 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	1
5.	RESPONSABILIDADES	2
6.	REGRAS BÁSICAS	2
7.	CONTROLE DE REGISTROS.....	39
8.	ANEXOS.....	40
9.	REGISTRO DE ALTERAÇÕES	42

1.OBJETIVO

Apresentar os requisitos mínimos de segurança da informação obrigatórios e recomendáveis para todos os serviços, aplicações e infraestrutura durante a implementação de projetos do **Grupo CPFL**.

2.ÂMBITO DE APLICAÇÃO

Este documento abrange toda e qualquer área ou equipe do **Grupo CPFL**.

3.DEFINIÇÕES


Não se aplica.

4.DOCUMENTOS DE REFERÊNCIA

Para o desenvolvimento deste documento foram considerados:

- a) Políticas e normas internas do Grupo;
- b) LGPD – Lei Geral de Proteção de Dados (nº 13.709, de 14 de agosto de 2018);
- c) Cobit 4.7 (DS1 ao 13, ME3, AI6);

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	1 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

- d) ISO 27001;
- e) ISO 27002;
- f) NIST Special Publication 800-144;
- g) NIST Special Publication 800-7;
- h) Cloud Security Alliance (CIA);
- i) GED 18846 - Procedimento para adoção de cláusulas de Proteção de Dados;
- j) GED 18836 - Norma de Proteção de Dados Pessoais para Fornecedores e Prestadores de Serviço;
- k) GED 18662 – Requisitos de segurança para soluções em Nuvem;

5. RESPONSABILIDADES

Gerência de Segurança da Informação

- Informar e avaliar os requisitos mínimos de segurança da informação em novos projetos;

Gerência de Proteção de Dados

- Informar e avaliar os requisitos mínimos de privacidade de dados em novos projetos;

6. REGRAS BÁSICAS

6.1 INTRODUÇÃO


Apresentar os requisitos mínimos de Segurança da Informação a serem endereçados em novos projetos da companhia, não somente os de Tecnologia da Informação, mas também nos projetos das áreas de negócio e operacionais. Para os itens de Privacidade de Dados estão apresentadas nas GEDs 18846 Procedimento para adoção de cláusulas de Proteção de Dados e 18836 Norma de Proteção de Dados Pessoais para Fornecedores e Prestadores de Serviço.

6.2 Matriz de Conformidade - Requisitos Não Funcionais – SaaS

6.2.1 Desenho Geral da Arquitetura

1. Modelagem de arquitetura . Apresentar o desenho da arquitetura macro da solução contemplando todos os módulos envolvidos, integrações, conexões e protocolos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	2 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

Principalmente contendo os pontos de exposição de serviços e integração com sistemas da CPFL.

2. Produto Escalável - Deve suportar o crescimento de negócio e utilização de ferramenta sem impactos de performance. Descrever os mecanismos da solução para atender a esse requisito.
3. Exposição de funcionalidades - Deve possuir APIs expostas via web services para integração com aplicações externas.
4. Detalhar as ferramentas e formas de customizações / configurações / parametrizações - Listar quais ferramentas e formas de customizações, configurações e parametrizações.
5. "Logs - Deve permitir a criação de logs, e fornecer mecanismos para seu acesso e configuração. Detalhar os tipos de log e seus mecanismos de gerenciamento. Os logs precisarão ser mantidos por pelo menos 90 dias"
6. Extensibilidade futura do sistema - Deve ser atualizável e informado o roadmap de evolução. As atualizações serão feitas diretamente pelo fornecedor da solução e não deverá incidir em indisponibilidade da solução.
7. A solução deve fornecer formas de extração de dados a fim de serem extraídos, transformados e carregados para soluções analíticas da CPFL. Necessário detalhar os mecanismos que fornece dados armazenados, Near-Real-Time e/ou Real-Time


6.2.1.1 Propriedade

8. "Todos os dados da aplicação são de propriedade da CPFL e, portanto, ela tem o direito de extrair seus dados a qualquer momento. A solução deverá prover o mecanismo que a CPFL poderá utilizar para essa extração."

6.2.2 Interoperabilidade e Integração

1. Integração SOA - Deve seguir os padrões de mercado com compatibilidade para comunicação com soluções ESB (Enterprise Service Bus) em especial, compatibilidade com SAP PI, SAP PO e interfaces SOAP Adapter
2. Deve seguir os padrões de OASIS e W3C para desenvolvimento de Web Services. Fornecer a lista de especificações suportadas (WS-*)
3. Deve possuir capacidade para utilizar um service registry para consultar os serviços através do protocolo UDDI (Universal Description Discovery and Integration)
4. As interfaces devem ser protegidas por mecanismos de autenticação. Os mecanismos suportados deverão ser descritos na proposta

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	3 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

5. A solução deve prever configuração de VPN site-to-site para integrações críticas onde seja necessário acessar base de dados ou serviços que não estão expostos à internet pela CPFL. Essa VPN deve ser configurada de forma a não expor de ambos os lados nada além do estritamente necessário para que a solução funcione.
6. Deve seguir os padrões de mercado com compatibilidade para comunicação com soluções de API Management e suporte RESTFul


6.2.3 Interfaces para Usuários

1. Deve possuir internacionalização de funcionalidades (Ex; idioma inglês e português e regionalização - moeda).
2. Deve permitir a exposição de serviços de apresentação (Portlets Remotos) caso seja especificado nos requisitos funcionais a necessidade de expor informações para outros sistemas
3. Acessibilidade - Deve possuir interfaces que sigam o padrão WCAG 2.0 definido pelo W3C (www.w3c.org). Detalhar as interfaces que seguem este padrão.
4. As interfaces com o usuário via Web, devem ser desenvolvidas de forma a tornar possível a visualização do conteúdo tanto em desktops como em dispositivos móveis (Tables e smartphones). De forma que o conteúdo da página se adeque às limitações do dispositivo o mínimo suficiente para que as operações possam ser executadas nos mesmos, exceto se houver requisito de negócio de defina de forma mais específica a interface.

6.2.4 Segurança da Informação


1. Toda informação deve ser armazenada em Banco de Dados de forma segura e garantindo a disponibilidade, integridade e confidencialidade.
2. Toda informação deve ser armazenada em um Banco de dados dedicado.
3. Toda informação confidencial deve ser criptografada em seu armazenamento.
4. Todas as senhas devem ser armazenadas em formato de hash com salt, nunca a senha original (mesmo que criptografada).
5. Todo armazenamento e/ou processamento dos dados pessoais deve ser em território nacional.
6. Deve garantir à CPFL a recuperação dos dados armazenados ou processados à qualquer tempo.
7. Deve garantir o descarte seguro de dados em caso de término do serviço contratado, realizando procedimento de wipe (sanitização de dados).

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	4 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos


8. Não deve ter usuários e senhas armazenados de forma hardcoded. Deve prover mecanismos onde a própria equipe da CPFL possa trocar usuários usados na aplicação sem recompilação de código.
9. Deve gerar registros (logs) de acessos e de operações críticas (data, hora, ID (login), endereço IP, operação (leitura, inclusão, alteração, exclusão, login, logoff)).
10. Deve armazenar registros (logs) por um período mínimo de 30 dias.
11. Deve proteger os registros (logs) de tal forma que seus dados não possam ser alterados.
12. Deve disponibilizar relatório de usuários vs. perfis.
13. Caso haja relatório de auditoria de segurança da informação relacionado ao sistema/ferramenta/produto deve ser apresentado.
14. A solução será submetida a testes de segurança com ferramentas de vulnerabilidades. O resultado da análise poderá impedir a entrega da solução em produção até a correção dos apontamentos.
15. Deve realizar testes de intrusão periodicamente a fim validar a segurança do ambiente e compartilhar o relatório com a CPFL.
16. Deve apresentar relatório de auditoria de segurança feito por entidade externa e idônea atestando a segurança da aplicação.
17. Deve realizar backup dos dados diariamente minimamente.
18. Deve realizar testes de restore periodicamente.
19. Deve armazenar as cópias de segurança em local externo ao local padrão de armazenamento dos dados.
20. Deve possuir perfis de acesso que atendem segregação de função, a fim de evitar fraudes (RBAC role-based access control).
21. Deve restringir o acesso a dados sensíveis.
22. Deve permitir a criação e manutenção de Perfis
23. Deve permitir associar o perfil de acesso a grupo correspondente no Active Directory.
24. Não deve necessitar de privilégio de administrador de sistema operacional ao usuário final.
25. Caso não seja possível associar o perfil de acesso a grupo correspondente no Active Directory, deve existir perfis segregados para as atividades de “criação de perfil” e “administração”.
26. Deve permitir a integração com ferramenta de gestão de identidades externa (IDM).

