Compliance e Infraestrutura

Documentação de Continuidade de Negócios e Segurança

Política de RTO/RPO

Código do Documento: POL-RTO-RPO-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes
Área Gestora: Segurança da Informação / TI	Aplica-se a: Todos os Serviços, Bancos de Dados e Aplicações

1. Resumo da Infraestrutura

A plataforma SISMETRO utiliza atualmente o motor de banco de dados MySQL 8.4 hospedado na Amazon Web Services (AWS) na região São Paulo (sa-east-1).
A arquitetura foi desenhada para garantir que os dados estejam sempre disponíveis e protegidos contra falhas de hardware ou desastres geográficos.

2. Objetivos de Recuperação (Métricas Principais)

Métrica	Objetivo	Descrição
RTO (Tempo de Recuperação)	1 Hora	Tempo máximo para o sistema voltar a operar após uma falha crítica na instância principal.
RPO (Ponto de Recuperação)	Próximo a Zero	Quantidade máxima de dados que podem ser perdidos. Graças à replicação síncrona, a perda é virtualmente nula.

3. Estratégias de Resiliência Aplicadas

A. Alta Disponibilidade (Multi-AZ)
Diferente de servidores convencionais, o nosso banco de dados opera em modo Multi-AZ (Multi-Availability Zones).

- **Replicação Síncrona:** Cada dado gravado no banco principal (sa-east-1a) é replicado instantaneamente para uma instância de reserva (standby) em uma zona isolada (sa-east-1c).
- **Failover Automático:** Se a zona principal sofrer uma interrupção, o AWS RDS detecta a falha e redireciona todo o tráfego para a reserva automaticamente em cerca de 60 segundos, sem necessidade de intervenção manual ou alteração de configurações pelos

usuários.

B. Política de Backup e Retenção
Utilizamos o AWS Backup para garantir camadas extras de proteção:

- **Snapshots Diários e Horários:** Mantemos um histórico rigoroso de snapshots (capturas de estado) criados automaticamente a cada hora.
- **Point-in-Time Recovery (PITR):** Podemos restaurar o banco de dados para qualquer segundo específico dos últimos 7 dias. Isso protege o cliente não apenas contra falhas técnicas, mas também contra erros humanos (como exclusões acidentais de dados).

C. Performance e Segurança
Armazenamento gp3: Utilizamos volumes SSD de última geração com IOPS provisionados, garantindo que a recuperação e o processamento de dados ocorram na velocidade máxima permitida pela tecnologia atual.

Criptografia: Todos os dados, tanto em repouso quanto nos backups, são criptografados usando chaves AES-256 (AWS KMS).

Definição de Separação de Dados Multi-tenant

Código do Documento: DEF-SEP-MUL-TEN-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes
Área Gestora: Segurança da Informação / TI	Aplica-se a: Todos os Serviços, Bancos de Dados e Aplicações

A arquitetura de isolamento por chaves de identificação (também conhecida como *Logical Multi-tenancy* ou *Row-Level Isolation*) é uma estratégia robusta e eficiente para sistemas SaaS que utilizam uma base de dados compartilhada.

1. O Conceito de Isolamento Lógico

Diferente de modelos onde cada cliente tem seu próprio banco de dados (o que elevaria drasticamente o custo de infraestrutura no AWS RDS), o SISMETRO utiliza um Banco de Dados Consolidado.

- **A Chave de Identificação:** Cada tabela que contém dados sensíveis ou de clientes possui uma coluna identificadora (tenant_id).
- **Filtro em Camada de Aplicação:** O isolamento ocorre no nível do código (Aplicação). Toda e qualquer consulta ao banco de dados é automaticamente "carimbada" com o ID do cliente logado (tenant_id), garantindo que um Cliente A jamais visualize registros do Cliente B, mesmo estando na mesma tabela física.

