

DOCUMENTO OFICIAL

Política de Segurança

Prestador de Serviço de Confiança da ICP-Brasil

BRENO MESQUITA R. DE SOUZA LTDA (UNIFOKAL)

CNPJ 46.157.128/0001-64

Versão 1.0

Aprovada em 22 de outubro de 2026

Vigente desde 22 de outubro de 2026

Versão publicada: <https://unifokal.com/legal/politica-de-seguranca>

Arquivo: <https://unifokal.com/legal/politica-de-seguranca.pdf>

Política de Segurança

UNIFOKAL | BRENO MESQUITA R. DE SOUZA LTDA | CNPJ 46.157.128/0001-64

1. Identificação

Item	Informação
Documento	Política de Segurança (PS) da UNIFOKAL
Razão social	BRENO MESQUITA R. DE SOUZA LTDA
Nome de fantasia	UNIFOKAL
CNPJ	46.157.128/0001-64
Sede	Joaquim Aristóteles de Oliveira, 100, Letícia, Belo Horizonte/MG, CEP 31570-090
Versão	1.0
Data de aprovação	22/10/2026
Início da vigência	22/10/2026
Aprovada por	Administração da sociedade (sócio administrador)
Responsável pela política	Gerência de Segurança da Informação da UNIFOKAL
Contato	privacidade@unifokal.com

Esta Política de Segurança é o documento formal da BRENO MESQUITA R. DE SOUZA LTDA (UNIFOKAL) para a atuação como Prestador de Serviço de Confiança (PSC) da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Ela é publicada nesta página, de acesso público e sem login, conforme exige o DOC-ICP-03 v7.2, item 2.2.7.1.1, alínea d.

2. Objetivos

Em consonância com o item 2 do DOC-ICP-02 v4.0, esta Política tem por objetivos:

1. definir o escopo da segurança da UNIFOKAL na prestação dos serviços de PSC;

2. orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir a integridade, o sigilo e a disponibilidade das informações, dos sistemas de informação e dos recursos;
3. permitir a adoção de soluções de segurança integradas;
4. servir de referência para auditoria, fiscalização, apuração e avaliação de responsabilidades.

3. Abrangência

Esta Política se aplica aos serviços de confiança que a UNIFOKAL presta, ou venha a prestar, como PSC credenciado na ICP-Brasil, nos termos do DOC-ICP-17.01 v3.0:

- serviço de armazenamento de chaves privadas de usuários finais;
- serviço de assinatura digital;
- serviço de verificação de assinatura digital.

Os serviços de PSC somente são prestados depois do deferimento do credenciamento e da publicação do ato no Diário Oficial da União (DOC-ICP-03 v7.2, item 2.2.7.3), e apenas nas modalidades credenciadas.

A Política alcança todos os recursos humanos, administrativos e tecnológicos ligados a esses serviços, em caráter permanente ou temporário (DOC-ICP-02 v4.0, item 6.1.1), e compreende:

- as pessoas: sócios, empregados, prestadores de serviço e quaisquer terceiros que tenham acesso a informações, instalações ou sistemas do PSC;
- os ativos de informação: chaves e certificados de usuários finais, dados de autenticação, registros de eventos, trilhas de auditoria, imagens, documentação e contratos;
- os ativos de processamento: hardware criptográfico (HSM), servidores, equipamentos de rede, estações de trabalho, sistemas e aplicações;
- os ambientes: as instalações físicas de operação e de contingência, a rede interna e as interfaces de serviço expostas a aplicações e titulares.

Os requisitos de segurança abrangem os quatro aspectos do DOC-ICP-02 v4.0, item 3: segurança humana, segurança física, segurança lógica e segurança dos recursos criptográficos.

4. Referências normativas

Esta Política foi elaborada sobre as versões vigentes dos documentos abaixo, publicadas pelo Instituto Nacional de Tecnologia da Informação (ITI). Em caso de alteração normativa, prevalece a redação vigente publicada pelo ITI, e esta Política é revista conforme a seção 22.

Documento	Título	Ato de aprovação
DOC-ICP-02 v4.0	Política de Segurança da ICP-Brasil	Resolução CG ICP-Brasil nº 193, de 16 de novembro de 2021
DOC-ICP-03 v7.2	Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil	Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020, com as alterações até a Resolução CG ICP-Brasil nº 216, de 19 de março de 2025
DOC-ICP-17 v2.0	Requisitos Mínimos para as Declarações de Práticas dos Prestadores de Serviço de Confiança da ICP-Brasil	Resolução CG ICP-Brasil nº 180, de 20 de outubro de 2020, com as alterações da Resolução CG ICP-Brasil nº 216, de 19 de março de 2025
DOC-ICP-17.01 v3.0	Procedimentos Operacionais Mínimos para os Prestadores de Serviço de Confiança da ICP-Brasil	Instrução Normativa ITI nº 20, de 23 de novembro de 2020

Aplicam-se ainda, nos termos do DOC-ICP-17.01 v3.0, os documentos DOC-ICP-01.01 (padrões e algoritmos criptográficos), DOC-ICP-08 (auditorias), DOC-ICP-09 (fiscalização), DOC-ICP-10 (homologação de sistemas e equipamentos), DOC-ICP-11 (carimbo do tempo) e o conjunto DOC-ICP-15 (assinaturas digitais e políticas de assinatura), além da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, e da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD).

