csurface

FICHA TÉCNICA

Matriz de Conformidad · CSURFACE × Regulaciones

MATRIZ DE CONFORMIDAD · 01 · MARCOS UNIVERSALES

Mapeo directo · control CSURFACE × cláusula regulatoria

Siete controles entregados por la plataforma CSURFACE, con la cláusula específica de cada marco que cada uno atiende — NIST CSF, ISO 27001:2022, CIS Controls v8, PCI DSS 4.0 y NIS2. Brasil y sectoriales en la página siguiente.

Ficha técnica 2026
CSURFACE

Por qué esta matriz importa. El auditor no pregunta "¿tienen ASM?". El auditor pregunta "¿cómo atienden el requisito X de la norma Y?". Esta matriz responde directamente — cada control entregado por CSURFACE con la cláusula específica que atiende, en siete marcos que aparecen en RFP y en dictamen regulatorio.

CONTROL 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 Directiva UE 2022/2555
Descubrimiento continuo de la superficie externa Inventario automático y continuo de los activos externos, sin agente.	**ID.AM-2** inventario de software	**A.5.9 · A.8.16** inventario · monitoreo	**1.1 · 1.5** asset inventory · descubrimiento	**11.3.2** escaneo externo trimestral+	**Art. 21.2(a)** política de riesgo
Inventario de activos con clasificación y propietario Asignación automática de propiedad, sector, categoría y área de negocio.	**ID.AM-1/2/6** hardware · software · roles	**A.5.9 · A.5.10** inventario · uso aceptable	**1.1 · 1.4 · 2.1** inventario · tags · software	**12.5.1** inventario en el alcance PCI	**Art. 21.2(a)** análisis de riesgo
Mapeo de cadena digital de proveedores Tres niveles — dependencia directa, subproveedor y subproveedor del subproveedor.	**ID.SC-2 · ID.SC-4** proveedores monitoreados	**A.5.20/21/22** cadena de proveedores	**15.1 · 15.4** inventario y contratos TPSP	**6.4.3 · 12.8.1** scripts en el checkout · TPSPs	**Art. 21.2(d)** seguridad de supply chain
Gestión continua de vulnerabilidades · priorización dinámica Índices de probabilidad de explotación y catálogos de explotación activa componiendo la fila en tiempo real.	**DE.CM-8 · ID.RA-1** escaneo continuo · vuln. identificadas	**A.5.7 · A.8.8** threat intel · vuln. técnicas	**7.1 · 7.2 · 7.6** proceso de vuln. mgmt	**6.3.1 · 11.3** vuln. identificadas y gestionadas	**Art. 21.2(e)** handling de vuln.
Monitoreo de credenciales filtradas Breach DBs, dark web, repositorios públicos — con validación activa no destructiva.	**ID.RA-3 · DE.CM-7** amenazas externas · monitoreo	**A.5.7 · A.8.16** threat intel · monitoreo	**17.2** canales de reporte de incidente	**8.3.1** MFA contra credenciales comprom.	**Art. 21.2(g)** higiene cibernética
Cuantificación financiera de riesgo · FAIR ALE y VaR sobre escenarios cuantificados — informe estándar para el consejo.	**ID.RA-4 · ID.RA-5** impacto · riesgo cuantificado	**A.5.4** responsabilidades de gestión	**17.1** programa de RM	**12.3.1** risk assessment formal	**Art. 21.2(a)** análisis de riesgo formal
Traza auditable de exposición → remediación Cada hallazgo con marcas de tiempo de detección, alerta, asignación y cierre.	**PR.IP-12 · DE.AE-2** plan de remediación · análisis	**A.5.24 · A.8.15** gestión de incidente · logging	**8.2 · 8.5** audit logs · procesamiento	**10.2.1** audit logs de eventos	**Art. 23** obligación de reporte

Mapeo construido a partir de las publicaciones oficiales (NIST CSF v1.1 y v2.0 · ISO/IEC 27001:2022 Anexo A · CIS Controls v8.1 · PCI DSS v4.0 · Directiva UE 2022/2555 NIS2). La adherencia completa a cada marco depende del alcance contratado y de la política interna de la organización — esta matriz indica dónde la capacidad técnica de la plataforma se conecta a cada cláusula.

MATRIZ DE CONFORMIDAD · 02 · BRASIL Y SECTORIALES · EVIDENCIA

BACEN, LGPD, SOX · y lo que sale como evidencia exportable

Los mismos siete controles, ahora mapeados al conjunto regulatorio brasileño y sectorial. Al lado, los tipos de artefacto que la plataforma exporta — lo que el auditor recibe cuando solicita evidencia.

Ficha técnica 2026
CSURFACE

CONTROL CSURFACE	BACEN 4.557 Riesgo operacional	BACEN 4.893 Política de ciberseguridad	LGPD Ley 13.709/2018	SOX · ITGCS Sarbanes-Oxley
Descubrimiento continuo de la superficie externa	**Art. 3º · 38º** gestión de riesgo operacional	**Art. 4º · I** identificar amenazas	**Art. 46** medidas técnicas	**Computer Ops** ITGC · monitoreo
Inventario de activos con clasificación y propietario	**Art. 3º · IV** identificación de riesgo	**Art. 3º · II** directrices de seguridad	**Art. 37 · 46** registro de tratamiento	**Access Control** ITGC · control de activos
Mapeo de cadena digital de proveedores	**Art. 33º** tercerización relevante	**Art. 5º** evaluación de proveedores críticos	**Art. 39 · 42** corresponsabilidad del operador	**Vendor Mgmt** ITGC · gestión de proveedores
Gestión continua de vulnerabilidades · priorización dinámica	**Art. 3º · V** monitoreo y mitigación	**Art. 4º · III · IV** detectar · responder	**Art. 46** medidas técnicas y administrativas	**Change Mgmt** ITGC · patch y change
Monitoreo de credenciales filtradas	**Art. 4º** riesgo de fraude y cibernético	**Art. 4º · III** detectar incidentes	**Art. 46 · 48** protección · comunicación a la ANPD	**Access Control** ITGC · privileged access
Cuantificación financiera de riesgo · FAIR	**Art. 3º · II · III** medición y evaluación	**Art. 3º · I** objetivos de ciberseguridad	**Art. 50** programa de gobernanza	**Sect. 404** evaluación de controles internos
Traza auditable de exposición → remediación	**Art. 5º · IV** documentación y reporte	**Art. 8º** plan de acción y respuesta	**Art. 48** traza de incidente	**Audit Logging** ITGC · logs y evidencia

Tipos de evidencia exportable · lo que el auditor recibe

1 Inventario fechado
CSV o JSON de todos los activos descubiertos con marca de tiempo de descubrimiento, asignación de propiedad y clasificación. Versionado.

2 Traza de descubrimiento
Para cada CVE relevante: tiempo de detección, alerta generada, asignación, apertura de ticket, cierre. JSON exportable.

3 Logs de auditoría
Acciones de usuario, cambios de configuración, accesos a evidencia. Retención integral durante la ventana operacional contratada.

4 Snapshot regulatorio
PDF fechado con mapeo de cada control CSURFACE × cláusula de la norma objetivo (BACEN, ISO, PCI). Listo para adjuntar a un dictamen.

5 Métricas KRI
Ventana de exposición, MTTD, MTTR, cobertura de descubrimiento, % de proveedores monitoreados — series históricas para el comité.

6 Informe CRQ
ALE y VaR P90/P99 con premisas documentadas, rangos de distribución y escenarios alternativos. Listo para el comité de auditoría.

Reciba el mapeo aplicado a su entorno

Solicitar mapeo