2. Vantagens Estratégicas para o Cliente

Ao descrever isso para um fornecedor ou auditoria, os pontos de destaque são:

- **Segurança de Dados:** O isolamento é garantido por políticas globais no código, o que minimiza o erro humano de esquecer um filtro em uma consulta específica.
- **Performance Consistente:** Utilizando de instâncias potentes, replicadas e armazenamento extensível, o ganho de escala beneficia todos os clientes. O banco de dados consegue gerenciar índices globais de forma muito mais performática do que centenas de pequenos bancos separados.
- **Agilidade em Atualizações:** Quando é atualizada a estrutura do banco (migrações), todos os clientes recebem as melhorias de segurança e performance simultaneamente.

Acordo de Nível de Serviço (SLA)

Código do Documento: DEF-SLA-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes
Área Gestora: Segurança da Informação / TI	Aplica-se a: Plataforma SISMETRO (APIs, Web e Arquitetura AWS)

1. Visão Geral e Objetivos

Este documento define os níveis formais de serviço, disponibilidade, metas de recuperação e responsabilidades de suporte técnico para a infraestrutura e ecossistema de software da plataforma SISMETRO.

O objetivo é garantir a continuidade do negócio, prever mitigação de riscos operacionais e estabelecer clareza sobre métricas chave de disponibilidade (Uptime), Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO).

2. Métricas Globais de Disponibilidade (Uptime)

A infraestrutura core do SISMETRO opera em alta disponibilidade na nuvem Amazon Web Services (AWS). O SLA global de disponibilidade da aplicação é estruturado da seguinte forma:

Componente / Serviço	**Meta de SLA (Uptime)**	**Janela de Indisponibilidade Máxima Estimada**
Infraestrutura AWS (ECS Fargate / RDS / CloudFront)	99,9%	~43 minutos/mês
Aplicações Web & APIs (Laravel / Angular)	99,5%	~3,6 horas/mês
Serviços de Terceiros e Integrações (Protheus / Provedores)	99,0%	~7,2 horas/mês

Nota: Janelas de manutenção programada precedidas de aviso prévio não contabilizam como indisponibilidade não planejada.

3. Continuidades e Tolerância a Desastres (RPO e RTO)

Os procedimentos de tolerância a falhas e planos de mitigação e contingência são apoiados por snapshots automáticos e rotinas do AWS Backup e replicação de dados no MySQL / RDS.

Métrica	Definição	Meta Garantida
RPO (Recovery Point Objective)	Quantidade máxima tolerável de perda de dados expressa em tempo.	≤ 1 hora (Backups contínuos / Transaction logs & Snapshots)
RTO (Recovery Time Objective)	Tempo máximo para restauração completa dos serviços após desastre.	≤ 2 horas (Ambiente multi-az / Fargate auto-recovery)

4. Classificação de Incidentes e Matriz de Resposta

Os chamados e incidentes reportados no SISMETRO são categorizados pelo seu nível de severidade e impacto no negócio:

Nível de Severidade	Descrição / Critério de Impacto	Tempo de Primeira Resposta	Tempo de Resolução / Solução Contorno
P1 - Crítico (Urgent)	Sistema totalmente inoperante para todos os usuários ou perda crítica de dados sem solução de contorno.	Até 15 minutos	Até 2 horas
P2 - Alto (High)	Funcionalidade principal afetada (ex: falhas em rotas cruciais de sincronização ou ordens de serviço), com impacto significativo.	Até 1 hora	Até 8 horas
P3 - Médio (Normal)	Problema parcial em funcionalidades secundárias ou degradação leve de performance sem paralisação.	Até 4 horas	Até 24 horas
P4 - Baixo (Low)	Dúvidas técnicas, solicitações de melhorias, bugs estéticos ou pequenos ajustes visuais.	Até 8 horas (dias úteis)	A combinar conforme Sprint

5. Procedimentos de Manutenção e Janelas Programadas

- Manutenções Preventivas / Deployments: Realizados preferencialmente fora do horário de pico comercial (22h às 05h - BRT).
- Notificação Prévia: Comunicados com pelo menos 48 horas de antecedência aos gestores técnicos em caso de impactos previstos superior a 15 minutos.
- Deploy Contínuo (CI/CD): Atualizações transparentes via pipeline GitHub / ECS sem downtime para correções pontuais.