5. Terminologia e definições

Todas as regras e diretrizes desta Política são obrigatórias e cogentes (DOC-ICP-02 v4.0, item 4). Aplicam-se as definições do item 5.1 do DOC-ICP-02 v4.0, entre elas:

- **Ativo de informação:** o patrimônio composto por todos os dados e informações gerados e manipulados na execução dos sistemas e processos do PSC.
- **Ativo de processamento:** o patrimônio composto por todos os elementos de hardware e software necessários à execução dos sistemas e processos do PSC.
- **Controle de acesso:** as restrições ao acesso às informações de um sistema, exercidas pela Gerência de Segurança da Informação.
- **Custódia:** a responsabilidade de guardar um ativo para terceiros, que não concede, por si, acesso ao ativo nem o direito de conceder acesso a outros.
- **Direito de acesso:** o privilégio associado a um cargo, pessoa ou processo para acessar um ativo.

- Incidente de segurança: qualquer evento que comprometa, ou ameace, a integridade, a autenticidade ou a disponibilidade de qualquer ativo do PSC.
- Senha fraca ou óbvia: a de fácil associação com o titular, simples ou curta, como datas, nomes, sequências numéricas simples e palavras de dicionário.

6. Papéis e responsabilidades

A segurança do PSC é exercida pelos papéis abaixo, com responsáveis formalmente designados.

- Administração da sociedade: aprova esta Política e suas revisões, designa formalmente a Gerência de Segurança da Informação e as pessoas que operam chaves criptográficas, participa do gerenciamento de riscos (DOC-ICP-02 v4.0, item 12.4.1.2) e assegura os recursos necessários ao seu cumprimento.
- Gerência de Segurança da Informação: estabelece e executa as regras de proteção dos ativos e as revisa pelo menos anualmente; decide as medidas em caso de violação; restringe e controla o acesso de usuários remotos e externos; elabora e mantém atualizado o Plano de Continuidade do Negócio; detecta, registra e comunica à AC Raiz as violações e tentativas de acesso não autorizado; define restrições de acesso por usuário; mantém os registros de atividade por no mínimo 7 (sete) anos; limita as contas de prestadores de serviço ao período do contrato; exclui contas inativas; e só concede senhas de contas privilegiadas a quem efetivamente precisa delas, com registro e controle (DOC-ICP-02 v4.0, item 7.4.4).
- Chefias: gerenciam o cumprimento da Política pelas pessoas sob sua supervisão, identificam desvios e adotam correções, comunicam formalmente à unidade que concede privilégios quem pode acessar informações e quem foi desligado, transferido, afastado ou está respondendo a processo, para habilitação ou inabilitação imediata (DOC-ICP-02 v4.0, item 7.4.2).
- Empregados e prestadores de serviço: preservam a integridade e o sigilo das informações, cumprem esta Política, usam os sistemas somente para os fins autorizados, mantêm o sigilo da própria senha, não compartilham informação confidencial com quem não tem autorização, respondem por todo acesso feito com a sua identificação, respeitam a legislação de propriedade intelectual e comunicam ao superior imediato qualquer irregularidade (DOC-ICP-02 v4.0, item 7.4.1).
- Responsáveis por ativos: cada área que detém ativos de informação ou de processamento responde pela sua proteção, conforme a classificação da informação, e todo ativo tem responsável definido (DOC-ICP-02 v4.0, item 7.4.3).

