



REQUISITOS DO SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Nº Doc. 1

	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >

Sumário

1. Introdução	3
2.1 Recursos de Dados	4
2.2 Recursos de Hardware	
3. Análise de riscos/continuidade/contingência de segurança física e lógica	7

 DevStream	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >


1. Introdução

Este documento estabelece os requisitos fundamentais para a implementação de um Sistema de Gestão de Continuidade de Negócios (SGCN), visando garantir a resiliência operacional e a proteção de ativos críticos em cenários de interrupção. Nele, são abordados os pilares essenciais para sustentar a continuidade das operações, incluindo a gestão de recursos de dados e hardware, além de estratégias robustas para mitigação de riscos.

A estrutura do documento inicia-se com a catalogação de recursos de dados, detalhando fluxos de informação, vulnerabilidades associadas e propostas de soluções técnicas, como validação automatizada e sistemas antifraude. Em seguida, são apresentados os investimentos em infraestrutura física e cloud, com ênfase na justificativa de custos CAPEX e OPEX para garantir desempenho e segurança.


A análise de riscos destaca a identificação de ameaças, vulnerabilidades e medidas de contingência alinhadas à norma ISO 27001, como criptografia de disco, autenticação multifator (MFA) e políticas de backup. Complementando a abordagem teórica, o documento inclui uma demanda prática: o desenvolvimento de um script em C# para inventariar hardware e software em ambientes Windows, integrando-se às necessidades de monitoramento contínuo.

Por fim, o documento reforça a importância de equilibrar custos de segurança e impactos operacionais, assegurando conformidade regulatória e preparação para incidentes. A integração entre processos automatizados, infraestrutura resiliente e práticas de governança sustenta a efetividade do SGCN proposto.

 DevStream	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >


2.1 Recursos de Dados

Informação	Origem	Processamento /Transformação	Saída	Ameaças/ Vulnerabilidade	Proposta de solução
Produto a ser vendido	Sistema de estoque	Validação de código, descrição e quantidade	Registro de produto no sistema	Duplicidade de cadastro (ex.: Stock Keeping Unit repetido)	Identificador único (ex.: código de barras) e validação automática
Requisitos do cliente	Formulário de solicitação (CRM)	Análise de viabilidade (estoques, prazos)	Lista de requisitos aprovados	Dados incompletos ou inconsistentes	Campos obrigatórios no formulário e validação em tempo real
Cotação padrão	Tabela de preços	Cálculo automático (preço unitário x quantidade + impostos)	Documento de cotação (PDF/Excel)	Erros manuais de cálculo	Sistema de precificação integrado com regras de negócio
Cotação personalizada	Solicitação de vendas	Validação técnica (equipe de engenharia/projetos)	Proposta técnica customizada	Especificações incompatíveis com a produção	Checklist de validação antes da emissão
Contrato	Banco de modelos legais	Preenchimento automático de dados do cliente e termos	Contrato pré-formatado	Cláusulas desatualizadas ou ambíguas	Atualização centralizada de templates e revisão jurídica
Aprovação do contrato	Assinatura digital (ex.: DocuSign)	Verificação de autenticidade e registro no sistema	Contrato assinado	Assinaturas falsificadas	Uso de certificados digitais e registro de logs
Pedido confirmado	Sistema de vendas	Verificação de estoque e emissão de ordem de produção	Ordem de produção	Venda de produtos sem estoque	Integração em tempo real com sistemas de estoque
Faturamento	Sistema financeiro	Geração automática de nota fiscal com base no pedido	Nota fiscal eletrônica	Erros de tributação ou dados do cliente	Validação automática de impostos e dados cadastrais
Pagamento	Gateway de pagamento	Processamento de transação (cartão, transferência)	Comprovante de pagamento	Fraude ou chargeback	Sistema antifraude com verificação em duas etapas