6. Exclusões de Cobertura do SLA

O presente SLA não se aplica a indisponibilidades decorrentes de:

1. Interrupção em provedores locais de internet do cliente ou falhas de hardware e rede local das unidades de atendimento.
2. Integrações com APIs de terceiros que estejam inoperantes fora do controle do SISMETRO.
3. Ações fraudulentas, mau uso deliberado do sistema ou violações de segurança originadas por credenciais comprometidas do próprio cliente.
4. Eventos de Força Maior ou desastres naturais que afetem regiões inteiras de datacenters da AWS.

Política de controle de acesso

Código do Documento: POL-CTL-ACS-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno
Área Gestora: Segurança da Informação / TI	Aplica-se a: Todos os Colaboradores e Prestadores de Serviço

1. OBJETIVO

Esta Política estabelece as diretrizes e padrões necessários para garantir a proteção, integridade, confidencialidade e disponibilidade dos ativos de informação da organização. Seu propósito principal é assegurar que o acesso a dados, sistemas, redes e infraestruturas seja concedido estritamente a usuários e serviços devidamente autorizados, prevenindo acessos indevidos, incidentes de segurança e vazamentos de dados.

2. ALCANCE E APLICAÇÃO

As diretrizes contidas neste documento aplicam-se obrigatoriamente a:

- Todos os colaboradores diretos, estagiários, diretores e prestadores de serviços terceirizados;
- Todas as plataformas, sistemas corporativos, bancos de dados, redes e infraestruturas em nuvem ou locais (*on-premises*);
- Serviços e integrações automatizadas (*APIs*, *jobs*, contas de serviço).

3. PRINCÍPIOS FUNDAMENTAIS

O controle de acesso corporativo deve seguir rigorosamente os três princípios abaixo:

Princípio	Descrição Operacional
Menor Privilégio (Least Privilege)	Todo usuário ou serviço receberá apenas o nível mínimo de permissões indispensável para a execução regular de suas atribuições.
Necessidade de Conhecer (Need-to-Know)	A concessão de acesso a informações restritas ou sensíveis fundamenta-se na necessidade técnica ou operacional, e não no nível hierárquico do solicitante.
Segregação de Funções (Separation of Duties - SoD)	Processos críticos que envolvam riscos operacionais ou financeiros devem exigir a atuação/aprovação de pessoas distintas, evitando a concentração de privilégios.

4. DIRETRIZES DE AUTENTICAÇÃO E IDENTIDADE

4.1. Credenciais Individuais e Intransferíveis

É expressamente proibido o compartilhamento de logins, senhas, chaves de API ou quaisquer outras credenciais de acesso entre colaboradores. Toda conta deve estar associada a uma identidade individual rastreável.

4.2. Autenticação Multi-Fator (MFA)

A utilização de Autenticação Multi-Fator (MFA) é obrigatória para todos os acessos a sistemas corporativos, plataformas em nuvem, ambientes de desenvolvimento e produção, sem exceções.

4.3. Requisitos de Senhas e Chaves

- As senhas corporativas devem atender aos requisitos mínimos de complexidade e tamanho estabelecidos pela equipe de TI;
- Chaves de acesso a ambientes de produção e APIs devem ser armazenadas em cofres de senhas corporativos e rotacionadas periodicamente.

5. GESTÃO DO CICLO DE VIDA DE ACESSOS

5.1. Concessão de Acesso

A liberação de acessos depende obrigatoriamente de solicitação formal realizada via canal oficial de TI, acompanhada da justificativa operacional e da aprovação expressa da liderança imediata e do responsável pelo recurso/sistema.

5.2. Movimentação e Desligamento

- Mudança de Cargo/Função: A área de Recursos Humanos deve notificar a TI sobre transferências internas para que os acessos anteriores sejam revogados e novos perfis ajustados.
- Desligamento: Em caso de encerramento do vínculo contratual, o bloqueio das contas e revogação das permissões devem ser executados imediatamente após a notificação oficial.