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	5 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos


27. Os acessos às informações devem ser feitos obrigatoriamente via aplicação, obedecendo os respectivos perfis de acesso.
28. Todos os administradores de banco de dados não devem ter acesso às informações sensíveis armazenadas na base.
29. Caso não seja possível a integração com o ADFS, deve possuir Política de Usuários e Senhas customizável para atender a política de senha da CPFL.
30. Deve oferecer controle de acessos em diferentes níveis através de identificação do usuário (credenciais de acesso) e das permissões do perfil de acesso associado a ele.
31. Deve informar ao usuário final a data e hora de último acesso.
32. Deve possuir arquitetura compatível com alta disponibilidade.
33. Deve fornecer relatório de SLA de disponibilidade mensalmente.
34. Deve integrar com o ADFS.
35. Deve ser compatível e integrável com as melhores soluções de duplo fator de autenticação.
36. Deve permitir autenticação de usuários via SingleSignOn através de integração com Microsoft ou, caso haja integração com sistemas específicos, detalhar o protocolo correspondente.
37. Deve ser aderente a LGPD - Lei Geral de Proteção de Dados.
38. Se aplicável, deve ser aderente ao BACEN 4893 - Política de segurança cibernética e requisitos para contratação de serviços em nuvem para sistemas financeiros.
39. Deve aplicar patches e hotfix de segurança para correções de vulnerabilidades identificadas com qualquer CVE/CVSS.
40. Deve possuir um processo de notificação aos clientes antes que sejam feitas manutenções e/ou alterações que possam afetar o serviço contratado.
41. Dados de produção não devem ser replicados ou usados em ambientes de não produção.
42. Deve possuir um processo de rescisão e medidas educativas para o colaborador que não cumpriu com o estabelecido nas Políticas de Segurança.
43. Deve possuir plano de conscientização de segurança para sensibilizar os colaboradores sobre os cuidados, como phishing e boas práticas de segurança.
44. Deve possuir contrato de confidencialidade assinado com funcionários e prestadores de serviços.
45. Deve possuir uma política de segurança da informação que tenha sido aprovada pela diretoria, comunicada aos funcionários e exista um responsável por mantê-la e revê-la.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	6 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

46. Deve possuir uma política de privacidade de dados que tenha sido aprovada pela diretoria, comunicada aos funcionários e exista um responsável por mantê-la e revê-la.
47. Deve possuir política e procedimentos de desenvolvimento seguro de software e processo de ciclo de vida (SDLC).
48. Deve possuir planos de continuidade de negócios e de resposta a incidentes de segurança implantados e testados.
49. Deve possuir medidas de proteção contra vazamento de dados implementados, bem como procedimentos de classificação da informação e mecanismos de rótulos.
50. Toda comunicação deverá ocorrer somente através de protocolos seguros/criptografados (SSH/IPSEC/TLS).
51. Deve possuir mecanismos que impeça a utilização de robôs nas tentativas de acesso e que dificultem ataques de força bruta.
52. Deve garantir proteção contra as principais técnicas de invasão de sistemas. Os principais e mais comuns podem ser conhecidos através de instituições como www.owasp.org
53. Deve prover mecanismos de Detecção e Prevenção contra-ataques ou acessos não autorizados.
54. Deve possuir Antimalware do tipo EDR Proteção Contra Software Malicioso no ambiente do fornecedor para evitar a execução de malware em dispositivos de terminal de usuário de propriedade organizacional e/ou gerenciados (estações de trabalho, laptops e dispositivos móveis emitidos), bem servidores e rede de infraestrutura de TI.
55. Deve prover medidas para fortalecer as configurações de segurança (hardening) dos sistemas virtualizados para fornecer apenas as portas, protocolos e serviços necessários para atender às necessidades de negócios e ter controles técnicos de suporte, como antivírus, monitoramento de integridade de arquivos e registro em log.
56. Deve prover configuração multitenant (multilocatário), que forneça separação de acesso e isolamento dos dados com os clientes.
57. Caso haja integrações com sistemas internos, deve ser estabelecida conexão VPN site-to-site para comunicação entre as partes.
58. Deve permitir a configuração de "time-out" de sessão, após período de inatividade do usuário.
59. Não deve necessitar ou fazer uso de protocolos considerados inseguros como telnet, FTP, etc.
60. Não deve possuir recursos técnicos que permitam que o usuário faça manutenção ou consulta direta ao banco de dados através de queries. Todo acesso ao banco de dados deve ser feito apenas por interfaces específicas para a função.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	7 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

61. Deve utilizar algoritmo de criptografia padrão de mercado ao invés de criar uma solução própria.
62. Deve possuir configuração de Whitelist / Allowlist para permitir somente os IP's do Proxy da CPFL e os IP's da rede acessar a aplicação.
63. Deve notificar em caso de incidentes de segurança da informação.
64. Deve ser compatível e integrável com as melhores soluções de SIEM do mercado.
65. O fornecedor deverá seguir as diretrizes da CPFL da política "Requisitos da Segurança da Cloud" como padrão para a solução a ser entregue, tendo os requisitos do capítulo 6.15 dessa política a constar no contrato.

6.2.5 Segurança de Aplicação

1. Single Sign On de usuário - Deve permitir autenticação de usuários através da autenticação integrada do Windows ou caso haja integração com sistemas específicos será necessário detalhar o protocolo correspondente.
2. Deve criptografar todos os dados considerados confidenciais


6.2.6 Desempenho e Volumetria

1. Deve especificar o volume de transações e o respectivo desempenho baseado nos requisitos funcionais, assim como os pontos de quebra desse desempenho que exigirão revisão na infraestrutura

6.2.7 Documentação

1. "Fornecer documentação sobre a arquitetura applicativa, incluindo, mas não se limitando a:
 - ✓ Desenho da arquitetura applicativa e integrações;
 - ✓ Especificações e Dicionário de bancos de dados;
 - ✓ Diagrama de entidade-relacionamento;
 - ✓ Leiaute de arquivos internos;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	8 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

- ✓ Desenho de telas;
- ✓ Fluxograma do sistema;
- ✓ Descrição dos Problemas mais comuns e guia de resolução (Troubleshooting)"

2. Deve possuir manual operacional contendo detalhamento das operações de monitoramento, recuperação, controles, arquivamento, segurança e controle de acesso em português (Brasil).
3. Deve possuir manual de usuário contendo informações para acesso ao sistema, navegação de telas e menus, relatórios existentes, workflow, mensagens de erro, entrada de dados, etc., em português (Brasil).

6.2.8 Infraestrutura

1. Caso haja solução hospedada em Data Center terceiro deverá apresentar certificações que atestem a segurança e qualidade do datacenter onde a solução está.
2. "Em caso de Projeto que envolva Data Center de Terceiro, o DATACENTER deverá ter as seguintes certificações:
 - ✓ - Tier III Design/Tier III Facilities - Uptime Institute
 - ✓ - ISO 27001 - Segurança da informação
 - ✓ - ISO/IEC 20000 - Qualidade de serviços
 - ✓ - ISO 14001 - Meio Ambiente
 - ✓ - ISO 37001 - Antissuborno

Caso o Data Center de Terceiro não possua as certificações recomendadas, deverá listar as certificações que possui e eventualmente justificar e apresentar contraponto das que não possui."


3. A solução como um todo deve apresentar uma disponibilidade de 99,5% atestada através de relatórios.
4. "Hardware - Estação Cliente

Detalhar a configuração (licenciamento, versionamento, compatibilidade, etc.) mínima E ideal das estações clientes (Hardware - CPUs, memória, storage,) para o produto proposto, tendo como base o plano de crescimento da solução.

Não é necessário precificar as estações clientes."

5. "Software - Estação Cliente

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	9 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

- ✓ Detalhar a necessidade de todos os softwares 'básicos' (Sistema Operacional, Browsers, Conectores clientes a banco de dados) para as estações clientes do produto proposto - licenciamento, versionamento, compatibilidade, etc.
- ✓ Não é necessário precificar as licenças dos softwares básicos.

Preferência:

- ✓ Sistema Operacional - Windows
- ✓ Browser - Internet Explorer 9.0 ou superior"

6. "Computadores da equipe do projeto. O fornecedor deverá prover o hardware e software necessário para que seus colaboradores executem o serviço. Qualquer necessidade que precise ser provida pela CPFL deverá ser expressa na proposta"
7. "Detalhar a necessidade de licenciamento do(s) produto(s) proposto(s), tendo como base o plano de crescimento da CPFL (enviado na planilha de volumetria).

É necessário precificar as licenças do(s) produto(s) da seguinte forma:

- ✓ Tomando como base a volumetria atual e esperada pela CPFL;
- ✓ ULA (Unlimited License Agreement)"

8. "Ambientes

Detalhar as informações separadas por ambiente:


- ✓ Desenvolvimento
- ✓ Homologação/Treinamento
- ✓ Produção"

9. "Banco de dados

Detalhar a tecnologias utilizada para banco de dados, bem como mecanismos para a extração em massa dos dados da CPFL a qualquer momento que a mesma entenda como necessário."

10. Em caso de solução hospedada em Data Center terceiro, fica vedado alterar o datacenter sem previa validação da CPFL, atestando de que todos os requisitos solicitados nesta avaliação continuam a ser atendidos pelo novo Datacenter. É necessário realizar uma nova avaliação des requisitos.
11. Não é permitido o compartilhamento de servidores onde os dados e a VPN site-to-site da CPFL que se pretendam hospedar com serviço de terceiros sem a validação interna da área de S.I da CPFL, para não gerar riscos de exposição dos dados da CPFL a outra aplicação ou empresa, bem como não expor a conexão com o datacenter da CPFL.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	10 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

12. O Datacenter da solução deverá estar localizado no Brasil, sem prejuízos ou limitações de funcionalidades com relação a outras localidades no planeta.