7. Regras gerais de gestão da segurança

- Esta Política é comunicada a todo o pessoal envolvido e amplamente divulgada, para que todos a conheçam e a pratiquem (DOC-ICP-02 v4.0, item 6.1.2). Um exemplar impresso fica disponível para consulta no nível 1 de segurança física do PSC (DOC-ICP-17.01 v3.0, item 1.5).
- A Política é seguida por todo o pessoal envolvido nas atividades do PSC, do quadro próprio ou contratado (DOC-ICP-17.01 v3.0, item 1.6).
- Um programa de conscientização em segurança da informação informa todo o pessoal sobre os riscos a que estão expostos os sistemas e operações, com treinamento específico sobre ataques de engenharia social para quem se relaciona com usuários (DOC-ICP-02 v4.0, item 6.1.4).
- Procedimentos documentados garantem que, na transferência, remanejamento, promoção ou desligamento de qualquer pessoa, os privilégios de acesso sejam revistos, modificados ou revogados (DOC-ICP-02 v4.0, item 6.1.5).
- Existe mecanismo e repositório centralizado para trilhas, registros de eventos e notificações de incidentes, usado pela equipe de resposta a incidentes para defesa ativa e corretiva (DOC-ICP-02 v4.0, item 6.1.6).
- As aquisições de bens e serviços, em especial de tecnologia da informação, observam esta Política (DOC-ICP-02 v4.0, item 6.1.7).
- Em segurança da informação, é proibido tudo o que não estiver previamente autorizado pela Gerência de Segurança da Informação (DOC-ICP-02 v4.0, item 6.1.8).
- Normas e procedimentos internos detalham estas diretrizes, considerando as particularidades do PSC (DOC-ICP-02 v4.0, item 1.1; DOC-ICP-17.01 v3.0, item 1.4).

8. Classificação da informação

Toda informação gerada e custodiada pelo PSC é classificada segundo o seu teor crítico e grau de confidencialidade, independentemente da mídia em que esteja armazenada ou do meio por que trafegue (DOC-ICP-17.01 v3.0, itens 8.1 e 8.2; DOC-ICP-02 v4.0, item 9.2.1). O meio de registro recebe a mesma classificação do ativo que contém.

Classe	O que abrange
Público	Informação que pode vir a público sem consequência danosa ao funcionamento do PSC, como esta Política.
Pessoal	Informação relacionada a pessoa natural, como dados pessoais de titulares, empregados e prestadores.
Interna	Informação de uso estritamente interno cuja divulgação não autorizada poderia causar impacto à imagem do PSC, como código-fonte, cronogramas e atas.
Confidencial	Informação crítica para o sigilo e a integridade das atividades do PSC, como chaves, dados de autenticação, configurações de segurança, trilhas de auditoria e relatórios de auditoria.

O tratamento de cada classe (rotulagem, armazenamento, transmissão, cópia, impressão e descarte) é definido em norma interna de classificação. Informação Confidencial ou Pessoal nunca é enviada a outra rede sem proteção criptográfica adequada (DOC-ICP-02 v4.0, item 9.3.3.17).

9. Inventário de ativos

- Todos os ativos do PSC são inventariados, classificados, mantidos permanentemente atualizados e têm gestor responsável formalmente designado (DOC-ICP-02 v4.0, item 6.3).
- O inventário dos ativos de processamento é atualizado, no mínimo, mensalmente (DOC-ICP-02 v4.0, item 8.2.12).
- Computadores, servidores, dispositivos de rede e os respectivos softwares são inventariados com informações que permitam a identificação inequívoca (DOC-ICP-17.01 v3.0, item 3.1.1.4, alínea h).
- Todos os ativos de processamento constam do Plano de Continuidade do Negócio (DOC-ICP-02 v4.0, item 7.4.3.1, alínea c).

10. Gerenciamento de riscos

O PSC mantém processo de gerenciamento de riscos, atualizado no mínimo anualmente, para prevenção contra riscos, inclusive os advindos de novas tecnologias, com planos de ação para proteger os componentes ameaçados (DOC-ICP-02 v4.0, item 6.2; DOC-ICP-17.01 v3.0, item 10). O processo cobre as fases do item 12.2 do DOC-ICP-02 v4.0:

1. identificação dos recursos a proteger: hardware, rede, software, dados, informações pessoais, documentação e suprimentos;
2. identificação das ameaças naturais, humanas ou de outra natureza;

3. análise das vulnerabilidades e dos impactos associados;
4. avaliação da probabilidade de ocorrência e do prejuízo provável;
5. tratamento: eliminar, prevenir, limitar, transferir ou aceitar o risco;
6. monitoração da eficácia dos controles adotados;
7. reavaliação periódica, em intervalo não superior a um ano.

A análise considera, entre outros, os riscos sobre dados e informação, pessoas, rede, hardware, software e sistemas, e recursos criptográficos listados no item 12.3 do DOC-ICP-02 v4.0. Os riscos que não puderem ser eliminados têm seus controles documentados e são levados ao conhecimento da AC Raiz (DOC-ICP-02 v4.0, item 12.4.1).

II. Segurança de pessoal

O PSC mantém Política de Gestão de Pessoas que dispõe sobre contratação, desligamento, descrição de cargos, avaliação de desempenho e capacitação (DOC-ICP-17.01 v3.0, item 2.1). Valem as diretrizes abaixo.