6. MONITORAMENTO, RASTREABILIDADE E AUDITORIA

Todos os sistemas, bancos de dados, aplicações e ativos de rede devem gerar registros de auditoria (*logs*) contendo:

- Identificação do usuário ou serviço;
- Data e hora exata do evento (*timestamp*);
- Tipo de tentativa de acesso (sucesso ou falha);
- Ação executada ou alteração efetuada em privilégios.

7. RESPONSABILIDADES E PENALIDADES

O descumprimento das normas estabelecidas nesta Política de Controle de Acesso sujeita o infrator às sanções disciplinares previstas em contrato de trabalho e no regimento interno da empresa, além de eventuais penalidades cíveis e criminais aplicáveis nos termos da legislação vigente.

Política de Segurança da Informação e da Prestação de Serviços

Código do Documento: PSI-SER-001	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Fornecedores
Área Responsável: Governança de TI e Segurança da Informação	Aplica-se a: Todos os Serviços, Sistemas e Colaboradores

1. OBJETIVO

Esta Política de Segurança da Informação (PSI) visa estabelecer os requisitos, diretrizes e padrões de segurança aplicáveis à prestação de serviços, manutenção de sistemas e gestão de infraestrutura de tecnologia. O objetivo principal é garantir a proteção contra acessos não autorizados, indisponibilidade, alterações indevidas ou vazamentos de dados, assegurando a conformidade com as melhores práticas do mercado e exigências regulatórias (incluindo LGPD).

2. ALCANCE E ESCOPO

As diretrizes estipuladas nesta norma aplicam-se integralmente a:

- Todos os serviços prestados, mantidos ou operados pela organização;
- Ambientes de produção, homologação e desenvolvimento (nuvem e on-premises);
- Bancos de dados, APIs, micros serviços, integrações e pipelines de implantação;
- Colaboradores, terceiros, fornecedores e prestadores de serviços que tenham acesso aos ambientes operacionais.

3. PILARES DA SEGURANÇA DA INFORMAÇÃO

A prestação e operação dos serviços são regidas por quatro pilares essenciais:

Pilar	**Descrição Técnica e Operacional**

Confidencialidade	Garantia de que os dados transacionados e armazenados no serviço estejam acessíveis exclusivamente por sistemas e pessoas formalmente autorizados.
Integridade	Salvaguarda da exatidão e do estado completo das informações e sistemas, protegendo-os contra modificações não autorizadas ou acidentais.
Disponibilidade	Garantia de que os serviços e dados permaneçam operacionais e acessíveis para os usuários autorizados sempre que necessário.
Rastreabilidade (Auditabilidade)	Capacidade de registrar, monitorar e auditar todas as ações, acessos e alterações realizadas no ambiente do serviço.

4. DIRETRIZES DE SEGURANÇA APLICÁVEIS AO SERVIÇO

4.1. Controle de Acesso e Gestão de Identidade

- Autenticação Forte: Obrigatoriedade do uso de Autenticação Multi-Fator (MFA) para todas as conexões administrativas e acesso aos ambientes de infraestrutura.
- Princípio do Menor Privilégio: Acesso a servidores, bancos de dados e ferramentas concedido estritamente com base na necessidade funcional (Need-to-Know).
- Contas de Serviço: Credenciais de integrações, APIs e processos automatizados devem utilizar chaves temporárias ou ser mantidas em cofres de segredos (*secret managers*) protegidos.

4.2. Segurança em Redes e Infraestrutura

- Segregação de Ambientes: Isolação lógica rigorosa entre ambientes de Desenvolvimento, Testes/Homologação e Produção.
- Proteção de Perímetro: Uso de firewalls de aplicação (WAF), restrições de redes privadas (VPC/Subnets) e proteção contra ataques de negação de serviço (DDoS).
- Criptografia: Criptografia obrigatória de dados em trânsito (HTTPS/TLS 1.2+) e de dados em repouso (*Data at Rest*) utilizando algoritmos consolidados.