6.2.8.1 Governança


O fornecedor deverá prover para a CPFL o relatório ISAE - Type1 e Type2

6.22 Matriz de Conformidade - Requisitos Não Funcionais – On Premisse

6.22.1 Desenho geral da arquitetura

1. "Produto Modular - Deve ser baseada em um ""core"" que é atualizado via liberações de versões de produto. Qualquer customização deve ser criada fora do ""core"" de aplicação, ou integrado a uma outra solução."
2. Produto Escalável - Deve suportar clusterização e load balancing para atender o crescimento de negócio e utilização de ferramenta.
3. Produto Multi-Instâncias - Deve ser possível a convivência com outras soluções que se encontram multi-instanciadas.
4. Deve possuir Arquitetura Aberta, não utilizando soluções de arquitetura proprietários do fornecedor.
5. Exposição de funcionalidades - Deve possuir APIs expostas via web services para integração com aplicações externas.
6. "Mecanismos de cache - Deve possuir mecanismos para armazenar informações em memória. Especificar a lista de mecanismos e suas formas de gerenciamento operacional."
7. "Linguagem de Programação - Especificar as linguagens de programação e versões utilizadas pelos módulos do produto e integrações. O padrão de arquitetura da CPFL direciona a solução para plataforma Microsoft .NET, linguagem C#. Qualquer proposta diferente deve ser submetida à CPFL para uma aprovação formal."
8. Ferramentas e formas de customizações / configurações / parametrizações
- Listar quais ferramentas e formas de customizações, configurações e parametrizações.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	11 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

9. Adaptabilidade, Flexibilidade e Time-to-market - Deve ser customizável e flexível através de configuração/parametrização, sem necessidade de alteração de código. Esclarecer a utilização de ferramentas de configuração/parametrização e codificação.
10. "Logs - Deve permitir a criação de logs, e fornecer mecanismos para seu acesso e configuração. Detalhar os tipos de log e seus mecanismos de gerenciamento. Os logs precisarão ser mantidos por pelo menos 90 dias"
11. Extensibilidade futura do sistema - Deve ser atualizável e informado o roadmap de evolução.
12. Deve possuir módulos de processamento batch e online. O processamento em batch não pode implicar na diminuição da performance de processos online.
13. Paralelismo de processamento - Deve permitir a execução e o controle dos processos paralelos. (Online e Batch)
14. Suporte a containers. A aplicação deve suportar ser executada em containers, porém não deve ser mandatório. Fica a critério da CPFL a melhor estrutura a aplicar.


6.22.2 Administração de Ambiente

15. Deve ser possível configurar o ambiente da aplicação. Detalhar as formas de configuração.
16. "Deve ser possível monitorar o ambiente da aplicação a partir de métricas definidas pela CPFL e configuração de alarmes. Detalhar as formas de monitoração e configuração de alarmes."
17. "Deve ser possível monitorar o ambiente da aplicação remotamente, via protocolos padrão de mercado. Detalhar a lista de protocolos disponíveis para monitoração remota."

6.22.3 Interoperabilidade e Integração

18. Integração SOA - Deve seguir os padrões de mercado com compatibilidade para comunicação com soluções ESB (Enterprise Service Bus) em especial, compatibilidade com SAP PI, SAP PO e interfaces SOAP Adapter

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	12 de 42


 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

19. Entregará especificação de todos os tipos/finalidade de integração entre os sistemas.
20. Deve possuir controle para que transações não sejam processadas em duplicidade.
21. Deve permitir o monitoramento e análise de problemas relacionados às transações.
22. Deve seguir os padrões de OASIS e W3C para desenvolvimento de Web Services. Fornecer a lista de especificações suportadas (WS-*)
23. Deve possuir capacidade para utilizar um service registry para consultar os serviços através do protocolo UDDI (Universal Description Discovery and Integration)
24. Suporte a protocolo REST
25. Suporte estrutura de microserviços
26. Exposição de WebAPIs

6.22.4 Interfaces para Usuários


27. Deve permitir a utilização de campos com valores default facilmente configuráveis, de forma a agilizar a entrada de dados.
28. Deve permitir a utilização de campos preenchíveis a partir de tabelas de valores configuráveis (look up tables).
29. Deve possuir a facilidade de seleção a partir de listas filtradas a partir de digitação parcial do texto.
30. Deve possuir diferenciação entre campos de preenchimento obrigatório e opcional.
31. Deve permitir a possibilidade de configuração de campos quanto à obrigatoriedade de preenchimento, sem necessidade de alteração de código.
32. Deve possuir a diferenciação entre campos digitáveis e campos apenas informativos.
33. Deve possuir preenchimento inteligente, facilidades de copy and paste e de undo/redo.
34. Deve possuir menu de funções amigáveis e autoexplicativos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	13 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

35. Deve permitir o transporte entre telas das informações comuns, evitando redigitação.
36. Deve permitir o acesso às transações online do sistema através de navegadores (browsers) padrões de mercado.
37. Campos de listas com apenas uma ocorrência válida deverão ser apresentados automaticamente na tela.
38. Deve permitir a navegação entre campos nas telas através de TAB ou de teclas de função.
39. Acesso de atendentes (CSR's) a aplicações de terceiros através de "janelas" em sua tela principal (em contexto).
40. Deve possuir internacionalização de funcionalidades (idioma e regionalização - moeda), com possibilidade de utilização em mais de um local definido no momento do login.
41. Deve possuir menus e interfaces em Português (Brasil).
42. Possibilidade de criação de dicionário personalizado, respeitando requisitos de internacionalização
43. Deve permitir a paginação e ordenação de registros, de maneira configurável
44. Deve oferecer facilidades de atalhos para funcionalidades muito utilizadas.
45. Permitir configuração do layout gráfico. Fornecer documentação dos mecanismos de gerenciamento de layout gráfico.
46. Deve oferecer facilidades de ajuda (help) sensível ao contexto, utilizando a internacionalização de acordo com o requisito
47. Deve oferecer facilidades de configuração das mensagens de erro apresentadas, utilizando a internacionalização de acordo com o requisito
48. Deve permitir a exposição de serviços de apresentação (Portlets Remotos) caso seja especificado nos requisitos funcionais a necessidade de expor informações para outros sistemas
49. Especificar quais os tipos de interface e suas tecnologias em cada módulo do produto.
50. Acessibilidade - Deve possuir interfaces que sigam o padrão WCAG 2.0 definido pelo W3C (www.w3c.org). Detalhar as interfaces que seguem este padrão.
51. Caso não seja necessário para atender algum requisito de negócio compatibilidade com versões de navegadores antigos e houver interfaces

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	14 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos


Web, as páginas devem ser desenvolvidas com HTML5 a fim de garantir compatibilidade com diversos navegadores e plataformas.

52. Caso haja interfaces Web, devem ser desenvolvidas de forma responsiva que atenda as necessidades de negócio de forma dinâmica.
53. Caso haja interfaces Web, devem ser desenvolvidas de forma a tornar possível a visualização do conteúdo tanto em desktops como em dispositivos móveis (Tables e smartphones). De forma que o conteúdo da página de adequa às limitações do dispositivo o mínimo suficiente para que as operações possam ser executadas nos mesmos, exceto se houver requisito de negócio de defina de forma mais específica a interface.
54. O sistema não deve fazer usu de pop-ups em janelas separadas. Quando for necessário deverá utilizar players HTML para exibição de mensagens.
55. Não deve possuir recursos (telas, formulários, gráficos) em Adobe Flash

6.22.6 Geral

56. Aderência à Política da CPFL - a ser validada em conjunto com a TI da empresa nas reuniões preliminares.
57. Controle de Acesso de Usuários - Deve oferecer controle de acessos em diferentes níveis através do registro de identificação o usuário, operação realizada e data. Deve permitir a integração com ferramenta de gestão de identidades externa. Deve assegurar regras de segregação de função, a fim de evitar fraudes.
58. Desejável que permita a integração com ferramenta de gestão de identidades externa (IDM).
59. Deve oferecer controle de acesso aos dados através do registro de identificação do usuário, operação realizada e data.
60. Deve restringir o acesso a dados sensíveis.
61. Deve gerar registros (logs) de operações realizadas.
62. Deve ser compatível e integrável com as melhores soluções de SIEM do mercado.
63. "Manutenção de usuários - Deve possuir funcionalidade para criação, alteração, exclusão e consulta de ""logins"" de acesso, permitindo:
 - Cadastramento de um único usuário, caso não seja possível integrar com o AD.
 - Cadastramento de múltiplos usuários


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	15 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

Estas funcionalidades devem ser disponibilizadas para chamadas externas, pois estas ações, em geral, serão realizadas pelo Gerenciador de Identidades da CPFL"

