

ID	Requisitos não funcionais	Forma de atendimento				Notas
		Nativo	Parametrização	Customização	Não atende	
REQNF01	O fornecimento dos ambientes necessários para o funcionamento do sistema e seus backups deverão ser feitos em ambiente de nuvem hospedado pela própria contratada como parte da própria prestação do serviço;	X				
REQNF02	A contratada deve fornecer, no mínimo, os ambientes de produção e homologação;	X				
REQNF03	A contratada será responsável pelo dimensionamento adequado dos ambientes na plataforma escolhida para atender o nível de serviço requerido para a quantidade de usuários contratada;	X				
REQNF04	A contratada será responsável por manter, durante a vigência do contrato, os ambientes em funcionamento e fazer qualquer ajuste de dimensionamento em recursos de processamento e armazenamento que forem necessários para a boa performance da solução;	X				
REQNF05	A Solução deverá atender dentro do mês o mínimo de 96% (noventa e seis por cento) de disponibilidade;	X				99,90%
REQNF06	O tempo de resposta máximo para as operações transacionais é de 3 segundos;	X				
REQNF07	O tempo de resposta máximo para a geração de relatórios é de 5 segundos;	X				
REQNF08	O tempo de parada utilizado para manutenções planejadas não será computado para aferição de disponibilidade, desde que não ultrapasse 2% do tempo em um mês e que haja anuência da Fhemig para realização da parada do sistema. As paradas para manutenção programada deverão ocorrer, preferencialmente, em finais de semana e feriados.	X				
REQNF09	A solução deve ser altamente parametrizável, permitindo que a Fhemig faça ajustes e customizações conforme suas necessidades operacionais e estratégicas. Isso inclui a personalização de relatórios, regras de negócio, e fluxos de trabalho específicos para diferentes departamentos.	X				
REQNF10	A solução deve ser escalável para atender ao crescimento da Fhemig e a inclusão de novas funcionalidades.	X				
REQNF11	Disponibilidade de acesso ao sistema 24 horas por dia, 7 dias por semana e 365 dias por ano;	X				
REQNF12	O sistema deverá ser executado nativamente na plataforma WEB, sendo responsivo e acessível dentro ou fora da unidade assistencial, via dispositivos móveis e computadores;	X				
REQNF13	O sistema deve ser compatível com os navegadores Firefox, Chrome e Edge em suas versões mais recentes;	X				
REQNF14	O sistema deverá ter banco de dados relacional;	X				
REQNF15	Permitir acessos ao sistema de múltiplos de usuários simultaneamente;	X				
REQNF16	O acesso dos usuários se dará por login e senha;	X				
REQNF17	Disponibilizar mecanismo de envio de login e senha aleatória individual e em massa via e-mail para os servidores;	X				

REQNF18	Disponibilizar mecanismo de recuperação de senhas através de envio de link por e-mail previamente cadastrado;	X				
REQNF19	Manutenção de senha pessoal pelo próprio usuário, com proteção por mecanismo de criptografia, e confirmação da senha escolhida;	X				
REQNF20	Possibilitar e permitir, ativar ou desativar, de forma parametrizável, o uso no Sistema de pontos de controle nos quais sejam necessários comprovar que o acesso está sendo realizado por humanos. Essa comprovação deverá ser realizada através da digitação correta do conteúdo das imagens geradas por ReCaptcha ou Captcha. Após N tentativas incorretas de acertar o desafio à aplicação será bloqueada para o usuário que gerou as respostas incorretas;	X				
REQNF21	Deverá ser exigida reautenticação do usuário após determinado período de tempo parametrizável ou para a confirmação de operações que gerem alterações em dados;	X				
REQNF22	Possuir mecanismo de obrigatoriedade de troca de senha do usuário após um período determinado;	X				
REQNF23	Possibilitar o desligamento do servidor no sistema, mantendo todo o histórico de dados vinculados a ele e bloquear automaticamente o login do servidor para que ele não tenha mais acesso ao sistema;	X				
REQNF24	O sistema deverá detectar atividades não autorizadas em seus dados;	X				
REQNF25	O tempo de resposta padrão de 9 em cada 10 requisições não deve ultrapassar 5 segundos. Toda e qualquer exceção a este requisito não funcional deve ter aprovação do contratante;	X				
REQNF26	A aplicação deverá possuir mecanismos de importação e exportação de dados em massa. Estes mecanismos devem ser capazes de lidar com altos volumes de dados;	X				
REQNF27	Garantir integridade referencial;	X				
REQNF28	Garantir a total integração entre os módulos do sistema, assegurando o compartilhamento das regras de negócio e funções implantadas;	X				
REQNF29	Apresentar a seguinte documentação técnica: Manual do Usuário, com descritivo das funções do Sistema; Help On-Line; Dicionário de dados. Toda documentação deverá estar no idioma português, em mídia digital e ser atualizada conforme as atualizações do sistema;	X				
REQNF30	A documentação produzida para a contratante, em tempo de projeto, deverá estar de acordo com o Processo de Software padrão utilizado pela contratante ou em formato a ser definido por ela;	X				
REQNF31	Interoperar com outros sistemas através de serviços seguindo os padrões definidos pelos Padrões de Interoperabilidade de Governo Eletrônico – ePING, sempre que aplicável;	X				
REQNF32	Suportar, de forma nativa, os padrões abertos de conectividade: HTTPS e Web Services;	X				
REQNF33	A referência de data no sistema deverá apresentar o ano com quatro (4) dígitos;	X				