 DevStream	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >

2.2 Recursos de Hardware

Categoria	Item	Custo (R\$)	Justificativa
CAPEX	Laptops Dell XPS 15	750000	Máquinas de alto desempenho para desenvolvedores e equipe comercial
	- 50 Laptops a R\$ 15.000 cada		
CAPEX	Periféricos	100000	Configuração ergonômica para o trabalho remoto
	- Monitores, Docks, Headsets, Mouses, Teclados, etc.		
Total CAPEX	Aquisição de equipamentos para funcionário	850000	
OPEX (anual)	Infraestrutura Cloud (AWS)	345000	
	- EC2 (instâncias t3.xlarge)	240000	Servidores virtuais para CI/CD, bancos de dados e aplicações críticas.
	- RDS (PostgreSQL Managed)	60000	Banco de dados gerenciado para armazenar pedidos, contratos e cotações.
	- S3 (Armazenamento)	30000	Armazenamento seguro para documentos (contratos, invoices).
	- Lambda (Serverless)	15000	Automação de processos (ex.: geração de cotações).
OPEX (anual)	Segurança	63000	
	- AWS Shield (DDoS)	45000	Proteção contra ataques às APIs de pagamento e autenticação.
	- AWS WAF (Firewall)	18000	Filtragem de tráfego malicioso.
OPEX (anual)	Ferramentas SaaS	150000	
	Zoom/Slack (Licenças)	60000	Comunicação assíncrona e síncrona para equipes remotas.
	Salesforce (CRM)	90000	Gestão de clientes e pipeline de vendas.

	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >

OPEX (anual)	Backup & Disaster Recovery		
	- AWS Backup	24000	Backup automatizado de bancos de dados e documentos.
OPEX (anual)	Suporte Cloud		
	- Suporte AWS Enterprise	120000	Suporte 24/7 para incidentes críticos.
OPEX (anual)	Treinamento		
	Certificações AWS/DevSecOps para colaboradores	50000	Capacitação da equipe em cloud e segurança.
Total OPEX (anual)			
		752000	


3. Projeto Navegável desenvolvido em C#:

Prints nas pastas em anexo (Prints Aplicação)

Código no repositório do GitHub: [DevStream](#)

4. Análise de riscos/continuidade/contingência de segurança física e lógica

Ativo	Ameaça	Vulnerabilidade	Impacto Potencial	Probabilidade	Nível de risco	Medida de Contingência	Tratamento ISO 27001
Dispositivos Remotos (laptops, USBs)	Roubo ou acesso não autorizado	Falta de criptografia, bloqueio de tela	Vazamento de dados críticos	Alta	Alto	Implementar criptografia total de disco e bloqueio automático	Reduzir
Roteadores domésticos	Ataques via firmware	Firmware desatualizado, configurações padrão	Acesso indevido à rede corporativa	Média	Médio	Reforçar política de BYOD, exigir atualização de firmware	Reduzir

 DevStream	Segurança da Informação				
	DEVSTREAM				
	Classificação	Data	Aprovador	Versão	Páginas
	Interno	21/05/2025	Grupo\$	1	< # >/< # >

Documentos físicos (contratos)	Acesso não autorizado, descarte incorreto	Impressão livre, falta de controle	Vazamento de dados sensíveis, compliance	Média	Médio	Política de impressão segura, descarte seguro (shredder)	Reduzir
APIs financeiras	Injeção de dados, adulterações	Falta de validação de entrada, sem testes regulares	Perda financeira, quebra de integridade	Alta	Alto	Aplicar validação robusta, realizar testes periódicos	Reduzir
Plataformas de e-signature	Phishing, autenticação fraca	Ausência de MFA, falhas de verificação	Assinatura fraudulenta, danos legais	Alta	Alto	Implantar MFA, uso de certificados digitais	Reduzir
Sistemas de precificação	Manipulação interna	Falta de revisão e logs	Distorção de preços, fraude interna	Média	Médio	Auditorias, dupla verificação de alterações	Reduzir
Repositórios de código	Vazamento, backdoors	Uso de plataformas pessoais, sem 2FA	Comprometimento de software, reputação	Alta	Alto	Adoção de repositórios oficiais com 2FA obrigatório	Reduzir
Redes domésticas	Ataques por IoT ou roteadores	Falta de VPN ou segmentação	Invasão indireta à rede corporativa	Média	Médio	Fornecer VPN corporativa, orientar sobre segurança doméstica	Reduzir
Dados em nuvem não homologado	Exposição acidental ou intencional	Uso de plataformas sem criptografia	Vazamento de dados, perda de controle	Alta	Alto	Restringir uso a plataformas homologadas, controle de acesso	Reduzir
Sistemas de autenticação	Ataques de força bruta, credential stuffing	Senhas fracas, sem MFA	Invasão a sistemas críticos	Alta	Alto	Implantar MFA, políticas de senha forte, monitoramento	Reduzir