64. Deverá permitir a integração com o Gerenciador de Identidades a fim de permitir as ações supracitadas através desta ferramenta.
65. Deve permitir a manutenção de Perfis
66. Autenticação do usuário - A autenticação do usuário deverá ser feita via LDAPS no Active Directory da Microsoft
67. Ser compatível e integrável com as melhores soluções de duplo fator de autenticação.
68. Controle de Acessos - Os acessos às informações deverão ser feitos sempre, obrigatoriamente, via aplicação, obedecendo os respectivos perfis de acesso. RBAC (role-based access control)
69. Armazenamento da informação - Toda informação deverá ser armazenada em Banco de Dados. As informações devem ser armazenadas de forma segura, garantindo a disponibilidade, integridade e confiabilidade.
70. Senha CASE SENSITIVE - Deverá permitir a utilização de Caracteres obrigatórios conforme checklist de segurança da informação
71. Não deve necessitar de senha de administrador de Banco ou sistema Operacional para funcionamento.
72. Conexão segura - Transações realizadas via Intranet ou Internet utilizando conexão segura, no padrão https (128 bits), principalmente para informações de login, senhas e mecanismos que dificultem ataques de força bruta.
73. Integração com repositório de autenticação - Deve ser possível integrar com o Active Directory, via DNS. Permitindo assim, redundância no momento da autenticação.
74. Deve garantir proteção contra as principais técnicas de invasão de sistemas. Os principais e mais comuns podem ser conhecidos através do site <https://www.owasp.org>
75. Deve permitir a configuração de "Time-out" de sessão, caso o usuário não realize operações no seu browser em intervalo de tempo.
76. A solução poderá ser submetida a testes de segurança com ferramentas de vulnerabilidades. O resultado da análise poderá impedir a entrega da solução em produção até a regularização do apontamento.
77. Deve ser aderente a LGPD - Lei Geral de Proteção de Dados, se aplicável.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	16 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos


78. No caso de não integração com AD, a senha deverá ter um tamanho mínimo de 8 caracteres, sem restrição no tamanho máximo, exigindo uma complexidade mínima na senha e não permitindo a repetição das última 5 senhas usadas
79. Caso a solução possua tela de login, deve possuir captcha e mecanismo para mitigar ferramentas brute-force
80. Não deve necessitar ou fazer uso de protocolos considerados inseguros como Telnet ou FTP
81. Caso exista suporte remoto, deve ser realizado obrigatoriamente por conexão VPN site-to-site.
82. Deve disponibilizar patches e hotfix de segurança para correções de vulnerabilidades identificadas com qualquer CVE/CVSS.
83. Caso a solução possua trilha de auditoria, a mesma deve ser protegida de tal forma que seus dados não possam ser alterados.
84. A solução não deve possuir recursos técnicos que permitam a manutenção ou consulta direta ao banco de dados através de queries. Todo acesso ao banco de dados deve ser feito apenas por interfaces específicas para a função.
85. A solução não deve expor em arquivos de configuração nenhum usuário/senha utilizada na solução
86. Mecanismos de atualização de usuários e senha. A solução não deve ter usuários e senhas armazenados de forma hardcoded. Deve prover mecanismos onde a própria equipe da CPFL possa trocar usuários usados na aplicação sem recompilação de código, isso deve observar o requisito de criptografia acima.

6.22.7 Criptografia

87. Deve utilizar um algoritmo de criptografia padrão de mercado ao invés de criar uma solução própria.
88. Deve ser possível cifrar todos os dados considerados confidenciais
89. Todas as senhas devem ser armazenadas em formato de hash com salt, nunca a senha original (mesmo que criptografada).

6.22.8 Segurança de Aplicações

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	17 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

90. Single Sign On de usuário - Deve permitir autenticação de usuários através da autenticação integrada do Windows ou caso haja integração com sistemas específicos será necessário detalhar o protocolo correspondente.
91. Segurança de Serviços - Deve permitir autenticação e autorização de serviços expostos para garantia que somente usuários e/ou aplicações autorizados acessar recursos. Fornecer a lista de formas de autenticação e autorização disponível e possível.
92. Autorização de usuário - Deve permitir integração com uma ferramenta de controle de políticas de segurança.

6.22.9 Gerenciamento de Dados


93. Gerenciamento de transações - Deve suportar a execução de transações de dados ad hoc para acesso aos dados armazenados no banco de dados, através de scripts parametrizáveis, armazenáveis e reutilizáveis, cujos resultados podem ser compartilhados com usuários autorizados.
94. Controle de transações - Deve oferecer controles que permitam a gestão de transações ofensoras da performance ou integridade do sistema.
95. Interface gráfica - Deve oferecer uma interface gráfica para construção, submissão, acompanhamento da execução e visualização de resultados de transações.
96. Disponibilização de dados - Oferecer ferramenta de extração de dados para disponibilização a outros sistemas.
97. Disponibilização de dados - Permitir a extração de dados através de outras ferramentas de mercado. Detalhar quais ferramentas e/ou tecnologias de mercado são suportadas.

6.22.10 Desempenho e Volumetria

98. Deve especificar o volume de transações e o respectivo desempenho baseado nos requisitos funcionais, assim como os pontos de quebra desse desempenho que exigirão revisão na infraestrutura
99. Tráfego máximo permitido por página web de 200KB.

6.22.11 Documentação

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	18 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

100. Fornecer documentação sobre a arquitetura aplicativa, incluindo, mas não se limitando a:

- * Desenho da arquitetura aplicativa e integrações;
- * Especificações e Dicionário de bancos de dados;
- * Diagrama de entidade-relacionamento;
- * Leiaute de arquivos internos;
- * Desenho de telas;
- * Fluxograma do sistema;
- * Descrição dos Problemas mais comuns e guia de resolução (Troubleshooting)"

101. "Deve possuir manual de instalação, operação e manutenção do sistema incluindo, mas não se limitando a:

- * Conteúdo da versão do produto
- * Requerimentos para integração com outras aplicações
- * Passo-a-passo para instalação do banco de dados
- * Estrutura de diretórios
- * Manual de configuração de ambiente
- * Scripts para inicialização
- * Manual de validação pós instalação"


102. Deve possuir manual operacional contendo detalhamento das operações de inicialização e parada do sistema, monitoramento, recuperação, controles, arquivamento, segurança e controle de acesso em Português (Brasil).

103. Deve possuir manual de usuário contendo informações para acesso ao sistema, navegação de telas e menus, relatórios existentes, workflow, mensagens de erro, entrada de dados, etc., em Português (Brasil).

6.22.12 Operações


104. Agendamento (Schedule) - Deve permitir o agendamento de execução de processos com facilidades de planejamento, monitoramento e realização de paradas preventivas e corretivas de sistema.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	19 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

105. Agendamento (Schedule) - Deve permitir a integração com softwares externos de controle de processos, em especial o TWS (Tivoli Workload Scheduler)
106. Deve garantir a consistência dos dados em situações normais e de falhas, permitindo desfazer transações incompletas, recuperar sistemas após ocorrência de falhas, evitar duplicidade de transações, mantendo registros adequados.
107. Deve prover informações suficientes para análise de falhas, permitindo realizar ações corretivas.
108. Controle de Eventos/Não-eventos - Deve gerar mensagens de estado de processamento online aos operadores, contemplando informações relativas aos jobs, e oferecer facilidades de reinicialização em casos de erros e falhas, a partir de um baseline de regras parametrizáveis.
109. Monitoramento e Alertas - Deve possuir um dashboard para monitorar os jobs em execução e agendados.
110. Monitoramento e Alertas - Permitir o envio de alertas e integração com ferramentas externas, preferencialmente o Zabbix.
111. Gerenciamento de Erros - Deve prover rotinas e documentação para gerenciamento de erros, além da manutenção de informações necessárias para a investigação de problemas ocorridos.
112. Roll back - Deve prover mecanismos para que transações possam ser desfeitas em casos de erros e/ou falhas de processamento, registrando o passo-a-passo da transação e controlando seu reproprocessamento de forma automática, sem perda de informações, nem problemas de integridade de dados.
113. Arquivamento e Recuperação - Deve oferecer facilidades de arquivamento e recuperação de arquivos de dados históricos, automático, baseado em critérios.
114. Auditabilidade e Rastreabilidade - Deve oferecer capacidade de registrar (logs) eventos ocorridos sobre sistemas, transações, parâmetros, contendo informações que garantam a auditabilidade e rastreabilidade das modificações feitas nesses elementos. Permite auditabilidade e rastreabilidade em diferentes níveis de detalhamento.
115. Auditabilidade e Rastreabilidade - Deve ser informado o nível de degradação de performance, caso seja utilizado o modo de auditoria mais detalhado em relação ao mais simples.
116. Produtividade - Deve oferecer estatísticas de uso de suas aplicações.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	20 de 42


 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

117. Sincronização de ambientes - Deve oferecer facilidades para promoção de versões de módulos e/ou configurações/parametrizações entre ambientes diferentes (homologação/pré-produção/produção).
118. Manutenção de dados - A base de dados do sistema deve ser aberta, permitindo a importação e exportação de dados de/para software externo.
119. Housekeeping - Deve ser possível realizar de forma automática a criação de base histórica e expurgo de dados, a partir de parâmetros configuráveis.
120. "Deve seguir a política de gestão de mudanças da CPFL para instalação de patches corretivos/evolutivos:
- Disponibilização de pacotes corretivos/evolutivos, com todas as documentações necessárias;
 - Confeção de documento de mudança, submissão do mesmo através do sistema de chamadas da CPFL e respeito aos protocolos de governança da empresa."
121. Os pacotes corretivos/evolutivos devem permitir a instalação automática, apenas com arquivos de parametrização editáveis.
122. Deve possibilitar a instalação de patches corretivos/evolutivos incrementais, sem necessidade de reinstalação/reinicialização de servidores.
123. Em caso de necessidade de disponibilização de aplicações em estações clientes, as atualizações de novas versões devem ser do tipo "automatic update", no momento de login do usuário na aplicação.
124. "A aplicação deve ser capaz de suportar e tratar Time Zones diferentes simultaneamente. A aplicação deve tomar como base a data e hora do servidor em que está instalada e não deve haver restrição quanto a sincronização de horário via NTP"
125. "Horário de Verão - A aplicação deve disponibilizar um mecanismo e/ou ferramenta para alteração da data e hora, devido a mudança do horário de verão, sem prejuízo para a aplicação, mantendo a integridade das informações, antes e após a mudança do horário. A aplicação deve tomar como base a data e hora do servidor em que está instalada."