REQNF34	Os dados numéricos, alfanuméricos, texto, monetários e datas deverão ser formatados segundo o padrão brasileiro;	X				
REQNF35	Emitir sempre mensagem de erro ou aviso autoexplicativo, quando ocorrer insucesso em alguma operação;	X				
REQNF36	Em todo o sistema, manter o padrão de leiaute e operação (template) nas telas dos diversos módulos;	X				
REQNF37	Uma única transação executada pelo usuário deve desencadear as ações a ela pertinentes;	X				
REQNF38	Garantir a atomicidade, consistência, isolamento e durabilidade das informações (ACID);	X				
REQNF39	As APIs da contratada para integração devem estar documentadas;	X				
REQNF40	Permitir o acesso eletrônico às informações e documentos pelas áreas envolvidas respeitando as regras de autenticação, autorização e integridade;	X				
REQNF41	Arquitetura deverá ser distribuída em no mínimo três camadas: apresentação, lógica de negócio e persistência, onde os elementos de uma aplicação estejam nitidamente separados nestas camadas de dados;	X				
REQNF42	Sinalizar a ocorrência de transações demoradas, através de mensagem informativa ou indicação gráfica;	X				
REQNF43	O sistema deverá possibilitar a inclusão de logomarca da contratante nas interfaces do sistema e relatórios, de forma parametrizada;	X				
REQNF44	Permitir reaproveitamento das parametrizações efetuadas quando da implantação de novas versões;	X				
REQNF45	Permitir controle de acesso por níveis hierárquicos e por natureza da operação, desta forma o usuário só poderá visualizar as funções liberadas para o seu perfil;	X				
REQNF46	Possuir controle de acesso, com atribuição de privilégios por perfil para os componentes do Sistema (telas, transações, áreas de negócio) e regras de negócio, a critério da contratante;	X				
REQNF47	Permitir que servidor designado para substituição de outro possua os mesmos acessos da pessoa que está substituindo por um período determinado;	X				
REQNF48	Os mecanismos de autorização deverão permitir a definição de perfis de acesso por meio de parâmetros. Exemplo: Perfil de Administrador, RH, Chefias, servidores, Auditoria, etc;	X				
REQNF49	Somente os usuários explicitamente autorizados poderão acessar os registros de trilha de auditoria;	X				
REQNF50	Possibilitar expurgo de dados de forma automatizada, conforme definições da contratante;	X				
REQNF51	Permitir a extração de dados históricos para mídia externa;	X				
REQNF52	Permitir visualizar o histórico dos servidores ativos e inativos no sistema (mudanças de setor, mudança de escala, carga horária, mudança de chefia, etc);	X				
REQNF53	Permitir inclusão, atualização e exclusão lógica de usuários do sistema;	X				