4.3. Desenvolvimento Seguro e Gestão de Mudanças

- Práticas de DevSecOps: Análise estática de código (SAST) e varreduras de vulnerabilidades automatizadas durante a esteira de build e deploy.
- Gestão de Dependências: Revisão e atualização contínua de bibliotecas e pacotes para prevenir vulnerabilidades conhecidas (CVEs).
- Versionamento e Revisão de Código: Nenhuma alteração pode ir para produção sem revisão por pares (*Peer Review*) e validação dos testes automatizados.

5. CONTINUIDADE DE NEGÓCIOS E BACKUP

Para assegurar a resiliência dos serviços, a infraestrutura deve seguir as diretrizes de backup e recuperação estipuladas:

- Rotina de Backups: Realização de backups diários incrementais e snapshots periódicos automatizados.
- Testes de Restauração: Execução regular de simulações de restauração para validar a integridade das cópias de segurança.
- Planos de RPO e RTO: Manutenção de metas de RPO (Objetivo de Ponto de Recuperação) e RTO (Objetivo de Tempo de Recuperação) compatíveis com o Acordo de Nível de Serviço (SLA) estabelecido.

6. GESTÃO DE INCIDENTES DE SEGURANÇA

Em caso de suspeita ou confirmação de incidente de segurança afetando o serviço:

- A equipe técnica deve conter imediatamente a ameaça, isolando os componentes afetados;
- Os registros e evidências devem ser preservados para análise forense e causa-raiz;
- Notificação formal aos gestores e partes interessadas conforme prazos legais e regimentais estabelecidos.

7. CONFORMIDADE E AUDITORIA

Esta política é revisada periodicamente para assegurar sua eficácia e adequação aos avanços tecnológicos e legais. O descumprimento destas diretrizes pode acarretar sanções contratuais e disciplinares cabíveis.

Gestão e Histórico de Releases

Código do Documento: GES-HTR-REL-001	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Engenharia de Software / DevOps	Aplica-se a: Todos os Serviços e Microsserviços

1. OBJETIVO

Esta declaração formal visa comprovar a existência e a aplicação contínua de processos padronizados de gestão de releases, controle de versão e auditoria de alterações no código-fonte dos sistemas e serviços mantidos pela organização.

2. ESTRUTURA E REPOSITÓRIO DE CÓDIGO (GITHUB)

A gestão de versões de todos os serviços da organização é centralizada no provedor **GitHub**, utilizando repositórios privados e seguros. O controle de mudanças e histórico de lançamentos é rastreado de forma automatizada atrelado à esteira de integração e entrega contínuas (CI/CD).

2.1. Modelo de Ramificação (Branching Strategy)

Os repositórios seguem um fluxo de trabalho estruturado, com ramificações (*branches*) específicas destinadas à segregação de ambientes e garantia de qualidade:

Branch / Ramo	**Ambiente Associado**	**Finalidade e Critérios de Aprovação**
`main` / `master` / `prod`	Produção (Prod)	Código em execução operacional. Alterações entram via Pull Requests (PRs) aprovados após validação em homologação e testes.
`staging` / `stage`	Homologação (Stage)	Ambiente pré-produção utilizado para validação final e aprovação do time de produto/cliente.
`qa` / `testing`	Qualidade / Testes (QA)	Ambiente dedicado para serviços aplicáveis, onde são executados testes de regressão e garantia de qualidade antes do merge para staging.

`feature/*` ou `fix/*`	Desenvolvimento Local	Ramos isolados para implementação de melhorias ou correções específicas, originando Pull Requests para revisão de código.