6.22.13 Infraestrutura

126. "Hardware - Servidores

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	21 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

Detalhar a configuração (licenciamento, versionamento, compatibilidade etc.) mínima E ideal dos servidores (Hardware - CPUs, memória, storage, etc.) para o produto proposto, tendo como base o plano de crescimento da solução.

Não é necessário precificar os servidores.

Requerido suporte a servidores Intel em Blade"

127. "Hardware - Estação Cliente

Detalhar a configuração (licenciamento, versionamento, compatibilidade etc.) mínima E ideal das estações clientes (Hardware - CPUs, memória, storage,) para o produto proposto, tendo como base o plano de crescimento da solução.

Não é necessário precificar as estações clientes."

128. "Software - Servidores

Detalhar a necessidade de todos os softwares 'básicos' (Sistema Operacional, Application Servers, Web Servers, etc.) para os servidores do produto proposto - licenciamento, versionamento, compatibilidade, etc.

Não é necessário precificar as licenças dos softwares básicos.

Diretriz:

Sistema Operacional - Windows Server 2012

Web Server - IIS 7.5 ou superior"

129. "Software - Estação Cliente

Detalhar a necessidade de todos os softwares 'básicos' (Sistema Operacional, Browsers, Conectores clientes a banco de dados) para as estações clientes do produto proposto - licenciamento, versionamento, compatibilidade, etc.

Não é necessário precificar as licenças dos softwares básicos.

Preferência:

Sistema Operacional - Windows


Browser - Internet Explorer 9.0 ou superior"

130. "Computadores da equipe do projeto

O fornecedor deverá prover o hardware e software necessário para que seus colaboradores executem o serviço.

Qualquer necessidade que precise ser provida pela CPFL deverá ser expressa na proposta"

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	22 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

131. "Licenças

Detalhar a necessidade de licenciamento do(s) produto(s) proposto(s), tendo como base o plano de crescimento da CPFL (enviado na planilha de volumetria).

É necessário precificar as licenças do(s) produto(s) da seguinte forma:

- 1) Tomando como base a volumetria atual e esperada pela CPFL;
- 2) ULA (Unlimited License Agreement)"

132. "Ambientes

Detalhar as informações separadas por ambiente:

- 1) Desenvolvimento
- 2) Homologação/Treinamento
- 3) Pré-produção"

133. "Banco de dados

As bases de dados utilizadas pela solução devem ser Oracle 12c. O dimensionamento considerar como servidor de banco de dados o equipamento SUN M9K. Caso não seja possível atender este requisito, o fornecedor deverá informar neste ponto qual o banco de dados e versão que utiliza, bem como o custo e prazo necessário para adequar a solução ao banco de dados utilizado pela CPFL.

- Deve informar se há necessidade de outras features."

134. "Sistema Operacional x Aplicações

Os aplicativos deverão ser instalados em file systems distintos do file system onde está instalado o Sistema Operacional."

135. "Clusterização

Deve ser possível clusterizar o ambiente da solução. Os clusters deverão ser planejados entre equipamentos distintos."

136. "Storage


Deve ser possível utilizar a solução em arquitetura SAN (Storage Area Network), sem a necessidade de instalação de discos locais."

137. "Rede

Deve ser compatível com redes Gigabit e 10Gigabit Ethernet."

138. "Balanceamento / Distribuição de carga

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	23 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

Deve permitir o balanceamento de carga entre servidores através de appliances externos."

139. Virtualização

140. Deve possuir suporte a Thin client.

141. "Acesso remoto VPN

Deve suportar a conectividade de aplicações e componentes, permitindo o suporte da solução remotamente."

142. "Acesso através da Internet

Deve suportar o protocolo HTTPS ou outro protocolo seguro para conectividade de aplicações e componentes."

143. "Browsers

Todas as aplicações e interfaces web disponíveis na aplicação devem ser compatíveis com o Internet Explorer 9.0 ou superior. Outros devem ser mencionados se necessários com a respectiva justificativa."


6.22.2 Administração de Ambiente

1. Deve ser possível configurar o ambiente da aplicação. Detalhar as formas de configuração.
2. Deve ser possível monitorar o ambiente da aplicação a partir de métricas definidas pela CPFL e configuração de alarmes. Detalhar as formas de monitoração e configuração de alarmes.
3. Deve ser possível monitorar o ambiente da aplicação remotamente, via protocolos padrão de mercado. Detalhar a lista de protocolos disponíveis para monitoração remota.

6.22.3 Interoperabilidade e Integração

1. Integração SOA - Deve seguir os padrões de mercado com compatibilidade para comunicação com soluções ESB (Enterprise Service Bus) em especial, compatibilidade com SAP PI, SAP PO e interfaces SOAP Adapter.
2. Entregará especificação de todos os tipos/finalidade de integração entre os sistemas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	24 de 42


 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

3. Deve possuir controle para que transações não sejam processadas em duplicidade.
4. Deve permitir o monitoramento e análise de problemas relacionados às transações.
5. Deve seguir os padrões de OASIS e W3C para desenvolvimento de Web Services. Fornecer a lista de especificações suportadas (WS-*).
6. Deve possuir capacidade para utilizar um service registry para consultar os serviços através do protocolo UDDI (Universal Description Discovery and Integration).
7. Suporte ao protocolo REST.
8. Suporte estrutura de micro serviços.
9. Exposição de WebAPIs.

6.22.4 Interface para Usuários


1. Deve permitir a utilização de campos com valores default facilmente configuráveis, de forma a agilizar a entrada de dados.
2. Deve permitir a utilização de campos preenchíveis a partir de tabelas de valores configuráveis (look up tables).
3. Deve possuir a facilidade de seleção a partir de listas filtradas a partir de digitação parcial do texto.
4. Deve possuir diferenciação entre campos de preenchimento obrigatório e opcional.
5. Deve permitir a possibilidade de configuração de campos quanto à obrigatoriedade de preenchimento, sem necessidade de alteração de código.
6. Deve possuir a diferenciação entre campos digitáveis e campos apenas informativos.
7. Deve possuir preenchimento inteligente, facilidades de copy and paste e de undo/redo.
8. Deve possuir menu de funções amigáveis e autoexplicativos.
9. Deve permitir o transporte entre telas das informações comuns, evitando redigitação.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	25 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

10. Deve permitir o acesso às transações online do sistema através de navegadores (browsers) padrões de mercado.
11. Campos de listas com apenas uma ocorrência válida deverão ser apresentados automaticamente na tela.
12. Deve permitir a navegação entre campos nas telas através de TAB ou de teclas de função.
13. Acesso de atendentes (CSR's) a aplicações de terceiros através de "janelas" em sua tela principal (em contexto).
14. Deve possuir internacionalização de funcionalidades (idioma e regionalização - moeda), com possibilidade de utilização em mais de um local definido no momento do login.
15. Deve possuir menus e interfaces em português (Brasil).
16. Possibilidade de criação de dicionário personalizado, respeitando requisitos de internacionalização
17. Deve permitir a paginação e ordenação de registros, de maneira configurável
18. Deve oferecer facilidades de atalhos para funcionalidades muito utilizadas.
19. Permitir configuração do layout gráfico. Fornece documentação dos mecanismos de gerenciamento de layout gráfico.
20. Deve oferecer facilidades de ajuda (help) sensível ao contexto, utilizando a internacionalização de acordo com o requisito.
21. Deve oferecer facilidades de configuração das mensagens de erro apresentadas, utilizando a internacionalização de acordo com o requisito.
22. Deve permitir a exposição de serviços de apresentação (Portlets Remotos) caso seja especificado nos requisitos funcionais a necessidade de expor informações para outros sistemas.
23. Especificar quais os tipos de interface e suas tecnologias em cada módulo do produto.
24. Acessibilidade - Deve possuir interfaces que sigam o padrão WCAG 2.0 definido pelo W3C (www.w3c.org). Detalhar as interfaces que seguem este padrão.
25. Caso não seja necessário para atender algum requisito de negócio compatibilidade com versões de navegadores antigos e houver interfaces Web, as páginas devem ser desenvolvidas com HTML5 a fim de garantir compatibilidade com diversos navegadores e plataformas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	26 de 42


 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

26. Caso haja interfaces Web, devem ser desenvolvidas de forma responsiva que atenda às necessidades de negócio de forma dinâmica.
27. Caso haja interfaces Web, devem ser desenvolvidas de forma a tornar possível a visualização do conteúdo tanto em desktops como em dispositivos móveis (Tables e smartphones). De forma que o conteúdo da página de adequa às limitações do dispositivo o mínimo suficiente para que as operações possam ser executadas nos mesmos, exceto se houver requisito de negócio de defina de forma mais específica a interface.
28. O sistema não deve fazer uso de pop-ups em janelas separadas. Quando for necessário deverá utilizar players HTML para exibição de mensagens.
29. Não deve possuir recursos (telas, formulários, gráficos) em Adobe Flash.