REQNF54	A interface da solução com o usuário final deve ser adequada a adaptações e personalizações que permitam sua utilização por usuários com necessidades especiais. Essas opções devem ser compatíveis com software especializado que possa vir a ser acoplado (por exemplo, leitores de tela para deficientes visuais), bem como seguir orientações específicas de acessibilidade de interface;	X				
REQNF55	Possuir rastreabilidade de usuários por meio de controle de Logs retratando todas as ocorrências, por período, por tipo, por cadastro, por operador;	X				
REQNF56	O servidor de gerenciamento de base de dados deverá comportar o volume de dados de todos os relógios de ponto instalados e que vierem a ser instalados na FHEMIG;	X				
REQNF57	O servidor de gerenciamento de base de dados deverá comportar o volume de dados de toda as pessoas da equipe assistencial e administrativa que foram cadastradas e que vierem a ser cadastradas no sistema pela FHEMIG;	X				
REQNF58	O armazenamento dos dados é de responsabilidade da contratada e deve seguir os parâmetros e regras definidos pela LGPD;	X				
REQNF59	A contratada deve atender às políticas de segurança definidas pela contratante;	X				
REQNF60	A contratada deverá atender aos requisitos de governança de tecnologia da informação dos CONTRATANTES, o que implica em fornecer informações sobre: a. infraestrutura / arquitetura de tecnologia da informação e de segurança atualizadas, b. organização de tecnologia da informação responsável pelo serviço; e c. alterações relativas à arquitetura e procedimentos de segurança, e sua correspondente avaliação de riscos.	X				
REQNF61	Os dados deverão ser armazenados de forma automatizada somente na solução contratada por todo o prazo contratual, até que seja finalizada a migração completa dos dados para a Fhemig ou para outra empresa indicada pela Fhemig. Após o fim do contrato, os dados coletados serão repassados de forma segura à contratante e permanentemente eliminados;	X				
REQNF62	Adotar medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade, privacidade e autenticidade das informações a serem tratadas no âmbito da prestação dos serviços de desenvolvimento, manutenção, sustentação, testes e controle de qualidade de software, inclusive no atendimento à LGPD;	X				
REQNF63	Implementar e manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;	X				
REQNF64	Implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela contratante, observando a periodicidade e tempo de guarda legalmente estabelecidos ou definidos pela contratante;	X				
REQNF65	Manter a resiliência e eficiência dos sistemas de informação do órgão/entidade;	X				

REQNF66	Adotar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade;	X				
REQNF67	Executar periodicamente análise de vulnerabilidades na Solução de TIC, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção. Além disso, é necessário que haja um processo documentado para gestão de vulnerabilidades em soluções de TIC. Ele deverá ser revisado e atualizado periodicamente, principalmente quando ocorrerem mudanças na organização;	X				
REQNF68	Utilizar técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação no processo;	X				
REQNF69	Registrar alterações em registros do sistema devem ser através de trilhas de auditoria que contenham: a. Data e hora da alteração; b. Funcionalidade ou assunto; c. Tipo da alteração (ex.: inclusão, alteração, exclusão, etc); Identificação do usuário responsável pela alteração; Identificação da origem da alteração (ex.: endereço IP, dispositivo do usuário, ponto de acesso, etc); d. Identificador do registro afetado pela alteração (por exemplo, campo chave do registro); e. Valores anterior e atual dos dados do registro alterado.	X				
REQNF70	Disponibilizar todos os recursos necessários, de forma tempestiva, para que a contratante, ou outra entidade por ela indicada, realize atividade continuada de auditoria de privacidade e segurança da informação relacionada ao objeto do contrato;	X				
REQNF71	Permitir acesso aos registros de trilha de auditoria apenas para usuários explicitamente autorizados pela CONTRATANTE;	X				
REQNF72	Guardar os logs coletados pelo sistema por pelo menos 1 (um) ano, em local seguro;	X				
REQNF73	Adotar práticas de codificação segura;	X				
REQNF74	Isolar instalações de desenvolvimento, testes e operacionais;	X				
REQNF75	Mapear problemas, cenários e soluções dos sistemas em produção;	X				
REQNF76	Realizar manutenções corretivas (eliminação de comportamentos do software que diferem de suas especificações ou que provoquem a interrupção inesperada de seu funcionamento);	X				
REQNF77	Remover erros ou falhas ocorridas que impeçam o funcionamento do sistema sob a sua responsabilidade, tais como cancelamento de programa, demora no processamento, parada de rotinas, resultados inesperados no processamento e quaisquer defeitos ou deficiências não cobertos pela Garantia;	X				
REQNF78	Fazer atualizações e correções de segurança do sistema operacional ou aplicativos somente após a devida validação no respectivo ambiente de homologação;	X				

