria e área de negócio.	**ID.AM-1/2/6** hardware · software · papéis	**A.5.9 · A.5.10** inventário · uso aceitável	**1.1 · 1.4 · 2.1** inventário · tags · software	**12.5.1** inventário no escopo PCI	**Art. 21.2(a)** análise de risco
Mapeamento de cadeia digital de fornecedores Três níveis — dependência direta, subfornecedor e subfornecedor do subfornecedor.	**ID.SC-2 · ID.SC-4** fornecedores monitorados	**A.5.20/21/22** cadeia de fornecedores	**15.1 · 15.4** inventário e contratos TPSP	**6.4.3 · 12.8.1** scripts no checkout · TPSPs	**Art. 21.2(d)** segurança de supply chain
Gestão contínua de vulnerabilidades · priorização dinâmica índices de probabilidade de exploração e catálogos de exploração ativa compondo a fila em tempo real.	**DE.CM-8 · ID.RA-1** scan contínuo · vuln. identificadas	**A.5.7 · A.8.8** threat intel · vuln. técnicas	**7.1 · 7.2 · 7.6** processo de vuln. mgmt	**6.3.1 · 11.3** vuln. identificadas e geridas	**Art. 21.2(e)** handling de vuln.
Monitoramento de credenciais vazadas Breach DBs, dark web, repositórios públicos — com validação ativa não-destrutiva.	**ID.RA-3 · DE.CM-7** ameaças externas · monitoramento	**A.5.7 · A.8.16** threat intel · monitoramento	**17.2** canais de reporte de incidente	**8.3.1** MFA contra credenciais comprom.	**Art. 21.2(g)** higiene cibernética
Quantificação financeira de risco · FAIR ALE e VaR sobre cenários quantificados — relatório padrão para conselho.	**ID.RA-4 · ID.RA-5** impacto · risco quantificado	**A.5.4** responsabilidades de gestão	**17.1** programa de RM	**12.3.1** risk assessment formal	**Art. 21.2(a)** análise de risco formal
Trilha auditável de exposição → remediação Cada descoberta com timestamps de detecção, alerta, atribuição e fechamento.	**PR.IP-12 · DE.AE-2** plano de remediação · análise	**A.5.24 · A.8.15** gestão de incidente · logging	**8.2 · 8.5** audit logs · processamento	**10.2.1** audit logs de eventos	**Art. 23** obrigação de reporte

Mapeamento construído a partir das publicações oficiais (NIST CSF v1.1 e v2.0 · ISO/IEC 27001:2022 Anexo A · CIS Controls v8.1 · PCI DSS v4.0 · Diretiva UE 2022/2555 NIS2). A aderência completa a cada framework depende do escopo contratado e da política interna da organização — esta matriz indica onde a capacidade técnica da plataforma se conecta a cada cláusula.

MATRIZ DE CONFORMIDADE · 02 · BRASIL E SETORIAIS · EVIDÊNCIA

BACEN, LGPD, SOX · e o que sai como evidência exportável

Os mesmos sete controles, agora mapeados ao conjunto regulatório brasileiro e setorial. Ao lado, os tipos de artefato que a plataforma exporta — o que o auditor recebe quando pede evidência.

Datasheet 2026
CSURFACE

CONTROLE CSURFACE	BACEN 4.557 Risco operacional	BACEN 4.893 Política de cibersegurança	LGPD Lei 13.709/2018	SOX · ITGCS Sarbanes-Oxley
Descoberta contínua da superfície externa	**Art. 3º · 38º** gestão de risco operacional	**Art. 4º · I** identificar ameaças	**Art. 46** medidas técnicas	**Computer Ops** ITGC · monitoramento
Inventário de ativos com classificação e proprietário	**Art. 3º · IV** identificação de risco	**Art. 3º · II** diretrizes de segurança	**Art. 37 · 46** registro de tratamento	**Access Control** ITGC · controle de ativos
Mapeamento de cadeia digital de fornecedores	**Art. 33º** terceirização relevante	**Art. 5º** avaliação de fornecedores críticos	**Art. 39 · 42** corresponsabilidade do operador	**Vendor Mgmt** ITGC · gestão de fornecedores
Gestão contínua de vulnerabilidades · priorização dinâmica	**Art. 3º · V** monitoramento e mitigação	**Art. 4º · III · IV** detectar · responder	**Art. 46** medidas técnicas e administrativas	**Change Mgmt** ITGC · patch e change
Monitoramento de credenciais vazadas	**Art. 4º** risco de fraude e cibernético	**Art. 4º · III** detectar incidentes	**Art. 46 · 48** proteção · comunicação à ANPD	**Access Control** ITGC · privileged access
Quantificação financeira de risco · FAIR	**Art. 3º · II · III** mensuração e avaliação	**Art. 3º · I** objetivos de cibersegurança	**Art. 50** programa de governança	**Sect. 404** avaliação de controles internos
Trilha auditável de exposição → remediação	**Art. 5º · IV** documentação e reporte	**Art. 8º** plano de ação e resposta	**Art. 48** trilha de incidente	**Audit Logging** ITGC · logs e evidência

Tipos de evidência exportável · o que o auditor recebe

1 Inventário datado
CSV ou JSON de todos os ativos descobertos com timestamp de descoberta, atribuição de propriedade e classificação. Versionado.

2 Trilha de descoberta
Para cada CVE relevante: tempo de detecção, alerta gerado, atribuição, abertura de ticket, fechamento. JSON exportável.

3 Logs de auditoria
Ações de usuário, alterações de configuração, acessos a evidência. Retenção integral durante a janela operacional contratada.

4 Snapshot regulatório
PDF datado com mapeamento de cada controle CSURFACE × cláusula da norma alvo (BACEN, ISO, PCI). Pronto para juntar a parecer.

5 Métricas KRI
Janela de exposição, MTTD, MTTR, cobertura de descoberta, % de fornecedores monitorados — séries históricas para o comitê.

6 Relatório CRQ
ALE e VaR P90/P99 com premissas documentadas, faixas de distribuição e cenários alternativos. Pronto para o comitê de auditoria.

Receba o mapeamento aplicado ao seu ambiente

Solicitar mapeamento