- Admissão com critérios rígidos, para selecionar pessoas reconhecidamente idôneas e sem antecedentes que comprometam a segurança ou a credibilidade do PSC, com pesquisa de histórico, verificação de antecedentes e de grau de instrução e entrevista por profissional qualificado (DOC-ICP-02 v4.0, itens 7.3.1, 7.3.3 e 7.3.4).
- Atribuições de cada função descritas, incluindo necessidade de acesso a informação sensível, grau de sensibilidade do setor e qualificação técnica exigida (DOC-ICP-02 v4.0, item 7.3.2). A comprovação da capacidade técnica do pessoal fica à disposição de auditorias e fiscalizações (DOC-ICP-17.01 v3.0, item 2.2).
- Não são admitidos estagiários nas atividades fim do PSC (DOC-ICP-17.01 v3.0, item 2.8).
- Todo o pessoal, próprio ou contratado, assina termo de sigilo com garantias jurídicas, válido mesmo após o desligamento ou o fim do contrato, com cláusula explícita de responsabilização em caso de quebra das regras da ICP-Brasil. O mesmo termo se aplica a qualquer entidade que tenha acesso a informações internas ou de terceiros (DOC-ICP-17.01 v3.0, itens 2.3 a 2.5).
- Cada pessoa tem dossiê com contrato ou comprovante de vínculo, verificação de antecedentes criminais, de situação de crédito e de histórico de empregos anteriores, comprovação de residência e de capacidade técnica, resultado da entrevista inicial assinado pelo entrevistador, declaração de conhecimento das atribuições e das regras da ICP-Brasil e o termo de sigilo (DOC-ICP-17.01 v3.0, item 2.7).

- O acesso a informação sensível depende de credencial de segurança concedida por autoridade competente, fundada na necessidade de conhecer, com validade máxima de 1 (um) ano, prorrogável por igual período enquanto houver necessidade do serviço (DOC-ICP-02 v4.0, item 7.3.6).
- Treinamento sobre esta Política e sobre as normas de tratamento de informação sigilosa é aplicado a empregados e prestadores de serviço (DOC-ICP-02 v4.0, item 7.3.7).
- O desempenho é acompanhado e avaliado periodicamente, com registro dos comportamentos relevantes e averiguação dos que possam comprometer a segurança (DOC-ICP-02 v4.0, itens 7.3.5 e 7.3.8).
- No desligamento, credenciais, crachás e acessos físicos e lógicos são revogados; o acesso do ex-empregado fica restrito às áreas públicas; ele declara não ter pendências; e a entrevista de desligamento o orienta sobre o dever de sigilo. O dossiê passa a conter as evidências de exclusão dos acessos e a declaração de ausência de pendências (DOC-ICP-02 v4.0, itens 7.3.9 a 7.3.11; DOC-ICP-17.01 v3.0, item 2.9).
- O PSC mantém procedimentos formais de apuração e responsabilização em caso de descumprimento das suas políticas ou das normas da ICP-Brasil (DOC-ICP-17.01 v3.0, item 2.6).

12. Segurança física

As responsabilidades pela segurança física são atribuídas a pessoas claramente identificadas (DOC-ICP-02 v4.0, item 8.2.1). O ambiente físico do PSC observa os níveis de acesso do DOC-ICP-17.01 v3.0, item 3.1.1:

Nível	Exigência
Nível 1	Após a primeira barreira de acesso; interface com clientes e fornecedores que precisem comparecer ao PSC.
Nível 2	Interno ao nível 1, com identificação individual por meio eletrônico e crachá; nível mínimo para qualquer processo operacional ou administrativo; acesso restrito a quem trabalha diretamente nos serviços do PSC ou na manutenção dos seus sistemas; equipamentos de gravação, fotografia, vídeo, som e computadores portáteis só com autorização formal e supervisão.
Nível 3	Interno ao nível 2, onde ocorre toda atividade de armazenamento de chaves e de assinatura e verificação; paredes de alvenaria ou equivalente, sem aberturas para o exterior além da porta única; entrada com dois mecanismos de controle (identificação individual e biometria ou senha); controle de entrada e de saída de cada pessoa.
Nível 3.1	Para o serviço de assinatura digital: gabinete reforçado de aço ou equivalente, trancado a chave, que abriga todo o hardware e software do serviço.
Nível 4	Para o serviço de armazenamento de chaves privadas: sala-cofre interna ao nível 3, construída segundo as normas brasileiras aplicáveis, com proteção contra acesso indevido, água, vapor, gases, fogo e interferência eletromagnética; cada acesso exige a identificação de no mínimo 2 (duas) pessoas autorizadas, que permanecem enquanto o ambiente estiver ocupado.