6.22.5 Geral


1. Aderência à Política da CPFL - a ser validada em conjunto com a TI da empresa nas reuniões preliminares.
2. Controle de Acesso de Usuários - Deve oferecer controle de acessos em diferentes níveis através do registro de identificação o usuário, operação realizada e data. Deve permitir a integração com ferramenta de gestão de identidades externa. Deve assegurar regras de segregação de função, a fim de evitar fraudes.
3. Desejável que permita a integração com ferramenta de gestão de identidades externa (IDM).
4. Deve oferecer controle de acesso aos dados através do registro de identificação do usuário, operação realizada e data.
5. Deve restringir o acesso a dados sensíveis.
6. Deve gerar registros (logs) de operações realizadas.
7. Deve ser compatível e integrável com as melhores soluções de SIEM do mercado.
8. Manutenção de usuários - Deve possuir funcionalidade para criação, alteração, exclusão e consulta de "logins" de acesso, permitindo: Cadastramento de um único usuário, caso não seja possível integrar com o AD. Cadastramento de múltiplos usuários. Estas funcionalidades devem ser disponibilizadas para chamadas externas, pois estas ações, em geral, serão realizadas pelo Gerenciador de Identidades da CPFL.
9. Deverá permitir a integração com o Gerenciador de Identidades a fim de permitir as ações supracitadas através desta ferramenta.
10. Deve permitir a manutenção de Perfis.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	27 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

11. Autenticação do usuário - A autenticação do usuário deverá ser feita via LDAPS no Active Directory da Microsoft.
12. Ser compatível e integrável com as melhores soluções de duplo fator de autenticação.
13. Controle de Acessos - Os acessos às informações deverão ser feitos sempre, obrigatoriamente, via aplicação, obedecendo os respectivos perfis de acesso. RBAC (role-based access control).
14. Armazenamento da informação - Toda informação deverá ser armazenada em Banco de Dados. As informações devem ser armazenadas de forma segura, garantindo a disponibilidade, integridade e confiabilidade.
15. Senha CASE SENSITIVE - Deverá permitir a utilização de Caracteres obrigatórios conforme checklist de segurança da informação.
16. Não deve necessitar de senha de administrador de Banco ou sistema Operacional para funcionamento.
17. Conexão segura - Transações realizadas via Intranet ou Internet utilizando conexão segura, no padrão https (128 bits), principalmente para informações de login, senhas e mecanismos que dificultem ataques de força bruta.
18. Integração com repositório de autenticação - Deve ser possível integrar com o Active Directory, via DNS. Permitindo assim, redundância no momento da autenticação.
19. Deve garantir proteção contra as principais técnicas de invasão de sistemas. Os principais e mais comuns podem ser conhecidos através do site <https://www.owasp.org>.
20. Deve permitir a configuração de "Time-out" de sessão, caso o usuário não realize operações no seu browser em intervalo de tempo.
21. A solução poderá ser submetida a testes de segurança com ferramentas de vulnerabilidades. O resultado da análise poderá impedir a entrega da solução em produção até a regularização do apontamento.
22. Deve ser aderente a LGPD - Lei Geral de Proteção de Dados, se aplicável.
23. No caso de não integração com AD, a senha deverá ter um tamanho mínimo de 8 caracteres, sem restrição no tamanho máximo, exigindo uma complexidade mínima na senha e não permitindo a repetição das última 5 senhas usadas.
24. Caso a solução possua tela de login, deve possuir captcha e mecanismo para mitigar ferramentas brute-force.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	28 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

25. Não deve necessitar ou fazer uso de protocolos considerados inseguros como Telnet ou FTP.
26. Caso exista suporte remoto, deve ser realizado obrigatoriamente por conexão VPN site-to-site.
27. Deve disponibilizar patches e hotfix de segurança para correções de vulnerabilidades identificadas com qualquer CVE/CVSS.
28. Caso a solução possua trilha de auditoria, a mesma deve ser protegida de tal forma que seus dados não possam ser alterados.
29. A solução não deve possuir recursos técnicos que permitam a manutenção ou consulta direta ao banco de dados através de queries. Todo acesso ao banco de dados deve ser feito apenas por interfaces específicas para a função.
30. A solução não deve expor em arquivos de configuração nenhum usuário/senha utilizada na solução.
31. Mecanismos de atualização de usuários e senha. A solução não deve ter usuários e senhas armazenados de forma hardcoded. Deve prover mecanismos onde a própria equipe da CPFL possa trocar usuários usados na aplicação sem recompilação de código, isso deve observar o requisito de criptografia acima.


6.22.6 Criptografia

1. Deve utilizar um algoritmo de criptografia padrão de mercado ao invés de criar uma solução própria.
2. Deve ser possível cifrar todos os dados considerados confidenciais.
3. Todas as senhas devem ser armazenadas em formato de hash com salt, nunca a senha original (mesmo que criptografada).

6.22.7 Segurança de Aplicação

1. Single Sign On de usuário - Deve permitir autenticação de usuários através da autenticação integrada do Windows ou caso haja integração com sistemas específicos será necessário detalhar o protocolo correspondente.
2. Segurança de Serviços - Deve permitir autenticação e autorização de serviços expostos para garantia que somente usuários e/ou aplicações autorizados acessar recursos. Fornecer a lista de formas de autenticação e autorização disponível e possível.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	29 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

3. Autorização de usuário - Deve permitir integração com uma ferramenta de controle de políticas de segurança.

6.22.8 Gerenciamento de Dados

1. Gerenciamento de transações - Deve suportar a execução de transações de dados ad hoc para acesso aos dados armazenados no banco de dados, através de scripts parametrizáveis, armazenáveis e reutilizáveis, cujos resultados podem ser compartilhados com usuários autorizados.
2. Controle de transações - Deve oferecer controles que permitam a gestão de transações ofensoras da performance ou integridade do sistema.
3. Interface gráfica - Deve oferecer uma interface gráfica para construção, submissão, acompanhamento da execução e visualização de resultados de transações.
4. Disponibilização de dados - Oferecer ferramenta de extração de dados para disponibilização a outros sistemas.
5. Disponibilização de dados - Permitir a extração de dados através de outras ferramentas de mercado. Detalhar quais ferramentas e/ou tecnologias de mercado são suportadas.


6.22.9 Desempenho e Volumetria

1. Deve especificar o volume de transações e o respectivo desempenho baseado nos requisitos funcionais, assim como os pontos de quebra desse desempenho que exigirão revisão na infraestrutura
2. Tráfego máximo permitido por página web de 200KB.

6.22.10 Documentação

1. Fornece documentação sobre a arquitetura aplicativa, incluindo, mas não se limitando a:
 - * Desenho da arquitetura aplicativa e integrações;
 - * Especificações e Dicionário de bancos de dados;
 - * Diagrama de entidade-relacionamento;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	30 de 42


 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

- * Leiaute de arquivos internos;
 - * Desenho de telas;
 - * Fluxograma do sistema;
 - * Descrição dos Problemas mais comuns e guia de resolução (Troubleshooting)"
2. "Deve possuir manual de instalação, operação e manutenção do sistema incluindo, mas não se limitando a:
 - * Conteúdo da versão do produto
 - * Requerimentos para integração com outras aplicações
 - * Passo-a-passo para instalação do banco de dados
 - * Estrutura de diretórios
 - * Manual de configuração de ambiente
 - * Scripts para inicialização
 - * Manual de validação pós instalação"
 3. Deve possuir manual operacional contendo detalhamento das operações de inicialização e parada do sistema, monitoramento, recuperação, controles, arquivamento, segurança e controle de acesso em português (Brasil).
 4. Deve possuir manual de usuário contendo informações para acesso ao sistema, navegação de telas e menus, relatórios existentes, workflow, mensagens de erro, entrada de dados etc., em português (Brasil).

6.22.11 Operações


1. Agendamento (Schedule) - Deve permitir o agendamento de execução de processos com facilidades de planejamento, monitoramento e realização de paradas preventivas e corretivas de sistema.
2. Agendamento (Schedule) - Deve permitir a integração com softwares externos de controle de processos, em especial o TWS (Tivoli Workload Scheduler)
3. Deve garantir a consistência dos dados em situações normais e de falhas, permitindo desfazer transações incompletas, recuperar sistemas após ocorrência de falhas, evitar duplicidade de transações, mantendo registros adequados.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	31 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

4. Deve prover informações suficientes para análise de falhas, permitindo realizar ações corretivas.
5. Controle de Eventos/Não-eventos - Deve gerar mensagens de estado de processamento online aos operadores, contemplando informações relativas aos jobs, e oferecer facilidades de reinicialização em casos de erros e falhas, a partir de um baseline de regras parametrizáveis.
6. Monitoramento e Alertas - Deve possuir um dashboard para monitorar os jobs em execução e agendados.
7. Monitoramento e Alertas - Permitir o envio de alertas e integração com ferramentas externas, preferencialmente o Zabbix
8. Gerenciamento de Erros - Deve prover rotinas e documentação para gerenciamento de erros, além da manutenção de informações necessárias para a investigação de problemas ocorridos.
9. Roll back - Deve prover mecanismos para que transações possam ser desfeitas em casos de erros e/ou falhas de processamento, registrando o passo-a-passo da transação e controlando seu reproprocessamento de forma automática, sem perda de informações, nem problemas de integridade de dados.
10. Arquivamento e Recuperação - Deve oferecer facilidades de arquivamento e recuperação de arquivos de dados históricos, automático, baseado em critérios.
11. Auditabilidade e Rastreabilidade - Deve oferecer capacidade de registrar (logs) eventos ocorridos sobre sistemas, transações, parâmetros, contendo informações que garantam a auditabilidade e rastreabilidade das modificações feitas nesses elementos. Permite auditabilidade e rastreabilidade em diferentes níveis de detalhamento.
12. Auditabilidade e Rastreabilidade - Deve ser informado o nível de degradação de performance, caso seja utilizado o modo de auditoria mais detalhado em relação ao mais simples.
13. Produtividade - Deve oferecer estatísticas de uso de suas aplicações.
14. Sincronização de ambientes - Deve oferecer facilidades para promoção de versões de módulos e/ou configurações/parametrizações entre ambientes diferentes (homologação/pré-produção/produção).
15. Manutenção de dados - A base de dados do sistema deve ser aberta, permitindo a importação e exportação de dados de/para software externo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	32 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