3. MEIOS DE REGISTRO E RASTREABILIDADE DE HISTÓRICO

O histórico completo de revisões, modificações relevantes e pacotes liberados em produção é mantido através das seguintes ferramentas nativas do GitHub:

- GitHub Releases & Tags: As versões oficiais enviadas para produção são marcadas por meio de *Tags* e consolidadas na aba *Releases* do repositório, adotando versionamento semântico (ex.: `v2.5.0`).
- Commits Auditáveis: Cada commit contém autor, data, hora e mensagem descritiva da alteração realizada no sistema.
- Rastreabilidade por Pull Requests (PRs): Todo envio de código para as branches de `qa`, `stage` e `prod` exige abertura de PR, vinculando a alteração à tarefa correspondente.
- GitHub Actions / CI-CD Logs: Cada alteração aprovada aciona pipelines automatizadas cujos históricos de compilação, testes e *deploy* permanecem salvos e auditáveis.

Plano de Recuperação de Desastres (Disaster Recovery Plan)

Código do Documento: PLN-DST-RCV-025	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Infraestrutura, Cloud & DevOps	Aplica-se a: Todos os Serviços, Bancos de Dados e Aplicações

1. OBJETIVO

Este documento estabelece a política, os procedimentos e as diretrizes técnicas de Recuperação de Desastres (*Disaster Recovery*) aplicáveis aos serviços prestados pela organização. Seu propósito é assegurar a restauração das operações em caso de indisponibilidades críticas, falhas catastróficas de infraestrutura, desastres naturais ou incidentes graves de segurança.

2. ESTRATÉGIA DE INFRAESTRUTURA EM NUVEM (AWS)

A arquitetura de hospedagem adota serviços gerenciados nativos da Amazon Web Services (AWS), projetada com redundância e alta disponibilidade por padrão:

- Computação (ECS / Fargate): Contêineres de aplicação implantados de forma distribuída em múltiplas Zonas de Disponibilidade (Multi-AZ), garantindo resiliência contra falhas em data centers individuais.
- Banco de Dados (Amazon RDS / MySQL): Utilização de instâncias Multi-AZ com replicação síncrona automática para um ambiente secundário e criação de snapshots periódicos gerenciados pelo AWS Backup.
- Entrega e Armazenamento (CloudFront & S3): Distribuição global de conteúdo estático via CDN (CloudFront) e armazenamento resiliente de objetos com replicação de dados.

3. MÉTRICAS CHAVE DE CONTINUIDADE (RPO E RTO)

O plano de recuperação fundamenta-se nas seguintes metas de nível de serviço para ambientes críticos de produção sendo as métricas e definições em documento próprio.

4. PROCEDIMENTOS DE BACKUP E RESTAURAÇÃO

4.1. Política de Backup Automatizado

- Snapshots de Banco de Dados: Capturas diárias retidas por 30 dias com habilitação de *Point-in-Time Recovery* (PITR), permitindo a restauração do banco de dados para qualquer segundo dentro do período de retenção.
- Infraestrutura como Código (IaC): Definições de infraestrutura, redes e contêineres mantidas em repositórios controlados no GitHub, permitindo a reconstrução automatizada do ambiente.
- Criptografia e Proteção: Todos os dados em repouso e backups são criptografados utilizando chaves gerenciadas via AWS KMS.

4.2. Fluxo de Restauração em Caso de Desastre

1. Identificação e Declaração de Incidente: Detecção do evento crítico via monitoramento de disponibilidade e acionamento da equipe de DevOps.
2. Isolamento da Origem: Bloqueio das entradas comprometidas ou redirecionamento de tráfego de rede via DNS/CloudFront.
3. Restauração da Base de Dados: Provisionamento de uma nova instância RDS a partir da réplica limpa ou do snapshot mais recente (PITR).
4. Redeployment dos Serviços: Execução das pipelines de CI/CD para subir os contêineres das aplicações no ECS Fargate apontando para a nova base.
5. Validação e Testes de Fumaça: Verificação da integridade das rotas, serviços de autenticação e persistência de dados antes da liberação.
6. Redirecionamento de Tráfego: Alteração dos registros de DNS para restabelecer o serviço para os usuários finais.