Além dos níveis, o ambiente físico atende às exigências do DOC-ICP-17.01 v3.0, item 3.1.1.4, e do DOC-ICP-02 v4.0, item 8.2:

- dispositivos que autenticam e registram o acesso de pessoas com data e hora, e imagens que permitem identificar quem acessa qualquer parte do ambiente, com data e hora sincronizadas entre os mecanismos de controle de acesso e de imagem;
- monitoramento em tempo real dos ambientes de processos críticos por circuito fechado de televisão, com gravação, e sistemas de detecção de intrusão testados regularmente, com alarme sempre ativo nas áreas não ocupadas;
- crachá de identificação visível para todos, inclusive visitantes, que são supervisionados e têm entrada, saída e destino registrados;
- lista atualizada de quem possui cartões ou chaves de acesso, com controle duplicado, e comunicação imediata de perda à Gerência de Segurança da Informação;
- trânsito de material de terceiros somente mediante registro de onde passou, quando e sob a responsabilidade de quem;
- prevenção e controle de incêndio, temperatura, umidade, iluminação e oscilação de corrente elétrica, e continuidade de energia nas áreas críticas até que todos os processos e dados estejam assegurados;

- destruição segura de material crítico inservível e apagamento irreversível dos dados de equipamento enviado para manutenção, antes de sair do ambiente;
- livro de registro de acesso físico quando os sistemas automáticos estiverem inoperantes;
- no serviço de armazenamento de chaves privadas, no mínimo dois ambientes físicos, um de operação e outro de contingência;
- acesso a painéis de energia, comunicações e cabeamento restrito ao pessoal autorizado;
- equipamentos e ambiente computacional com data e hora sincronizadas com a Entidade de Auditoria do Tempo (EAT) da ICP-Brasil.

13. Segurança lógica

A informação é protegida de acordo com o seu valor, sensibilidade e criticidade, contra ameaças e ações não autorizadas, acidentais ou não (DOC-ICP-02 v4.0, itens 9.2.1 e 9.2.2). Valem as regras abaixo (DOC-ICP-02 v4.0, item 9.3; DOC-ICP-17.01 v3.0, item 4).

- Acesso lógico ao ambiente computacional do PSC somente por usuário individual e senha, trocada periodicamente, e apenas por pessoas autorizadas.
- Política explícita de cadastro, suspensão e remoção de usuários, com perfis de acesso de privilégio mínimo e acesso motivado pela função.
- Usuários especiais (root e administrador de sistemas operacionais, do hardware criptográfico, do banco de dados e das aplicações) com senhas segregadas, de modo que o acesso exija no mínimo duas pessoas autorizadas.
- Nenhum usuário obtém os direitos de acesso de outro; a informação de direitos de acesso é protegida contra alteração não autorizada; o arquivo de senhas é cifrado e de acesso controlado.
- Senhas individuais, secretas e intransferíveis, com conjunto de caracteres, tamanho mínimo e máximo, prazo de validade e forma de troca definidos em norma; o sistema impede senhas fracas ou óbvias, exige a troca da senha inicial no primeiro acesso, não exibe a senha digitada e só troca senha bloqueada após identificação positiva do usuário.
- Bloqueio de usuário por inatividade e por tentativas sucessivas malsucedidas; bloqueio de sessão inativa com nova autenticação; aviso, na tela inicial, de que o serviço é de uso exclusivo de usuários autorizados, e informação do último acesso no momento da conexão.
- Usuários e administradores do controle de acesso conscientizados de suas responsabilidades mediante termo de compromisso.
- É vedado qualquer acesso remoto dos operadores do PSC ao ambiente de nível 3.

- Sistemas avaliados quanto à segurança, com testes de vulnerabilidade, antes de entrar em produção, e vulnerabilidades do ambiente avaliadas periodicamente, com adoção das recomendações.
- Sistemas operacionais, antivírus, aplicativos de segurança e demais softwares básicos mantidos atualizados conforme as recomendações dos fabricantes; somente software autorizado e licenciado é instalado, com controle de distribuição e instalação.
- Combate sistematizado a código malicioso em servidores, estações de trabalho e equipamentos portáteis.
- Integridade dos arquivos de configuração do sistema operacional e de outros arquivos críticos monitorada; configuração de todo ativo verificada na instalação inicial, para corrigir as vulnerabilidades da configuração padrão.
- Proteção adicional, inclusive criptografia, quando necessária para evitar acesso não autorizado; estações que executam operações sensíveis com proteção lógica e física adicional.
- Mídias eliminadas de forma segura, por procedimento formal, quando não forem mais necessárias; impressão de documento sigiloso sob supervisão do responsável.
- Documentação dos sistemas mantida atualizada e necessidades de segurança identificadas em cada etapa do ciclo de vida.