16. Housekeeping - Deve ser possível realizar de forma automática a criação de base histórica e expurgo de dados, a partir de parâmetros configuráveis.
17. Deve seguir a política de gestão de mudanças da CPFL para instalação de patches corretivos/evolutivos:
 - Disponibilização de pacotes corretivos/evolutivos, com todas as documentações necessárias;
 - Confeção de documento de mudança, submissão do mesmo através do sistema de chamadas da CPFL e respeito aos protocolos de governança da empresa."
18. Os pacotes corretivos/evolutivos devem permitir a instalação automática, apenas com arquivos de parametrização editáveis.
19. Deve possibilitar a instalação de patches corretivos/evolutivos incrementais, sem necessidade de reinstalação/reinicialização de servidores.
20. Em caso de necessidade de disponibilização de aplicações em estações clientes, as atualizações de novas versões devem ser do tipo "automatic update", no momento de login do usuário na aplicação.
21. A aplicação deve ser capaz de suportar e tratar Time Zones diferentes simultaneamente. A aplicação deve tomar como base a data e hora do servidor em que está instalada e não deve haver restrição quanto a sincronização de horário via NTP.


Horário de Verão - A aplicação deve disponibilizar um mecanismo e/ou ferramenta para alteração da data e hora, devido a mudança do horário de verão, sem prejuízo para a aplicação, mantendo a integridade das informações, antes e após a mudança do horário. A aplicação deve tomar como base a data e hora do servidor em que está instalada.

6.22.12 Infraestrutura

1. Hardware - Servidores

- * Detalhar a configuração (licenciamento, versionamento, compatibilidade, etc.) mínima E ideal dos servidores (Hardware - CPUs, memória, storage, etc.) para o produto proposto, tendo como base o plano de crescimento da solução.
- * Não é necessário precificar os servidores.
- * Requerido suporte a servidores Intel em Blade"

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	33 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

2. Hardware - Estação Cliente. Detalhar a configuração (licenciamento, versionamento, compatibilidade etc.) mínima E ideal das estações clientes (Hardware - CPUs, memória, storage,) para o produto proposto, tendo como base o plano de crescimento da solução. Não é necessário precificar as estações clientes."

3. Software – Servidores. Detalhar a necessidade de todos os softwares 'básicos' (Sistema Operacional, Application Servidores, Web Servers, etc.) para os servidores do produto proposto - licenciamento, versionamento, compatibilidade, etc. Não é necessário precificar as licenças dos softwares básicos.

Diretriz: Sistema Operacional - Windows Server 2012. Web Server - IIS 7.5 ou superior"

4. Software - Estação Cliente. Detalhar a necessidade de todos os softwares 'básicos' (Sistema Operacional, Browsers, Conectores clientes a banco de dados) para as estações clientes do produto proposto - licenciamento, versionamento, compatibilidade etc. Não é necessário precificar as licenças dos softwares básicos.

Preferência: Sistema Operacional – Windows. Browser - Internet Explorer 9.0 ou superior"

5. Computadores da equipe do projeto. O fornecedor deverá prover o hardware e software necessário para que seus colaboradores executem o serviço. Qualquer necessidade que precise ser provida pela CPFL deverá ser expressa na proposta"

6. Licenças. Detalhar a necessidade de licenciamento do(s) produto(s) proposto(s), tendo como base o plano de crescimento da CPFL (enviado na planilha de volumetria). É necessário precificar as licenças do(s) produto(s) da seguinte forma:


- 1) Tomando como base a volumetria atual e esperada pela CPFL;
- 2) ULA (Unlimited License Agreement)";

7. Ambientes. Detalhar as informações separadas por ambiente:

- 1) Desenvolvimento
- 2) Homologação/Treinamento
- 3) Pré-produção"

8. Banco de Dados. As bases de dados utilizadas pela solução devem ser Oracle 12c. O dimensionamento considerar como servidor de banco de dados o equipamento SUN M9K. Caso não seja possível atender este requisito, o fornecedor deverá informar neste ponto qual o banco de dados e versão que utiliza, bem como o custo e prazo necessário para adequar a solução ao banco de dados utilizado pela CPFL.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	34 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

- Deve informar se há necessidade de outras features."

9. Sistema Operacional x Aplicações. Os aplicativos deverão ser instalados em file systems distintos do filesystem onde está instalado o Sistema Operacional."
10. Clusterização. Deve ser possível clusterizar o ambiente da solução. Os clusters deverão ser planejados entre equipamentos distintos."
11. Storage. Deve ser possível utilizar a solução em arquitetura SAN (Storage Area Network), sem a necessidade de instalação de discos locais."
12. Rede. Deve ser compatível com redes Gigabit e 10Gigabit Ethernet."
13. Balanceamento / Distribuição de carga. Deve permitir o balanceamento de carga entre servidores através de appliances externos."
14. Virtualização. Deve possuir suporte a Thin client.
15. Acesso remoto VPN. Deve suportar a conectividade de aplicações e componentes, permitindo o suporte da solução remotamente."
16. Acesso através da Internet. Deve suportar o protocolo HTTPS ou outro protocolo seguro para conectividade de aplicações e componentes."
17. Browsers. Todas as aplicações e interfaces web disponíveis na aplicação devem ser compatíveis com o Internet Explorer 9.0 ou superior. Outros devem ser mencionados se necessários com a respectiva justificativa."


6.23 Matriz de Conformidade - Requisitos Não Funcionais - Gestão

6.23.1. Documentos e Manuais

1. Os treinamentos deverão ser conduzidos, bem como o material disponibilizado em português. Detalhar os treinamentos disponíveis e a metodologia.
2. Os treinamentos deverão ocorrer em português, nas dependências da CPFL em Campinas em horário comercial.
3. Detalhar se os materiais de treinamento poderão ser modificados para atender as especificidades da CPFL.
4. A proponente deve informar os tipos de manuais impressos e/ou eletrônicos que acompanham os treinamentos.
5. O PROPONENTE deve encaminhar o conteúdo programático dos treinamentos que serão ministrados na CPFL.

6.23.2. Conteúdo dos treinamentos

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	35 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

6. O conteúdo do treinamento deverá ser customizado para atender os públicos e o novo modelo operacional. O treinamento deve ser preferencialmente hands-on.
7. O fornecedor deve considerar para cada frente do projeto, no mínimo, os seguintes treinamentos:
8. 1) Usuários/Analistas de Negócio:
9. O PROPONENTE deve considerar treinamento técnico suficiente para a operação diária do sistema, visando capacitá-los a realizar a gestão dos processos das aplicações, realizar suporte básico aos usuários e checar o perfeito funcionamento das rotinas e dos processos implementados/modificados.
10. O PROPONENTE deve utilizar o ambiente de Qualidade (configurado, customizado e com os dados históricos migrados) para execução do treinamento, pelo qual deve ser Hand-on.
11. Estima-se que cerca de 30 pessoas com esse perfil serão treinadas.
12. Após o treinamento será preenchido uma avaliação de reação pela equipe da CPFL, sendo que o índice de aprovação deve ser superior a 80%.

6.23.3. Metodologia


13. O proponente é responsável por apresentar padrões e metodologias de testes que possui atualmente, incluindo e não limitado a funcionalidades existentes, novas funcionalidades requeridas, testes de stress, backup/recover.
14. O fornecedor deverá adaptar sua metodologia de testes para o padrão da CPFL.

6.23.4. Testes Unitários

15. O fornecedor é responsável pela execução dos testes unitários em todos os sistemas implementados/modificados durante o projeto.
16. O fornecedor deverá apresentar o plano e testes unitários, bem como todos os cenários de testes para a aprovação da CPFL.
17. Deverá ser apresentado as evidências de sucesso dos testes unitários para aprovação da CPFL.

6.23.5. Testes Integrados TI

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	36 de 42

 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

18.O fornecedor é responsável pela execução de um ciclo de testes integrados de TI em todos os sistemas implementados/modificados durante o projeto, visando minimizar os erros de integração entre os sistemas.

19.Esses testes visão também validar a conectividade entre as soluções integradas.

20.O fornecedor deverá apresentar o plano e testes integrados de TI, bem como todos os cenários de testes para a aprovação da CPFL.

21.O fornecedor deverá informar no cronograma Macro e detalhado o período de testes de Integrados de TI

22.Deverá ser apresentado as evidências de sucesso dos testes integrados de TI para aprovação da CPFL.

23.Realizar homologação de testes em conjunto com o Printcenter.