5. TESTES E AUDITORIA PERIÓDICA

A eficácia do Plano de Recuperação de Desastres é validada periodicamente por meio de:

- Simulação de Restauração: Testes semestrais de recuperação da base de dados e reprovisionamento de contêineres em ambiente de homologação (*Stage*);
- Revisão de Políticas: Atualização anual deste documento ou sempre que houver mudanças relevantes na arquitetura do sistema.

Declaração de Governança de Fornecedores

Código do Documento: DEC-FOR-TER	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Engenharia de Software & DevOps	Aplica-se a: Gestão de Infraestrutura e Serviços em Nuvem

1. OBJETIVO

Este documento apresenta a declaração formal de identificação de terceiros críticos e a estratégia de validação e governança de fornecedores.

2. IDENTIFICAÇÃO DE TERCEIROS CRÍTICOS

A prestação de serviços utiliza uma estrutura de terceiros que abrange infraestrutura em nuvem, suporte técnico especializado e serviços de desenvolvimento de software terceirizado:

Fornecedor / Terceiro	Papel / Escopo Técnico	Nível de Criticidade	Controles & Certificações de Segurança
AWS (Amazon Web Services) São Paulo	Provedor global de infraestrutura em nuvem (hospedagem ECS/Fargate, bancos de dados RDS MySQL, armazenamento S3, redes e backups).	Alta	Certificações mundiais de conformidade ativa, incluindo ISO/IEC 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI-DSS e conformidade com LGPD/GDPR.
Nuvme (AWS Partner)	Parceiro especializado para suporte técnico consultivo, arquitetura de infraestrutura e sustentação do ambiente AWS.	Média	Acesso restrito via credenciais temporárias (IAM) sob o princípio do menor privilégio, contrato de confidencialidade (NDA) e canal oficial de chamados.

Desenvolvedores / Consultorias Terceirizadas de Software	Desenvolvimento, manutenção de código-fonte, correção de bugs e evolução das aplicações do ecossistema.	Média/Alta	Contratos com cláusulas estritas de confidencialidade (NDA), acessos nomeados e individuais no GitHub com MFA obrigatório, revisão de código (Code Review) antes do merge para produção e sem acesso direto a dados sensíveis de produção.

3. VALIDAÇÃO E GOVERNANÇA DE FORNECEDORES

3.1. Validação do Provedor de Infraestrutura (AWS)

Por tratar-se de uma plataforma global de *Cloud Computing* amplamente consolidada, a validação da AWS fundamenta-se no Modelo de Responsabilidade Compartilhada e na revisão contínua das certificações oficiais emitidas por auditores independentes via portal *AWS Artifact* (Relatórios SOC 2 Type II e certificações ISO 27001).

3.2. Validação e Gestão de Riscos do Parceiro de Suporte (Nuvme)

A atuação da Nuvme como parceira de suporte de infraestrutura é validada e monitorada através da seguinte estratégia baseada em riscos:

- Credenciamento e Parceria AWS: Validação das certificações técnicas da equipe e do status oficial de *AWS Partner Network (APN)*;
- Controle e Isolamento de Acessos: A Nuvme não possui acesso direto irrevogável ou permanente. Os acessos aos ambientes da AWS ocorrem obrigatoriamente por meio de funções IAM com MFA ativado e registros detalhados via AWS CloudTrail;
- Auditoria e Rastreabilidade: Toda alteração promovida na infraestrutura pela equipe de suporte fica registrada de forma imutável nos logs de auditoria do ambiente;
- Acordo de Nível de Serviço (SLA): Abertura de chamados e atendimento regidos por prazos de resposta vinculados aos níveis de severidade do incidente.