14. Segurança de rede

- O tráfego de informações na rede é protegido contra danos, perdas, acesso, uso ou exposição indevidos (DOC-ICP-17.01 v3.0, item 5.1; DOC-ICP-02 v4.0, item 9.3.3.1).
- Não são admitidos acessos externos à rede interna do PSC. As tentativas são inibidas e monitoradas por barreiras e filtros de acesso (firewall) e por mecanismos de detecção de intrusão (DOC-ICP-17.01 v3.0, item 5.2; DOC-ICP-02 v4.0, itens 9.3.3.19 e 9.3.3.30).
- Testes de segurança na rede interna e externa, com aplicativos especializados, no mínimo uma vez por mês, documentados, com correção das vulnerabilidades detectadas (DOC-ICP-17.01 v3.0, item 5.3).
- Servidores, roteadores, switches e firewalls operam em ambiente de segurança no mínimo equivalente ao nível 3.1 (assinatura digital) ou ao nível 4 (armazenamento de chaves privadas), com acesso lógico restrito por autenticação e autorização (DOC-ICP-17.01 v3.0, item 3.1.1.3).
- Ambientes de rede críticos isolados dos demais; conexões com redes externas restritas às necessárias aos processos; todo serviço de rede não explicitamente autorizado é bloqueado ou desabilitado (DOC-ICP-02 v4.0, itens 9.3.3.18, 9.3.3.24 e 9.3.3.25).
- Conexões com outros ambientes e alterações de topologia e configuração são autorizadas pela administração da rede e pela Gerência de Segurança da Informação e documentadas; diagrama topológico, configuração e inventário mantidos atualizados (DOC-ICP-02 v4.0, item 9.3.3.9).

- A comunicação entre sistemas do PSC, e entre redes de uma mesma organização por rede pública, usa mecanismos criptográficos que asseguram sigilo e integridade, como redes privadas virtuais (DOC-ICP-02 v4.0, itens 9.3.3.29 e 10.3.2).
- O tráfego é monitorado para verificar a normalidade e detectar situações anômalas; testes ou monitoração sobre a rede só com autorização formal e supervisão (DOC-ICP-02 v4.0, itens 9.3.3.8 e 9.3.3.15).

15. Recursos criptográficos e gestão de chaves

Os recursos criptográficos observam o item 10 do DOC-ICP-02 v4.0 e o item 6 do DOC-ICP-17.01 v3.0.

- As chaves privadas dos usuários finais, para os tipos de certificado que exigem geração e armazenamento em hardware criptográfico, ficam dentro da fronteira criptográfica e de segurança física de HSM com certificação Inmetro válida no âmbito da ICP-Brasil, endereçadas por conta de usuário (DOC-ICP-17.01 v3.0, item 6.1.1).
- O uso e a exportação da chave privada são de conhecimento e controle exclusivos do titular, sem possibilidade de acesso por outros titulares, por empregados do PSC ou por quem dependa de outras chaves (DOC-ICP-17.01 v3.0, item 6.1.2).
- O acesso do titular à chave privada exige duplo fator de autenticação, de classes diferentes (conhecimento, posse ou biometria), com proteção criptográfica da transmissão e dos dados de autenticação, nos mecanismos admitidos pelo DOC-ICP-17.01 v3.0, item 6.1.3.
- As chaves dos usuários finais são copiadas para o ambiente físico de contingência, com os mesmos requisitos de armazenamento do ambiente principal, e a entrada em operação da contingência ocorre em até 48 (quarenta e oito) horas (DOC-ICP-17.01 v3.0, item 6.1.4).
- Os processos com chaves criptográficas são executados pelo número mínimo e essencial de pessoas, formalmente designadas, com funções, privilégios e responsabilidades explicitamente definidos (DOC-ICP-02 v4.0, itens 10.2.1 e 10.2.2).
- Algoritmos e tamanhos de chave seguem o DOC-ICP-01.01; equipamentos de criação de assinatura têm certificação Inmetro válida no âmbito da ICP-Brasil, conforme o DOC-ICP-10 (DOC-ICP-17.01 v3.0, itens 7.3.3 e 7.5.1).
- Todo parâmetro crítico cuja exposição comprometa a segurança do sistema criptográfico é armazenado cifrado (DOC-ICP-02 v4.0, item 10.1.4); chaves sob custódia de responsável são fisicamente protegidas contra acesso, uso ou duplicação não autorizados (DOC-ICP-02 v4.0, item 8.2.5).
- O transporte de chaves e de parâmetros criptográficos tem integridade e sigilo assegurados por soluções criptográficas específicas (DOC-ICP-02 v4.0, item 10.3.1).