REQNF79	Emitir sempre mensagem de erro ou aviso autoexplicativo, quando ocorrer insucesso em alguma operação;	X				
REQNF80	Garantir a atomicidade, consistência, isolamento e durabilidade das informações (ACID);	X				
REQNF81	Garantir que apenas arquivos e componentes indispensáveis para o correto funcionamento do sistema estejam presentes no ambiente de produção;	X				
REQNF82	Anonimizar dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação);	X				
REQNF83	Realizar atualizações de segurança somente após validação adequada;	X				
REQNF84	Mapear problemas, cenários e soluções em sistemas em produção;	X				
REQNF85	Utilizar o protocolo HTTPS e Certificado Digital WEB SSL válido entre a conexão do usuário e o Front-end;	X				
REQNF86	Entregar ao CONTRATANTE, além do Código-Fonte, a Documentação referente a cada desenvolvimento;			X		Por questões de proteção de dados e privacidade e segurança, assim como devido aos direitos de autor do produto, a SISQUAL não fornece o código fonte do produto. Sempre que for solicitado um RFC em plugin (externo ao produto), a SISQUAL está em condições de fornecer o código sempre que for solicitado. Em ambos os casos a documentação é sempre fornecida.
REQNF87	Elaborar ou atualizar a documentação de sistemas legados. Em caso de impossibilidade de trabalho na documentação do sistema legado, elaborar a documentação da funcionalidade objeto da mudança;	X				
REQNF88	Possuir e implementar um Plano de Continuidade Operacional e um Plano de Contingência relacionados ao objeto contratado, que garantam o nível requerido de continuidade para a segurança da informação durante uma situação adversa;	X				
REQNF89	Realizar e apresentar análise/avaliação de riscos periodicamente;	X				
REQNF90	Realizar e apresentar à contratante periodicamente uma análise/avaliação de riscos da arquitetura de Solução de TIC, indicando os eventos de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela contratante;	X				
REQNF91	Comunicar imediatamente à CONTRATANTE a ocorrência de qualquer incidente envolvendo os serviços contratados, tomando de imediato todas as medidas que possam minimizar eventuais perdas e danos causados em razão do incidente, além de aplicar os melhores esforços para cessar o incidente com a maior brevidade possível;	X				

REQNF92	Possuir e implementar política de backup das informações e dos registros de log da solução contratada, em conformidade com os dispositivos legais aplicáveis, a ser homologada pela contratante, que assegure a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica, os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha ou por solicitação da contratante, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante;	X				
REQNF93	Manter os backups em local apartado dos dados originais;	X				
REQNF94	Garantir a integridade dos backups de banco de dados dos módulos operacionais do sistema;	X				
REQNF95	Realizar backups automatizados preferencialmente nas chamadas “janelas de backup”, períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática;	X				
REQNF96	Gerir restauração com planejamento, implantação e testes dos procedimentos de recuperação (incluindo login pelos usuários finais) necessários para restabelecer a funcionalidade do Serviço, Sistema Operacional do sistema, bancos de dados, aplicativos, e dados dos usuários, em caso de uma falha;	X				
REQNF97	Implementar controle de acesso para evitar acesso não autorizado;	X				
REQNF98	Prevenir acesso não autorizado às informações disponibilizadas para prestação dos serviços de desenvolvimento, manutenção, sustentação, testes e controle de qualidade de software;	X				
REQNF99	Possuir identificação única para cada usuário, por meio de logins e senhas individualizadas, de forma a permitir auditoria, controle de erros e de tentativas de invasão;	X				
REQNF100	Armazenar e transmitir as senhas para acesso à aplicação criptografadas;	X				
REQNF101	Atender às políticas de segurança definida pela CONTRATANTE nas regras de configuração de senha;	X				
REQNF102	Implementar controle de acesso para evitar que informações sejam acessadas ou alteradas por indivíduos não autorizados;	X				
REQNF103	Possuir e implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato. Assegurar a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa;	X				
REQNF104	Reportar de imediato à contratante incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC;	X				

REQNF105	Possibilidade de executar o sistema na infraestrutura de rede das unidades, especificadas no Anexo VI – Rede unidades Fhemig;	X				
REQNF106	Os computadores utilizados para acessar o sistema serão disponibilizados pela Fhemig nas unidades assistenciais.	X				
REQNF107	Garantir que o sistema possa ser acessado por rede wi-fi e por rede local (LAN), pois nem todas as unidades assistenciais possuem wi-fi instalado.	X				