3.3. Validação e Gestão de Riscos de Desenvolvedores Terceirizados

A contratação e atuação dos desenvolvedores terceirizados são validadas e controladas sob rígidos critérios de governança de código e gestão de acessos:

- Validação Contratual e Jurídica: Formalização de contratos de prestação de serviços com cláusulas expressas de confidencialidade (NDA), propriedade intelectual e adequação à LGPD;
- Segregação de Ambientes e Proteção de Dados: Os desenvolvedores terceirizados atuam em ambientes de desenvolvimento/homologação;
- Controle de Versão e Aprovação de Código (Code Review): Os terceiros trabalham através de *Pull Requests* no GitHub. Nenhum código de terceiros é implantado diretamente em

produção;

- Gestão de Credenciais e Rastreabilidade: Contas individuais no GitHub com exigência de Autenticação Multi-Fator (MFA). Revogação imediata dos acessos ao término do contrato/alocação.

Certificações e relatórios independentes

Código do Documento: DEC-CRT-022	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Governança de TI, Segurança & DevOps	Aplica-se a: Todos os Serviços e Infraestrutura em Nuvem

1. OBJETIVO

Esta declaração formal visa esclarecer o escopo de certificações e relatórios de auditoria independente aplicáveis ao serviço, garantindo o atendimento técnico.

2. ENQUADRAMENTO DA CONFORMIDADE (PARCIAL)

O enquadramento da conformidade do serviço é classificado formalmente como PARCIAL, fundamentado no Modelo de Responsabilidade Compartilhada em Nuvem (AWS Shared Responsibility Model). Esse modelo delimita com clareza as responsabilidades entre o provedor de infraestrutura de nuvem e a organização prestadora do serviço.

Camada / Âmbito	**Entidade Responsável**	**Status de Certificação / Auditoria**	**Descrição do Escopo do Atendimento**
Segurança DA Nuvem (Infraestrutura, Data Centers, Hardware e Hipervisores)	Amazon Web Services (AWS)	Totalmente Certificado	Cobertura integral por auditorias independentes mundiais e relatórios atestando a segurança física e lógica da infraestrutura base.
Segurança NA Nuvem (Aplicação, Código-Fonte, Regras de Negócio e Gestão de Dados)	Organização (Desenvolvimento e Operação)	Controles Internos Aplicados	Segurança assegurada por meio de políticas e controles internos de governança (DevSecOps, testes automatizados, auditoria de código e gestão de acessos).

3. CERTIFICAÇÕES VIGENTES DA INFRAESTRUTURA (AWS)

A infraestrutura de nuvem subjacente onde os serviços são hospedados e processados (AWS) possui as seguintes certificações e relatórios de conformidade independentes em vigor:

- ISO/IEC 27001:2013 / 27001:2022: Sistema de Gestão de Segurança da Informação (SGSI);
- ISO/IEC 27017:2015: Código de Prática para Controles de Segurança da Informação para Serviços em Nuvem;
- ISO/IEC 27018:2019: Código de Prática para Proteção de Dados Pessoais Identificáveis (PII) em Nuvens Públicas;
- SOC 1, SOC 2 (Type II) e SOC 3: Relatórios de auditoria independente cobrindo os critérios de Segurança, Disponibilidade, Integridade de Processamento, Confidencialidade e Privacidade;
- PCI-DSS Level 1: Padrão de Segurança de Dados do Setor de Cartões de Pagamento (camada de infraestrutura).

Nota: Cópias formais e vigentes dos certificados e relatórios SOC podem ser fornecidas ou validadas diretamente por meio do portal oficial AWS Artifact.

4. CONTROLES DE SEGURANÇA DA CAMADA DE APLICAÇÃO

Para garantir que a camada sob responsabilidade da organização permaneça alinhada às exigências da ISO 27001 e às boas práticas do mercado, adotam-se os seguintes controles de segurança complementares:

- Gestão de Alterações e Código: Versionamento em repositórios privados no GitHub com ramificações segregadas, aprovação por pares (Peer Review) e esteiras automatizadas de integração e entrega (CI/CD);
- Controle de Acessos e Identidade: Uso obrigatório de Autenticação Multi-Fator (MFA) e políticas do menor privilégio para todos os acessos administrativos;
- Continuidade e Recuperação: Plano formal de Recuperação de Desastres (DRP) com rotinas diárias de backup criptografado em repouso e em trânsito.