- As interfaces de serviço usam TLS e o framework OAuth 2.0 (RFC 6749 e RFC 7636); as aplicações não coletam fatores de autenticação do titular, que trafegam diretamente entre o PSC e o equipamento previamente cadastrado do titular, nos termos do DOC-ICP-17.01 v3.0, item 6.4.

16. Serviços de assinatura e de verificação de assinatura

- Antes de assinar, o sistema verifica a validade do certificado, e confere a assinatura devolvida com a chave pública (DOC-ICP-17.01 v3.0, item 7.2.3).
- A criação de assinatura só é requerida com a autenticação do titular, que tem controle exclusivo da chave privada, por mais de um mecanismo de autenticação resistente a ataques de representação, com toda a troca entre aplicação e dispositivo cifrada (DOC-ICP-17.01 v3.0, item 7.4).
- As assinaturas seguem as políticas de assinatura padronizadas e aprovadas na ICP-Brasil, nos formatos CAdES, XAdES e PAdES definidos no conjunto DOC-ICP-15, com carimbo do tempo de Autoridade de Carimbo do Tempo credenciada quando a política o exigir (DOC-ICP-17.01 v3.0, itens 7.6 e 7.7).
- A validação é feita contra a mesma política de assinatura usada na criação, com conferência da Lista de Políticas de Assinatura Aprovadas (LPA) da AC Raiz, e gera relatório com a situação Válida, Inválida ou Indeterminada e o detalhe de cada restrição (DOC-ICP-17.01 v3.0, item 7.8).
- O acordo de nível de serviço de todos os serviços credenciados é de no mínimo 99,99% (DOC-ICP-17.01 v3.0, item 7.9.1).

17. Registros de eventos, auditoria e fiscalização

- Todo equipamento do PSC mantém registro de eventos ativo, com horário sincronizado com fonte confiável do tempo da ICP-Brasil (DOC-ICP-17.01 v3.0, item 4.6; DOC-ICP-02 v4.0, item 9.3.2.4).
- Os registros contêm data e hora, identificação do usuário, comandos executados e seus argumentos, estação de origem da conexão, processos e condições de erro, como tentativas rejeitadas (DOC-ICP-02 v4.0, item 7.4.4.1, alínea i).
- Registros de eventos, trilhas de auditoria do armazenamento de chaves e do serviço de assinatura, registros de acesso físico e lógico e imagens têm cópia de segurança guardada por 7 (sete) anos (DOC-ICP-17.01 v3.0, item 4.7).
- Todos os registros (logs, trilhas e imagens) são analisados no mínimo mensalmente, com relatório assinado pelo responsável pelo PSC (DOC-ICP-17.01 v3.0, item 12).

- Os registros são protegidos e armazenados de acordo com a sua classificação, e as violações de segurança registradas são analisadas para fins corretivos, legais e de auditoria (DOC-ICP-02 v4.0, itens 9.2.3 e 9.3.1.3).
- O PSC se submete às auditorias pré-operacional e operacionais e à fiscalização da AC Raiz, a qualquer tempo e sem aviso prévio, nos termos do DOC-ICP-08 e do DOC-ICP-09 (DOC-ICP-02 v4.0, item 11).

18. Gestão de incidentes de segurança

O PSC mantém Plano de Resposta a Incidentes, que estabelece:

1. Identificação: monitoramento dos registros de eventos, do tráfego de rede, dos sistemas de detecção de intrusão e dos controles físicos, e canal para que qualquer pessoa comunique suspeita de incidente.
2. Registro: todo incidente é registrado no repositório centralizado, com data e hora, ativos envolvidos, evidências e responsável pelo tratamento.
3. Comunicação à AC Raiz: todo incidente é reportado à AC Raiz imediatamente, a partir da verificação da ocorrência, de modo sigiloso, às pessoas especialmente designadas para isso (DOC-ICP-02 v4.0, item 6.4.4).
4. Contenção e resposta: isolamento dos ativos afetados, interrupção ou suspensão de serviços quando necessário e preservação das trilhas de auditoria para investigação (DOC-ICP-02 v4.0, item 13.2.2.1).
5. Investigação: análise das trilhas de auditoria e das evidências para determinar causa, alcance e responsabilidade.
6. Tratamento e recuperação: correção da causa, restauração segura do serviço e, quando houver comprometimento de chave, as medidas de revogação e de comunicação previstas nas normas da ICP-Brasil.
7. Comunicação a titulares e autoridades: quando o incidente envolver dados pessoais e puder acarretar risco ou dano relevante aos titulares, comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, nos termos do art. 48 da LGPD e da regulamentação da ANPD.
8. Lições aprendidas: revisão dos controles e do gerenciamento de riscos após o encerramento do incidente.

Comunicações de incidente ou de vulnerabilidade podem ser enviadas a privacidade@unifokal.com.

19. Continuidade do negócio e salvaguarda de ativos

O PSC mantém Plano de Continuidade do Negócio (PCN), implementado e testado pelo menos uma vez por ano, para manter os serviços críticos em caso de inoperância total ou parcial do ambiente (DOC-ICP-02 v4.0, item 6.4.1; DOC-ICP-17.01 v3.0, item 11), e Plano de Recuperação de Desastres. Os planos tratam, no mínimo, dos elementos do item 13.2.2 do DOC-ICP-02 v4.0: condições de ativação, procedimentos de emergência, de fallback e de restauração, responsabilidades individuais, objetivo de tempo de recuperação (RTO), testes regulares, guarda de material criptográfico crítico em local alternativo, frequência das cópias de segurança e distância entre a instalação de recuperação e o local principal.

Os planos consideram o comprometimento de chave privada, a invasão de sistema ou rede, incidentes de segurança física e lógica, a indisponibilidade da infraestrutura e a notificação à comunidade de usuários (DOC-ICP-02 v4.0, item 13.2.2.1). Sistemas e dispositivos redundantes garantem a continuidade dos serviços críticos (item 13.2.1), e todo o pessoal envolvido com o PCN recebe treinamento específico (item 13.2.3).

A salvaguarda de ativos de informação em formato eletrônico (backup) é definida em norma interna que descreve, conforme o DOC-ICP-17.01 v3.0, item 9.2:

- os procedimentos de backup e as indicações de uso de cada método;
- a tabela de temporalidade;
- o local e as restrições de armazenamento conforme a fase de uso;
- os tipos de mídia e os controles ambientais do armazenamento;
- os controles de segurança;
- o teste de restauração de backup.

Os procedimentos de cópia de segurança e de recuperação são documentados, mantidos atualizados e testados regularmente (DOC-ICP-02 v4.0, item 9.3.2.9). O PSC mantém ainda política de recebimento, manipulação, depósito e descarte de materiais de terceiros (DOC-ICP-17.01 v3.0, item 9.3).

20. Planejamento de capacidade operacional

O PSC elabora e atualiza anualmente o Planejamento de Capacidade Operacional (PCO), que determina os níveis de serviço requeridos pelos usuários, analisa a capacidade de processamento instalada e dimensiona a infraestrutura, o hardware, a comunicação de dados e os links de internet

para os níveis de serviço atuais e futuros, considerando crescimento, picos de uso e sazonalidade (DOC-ICP-17.01 v3.0, item 13).

21. Terceiros, fornecedores e proteção de dados pessoais

- Os contratos com prestadores de serviço contêm cláusulas de responsabilidade pelo cumprimento desta Política e das suas normas e procedimentos (DOC-ICP-02 v4.0, item 7.4.5).
- Fornecedores e prestadores com acesso a informações internas ou de terceiros assinam o termo de sigilo da seção 11 (DOC-ICP-17.01 v3.0, item 2.5), e as suas contas de acesso valem somente durante o contrato (DOC-ICP-02 v4.0, item 7.4.4.1, alínea j).
- A contratação de bens e serviços de infraestrutura considera o gerenciamento de riscos da seção 10 e os requisitos desta Política (DOC-ICP-02 v4.0, item 6.1.7).
- Hardware criptográfico, equipamentos e sistemas de certificação digital utilizados atendem à homologação exigida pelo DOC-ICP-10 e pelo DOC-ICP-17.01 v3.0.
- O tratamento de dados pessoais nos serviços do PSC observa a LGPD, com finalidade definida, minimização, segurança e registro das operações de tratamento, e com o canal do encarregado divulgado na Política de Privacidade da UNIFOKAL.

22. Sanções, revisão e aprovação

O descumprimento desta Política sujeita o responsável às sanções disciplinares, contratuais e legais cabíveis (DOC-ICP-02 v4.0, itens 7.4.1.1, alínea b, e 7.5), apuradas pelos procedimentos formais da seção 11.

Esta Política é revista pelo menos uma vez por ano e sempre que houver alteração das normas da ICP-Brasil, dos serviços credenciados, do ambiente do PSC ou do resultado do gerenciamento de riscos. Cada nova versão é aprovada formalmente pela Administração da sociedade, recebe número de versão e datas de aprovação e de vigência, e é publicada nesta mesma página, que permanece no mesmo endereço. As versões anteriores ficam registradas no histórico abaixo.

Versão	Aprovação	Vigência	Aprovada por	Descrição
1.0	22/10/2026	22/10/2026	Administração da sociedade (sócio administrador)	Primeira versão, elaborada sobre o DOC-ICP-02 v4.0 e o DOC-ICP-17.01 v3.0.