6.23.6. Testes de Stress

24.O fornecedor é responsável pela execução de um ciclo de testes de Stress em todos os sistemas implementados/modificados durante o projeto, visando minimizar os erros de integração entre os sistemas.

25.Esses testes visão também validar a conectividade entre as soluções integradas.

26.O fornecedor deverá apresentar o plano e testes de Stress, bem como todos os cenários de testes para a aprovação da CPFL.

27.O fornecedor deverá informar no cronograma Macro e detalhado o período De testes de Stress

28.Deverá ser apresentado as evidências de sucesso dos testes de Stress para aprovação da CPFL.

29.Estes testes serão acompanhados e definidos em conjunto com a equipe de TI da CPFL.


30.O PROPONENTE será responsável por executar um ciclo de testes de stress em cada interface ajustada ou reimplementada durante o projeto.

6.23.7. Testes Integrados de Negócio

31.O fornecedor será responsável por suportar presencialmente a equipe de testes, além de corrigir erros/problemas encontrados durante essa fase.

32.Deve ser considerado a realização de 2 ciclos de testes integrados de Negócio

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	37 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

33.O Ciclo de testes será encerrado apenas mediante a finalização de todos os testes e a correção de todos os incidentes abertos durante o ciclo.

6.23.8. Testes de Aceitação (UAT)

34.O fornecedor será responsável por suportar presencialmente a equipe de testes, além de corrigir erros/problemas encontrados durante essa fase.

35.Será realizado um ciclo de testes de aceitação.

6.23.9. Gestão dos Testes

36.O PROPONENTE deve suportar a equipe CPFL na elaboração dos planos de testes, bem como prover os cenários de testes que o fornecedor julgue necessário serem testados.

37.O PROPONENTE deverá descrever a estratégia, a metodologia e ferramentas utilizadas nas etapas de teste, contemplando testes unitários, testes integrados e processos de homologação tanto para o software “padrão” configurado para a CPFL, quanto para novos desenvolvimentos (de novas funcionalidades, interfaces e rotinas de carga de dados).

38.Uma equipe do proponente deverá coordenar e executar, com a participação das áreas usuárias e de TI, todas as etapas de testes na implantação de novas soluções de software, atendendo a todos os padrões da metodologia da CPFL.


6.23.10. Time do Fornecedor

39.O fornecedor deverá alocar Especialistas técnicos para realizar o processo de "Retrofit" entre os ambientes de Desenvolvimento e Qualidade (projetos e sustain), referente a todas as tecnologias descritas nessa proposta, como por exemplo, o SAP ECC.

6.23.11. Transferência de Conhecimento

40.O fornecedor será responsável por realizar a transferência de conhecimento para os times de sustentação da CPFL.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	38 de 42

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

41.Toda a transferência de conhecimento deverá ser formalizada através de atas e termo de aceite do KT (knowlogement Transfer).


6.23.12. Estimativa de Prazo e Custos

42.O Fornecedor deverá enviar para a CPFL uma proposta Técnica contendo o prazo de implementação do projeto para os seguintes Cenários:

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Orientações técnicas para Cloud Computing	Eletrônico (GED)	Restrição de Acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	39 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

8. ANEXOS

Anexo 01 – CPFL Requisitos Não Funcionais SaaS

Segurança em Projetos Requisitos Não Funcionais - (SaaS)							
ID	Fronte	Macro Requisito	Requisito	Requisito Imprescindível, importante ou desejável	Requisito funcional ou não funcional	Resposta do Avaliado	Comentários do Fornecedor
1				Eligibilidade do Requisito	Categoria	1 - Atende 0 - Não Atende 0,5 - Atende Parcialmente	
1.1	Desenho Geral da Arquitetura	Modelagem de arquitetura	Apresentar o desenho da arquitetura macro da solução contemplando todos os módulos envolvidos, integrações, conexões e protocolos. Principalmente contendo os pontos de exposição de serviços e integração com sistemas da CPFL.	Imprescindível	Não Funcional - Arquitetura		
1.2	Desenho Geral da Arquitetura	Produto Escalável	Produto Escalável - Deve suportar o crescimento de negócio e utilização de ferramenta sem impactos de performance. Descrever os mecanismos da solução para atender a esse requisito.	Imprescindível	Não Funcional - Escalabilidade		
1.3	Desenho Geral da Arquitetura	Exposição de Funcionalidades	Exposição de funcionalidades - Deve possuir APIs expostas via web services para integração com aplicações externas.	Importante	Não Funcional - Arquitetura		
1.4	Desenho Geral da Arquitetura	Ferramentas e Formas De Customizações / Configurações / Parametrizações	Detalhar as ferramentas e formas de customizações / configurações / parametrizações - Listar quais ferramentas e formas de customizações, configurações e parametrizações.	Importante	Não Funcional - Operação		
1.5	Desenho Geral da Arquitetura	Logs	Logs - Deve permitir a criação de logs, e fornecer mecanismos para seu acesso e configuração. Detalhar os tipos de log e seus mecanismos de gerenciamento. Os logs precisam ser mantidos por pelo menos 90 dias.	Importante	Não Funcional - Operação		
1.6	Desenho Geral da Arquitetura	Extensibilidade futura Do Sistema	Extensibilidade futura do sistema - Deve ser atualizável e informado o roadmap de evolução. As atualizações serão feitas diretamente pelo fornecedor da solução e não deverá incidir em indisponibilidade da solução.	Importante	Não Funcional - Arquitetura		
1.7	Desenho Geral da Arquitetura	Analytics	A solução deve fornecer formas de extração de dados a fim de serem extraídos, transformados e carregados para soluções analíticas da CPFL. Necessário detalhar os mecanismos que fornece dados armazenados, Near-Real-Time e/ou Real-Time.	Importante	Não Funcional - Arquitetura		
1.8	Propriedade	Propriedade dos dados	Todos os dados da aplicação são de propriedade da CPFL e portanto ela tem o direito de extrair seus dados a qualquer momento. A solução deverá prover o mecanismo que a CPFL poderá utilizar para essa extração.	Imprescindível	Não Funcional - Arquitetura		
2							
2.1	Interoperabilidade e Integração	Integração SOA	Integração SOA - Deve seguir os padrões de mercado com compatibilidade para comunicação com soluções ESB (Enterprise Service Bus) em especial, compatibilidade com SAP FI, SAP PO e interfaces SOAP Adapter.	Importante	Não Funcional - Arquitetura		
2.2	Interoperabilidade e Integração	Padrões de Integração	Deve seguir os padrões de OASIS e W3C para desenvolvimento de Web Services. Fornecer a lista de especificações suportadas (WS-*)	Desejável	Não Funcional - Arquitetura		
2.3	Interoperabilidade e Integração	Service Registry	Deve possuir capacidade para utilizar um service registry para consultar os serviços através do protocolo UDDI (Universal Description Discovery and Integration)	Desejável	Não Funcional - Arquitetura		
2.4	Interoperabilidade e Integração	Segurança	As interfaces devem ser protegidas por mecanismos de autenticação. Os mecanismos suportados deverão ser descritos na proposta	Imprescindível	Não Funcional - Arquitetura		


Anexo 02 – CPFL Requisitos Não Funcionais On-Premises

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	40 de 42





Tipo de Documento:	Procedimento
Área de Aplicação:	Tecnologia de Informação
Título do Documento:	Requisitos de Segurança para Projetos

CPFL Energia		Segurança em Projetos		O Fim do Escopo		O Não Atendido	O Não Atendido	O Não Atendido
Requisitos Não Funcionais - (On Premise)		Requisitos		Desvio do Escopo		Atendimentos	Atendimentos	Atendimentos
ID	Evento	Matriz Requisitos	Requisito	Exemplo		Exemplo	Exemplo	Exemplo
1	Arquitetura	Desenho geral da arquitetura	Produto Modular: Deve ser baseado em um "core" que é atualizado via librerias de versões de produtos. Qualquer customização deve ser criada fora do "core" da aplicação, ou integrado a uma outra instância.	A solução deve ser baseada em módulos para que a CPFL possa escolher as componentes, e requisitos conforme as necessidades atuais e futuras.				
2	Arquitetura	Desenho geral da arquitetura	Produto Facilitar: Deve suportar clonagem e load balancing para atender o crescimento de requisições e utilização de ferramenta.	Crescimento deve ser baseado em análise de crescimento que deve acompanhar documentação de utilização.				
3	Arquitetura	Desenho geral da arquitetura	Produto Multi-Instância: Deve ser possível a conexão com outras soluções que se encontrem em multi-instâncias.	Integração do Billing e/ou Catálogo com o sistema da CPFL, eventualmente separados em diferentes instâncias.				
4	Arquitetura	Desenho geral da arquitetura	Deve possuir Arquitetura Aberta, não utilizando soluções de arquitetura proprietárias de fornecedores.	A solução deve utilizar padrões de mercado.				
5	Arquitetura	Desenho geral da arquitetura	Exposição de funcionalidades: Deve possuir API's expostas via web services para integração com aplicações externas.					
6	Arquitetura	Desenho geral da arquitetura	Mecanismos de cache: Deve possuir mecanismos para armazenar informações em memória. Exatidão e lista de mecanismos e suas formas de gerenciamento operacional.					
7	Arquitetura	Desenho geral da arquitetura	Linguagens de Programação: Especificar as linguagens de programação e versões utilizadas pelos módulos de produtos e integrações. O padrão de arquitetura da CPFL define a solução para plataforma Microsoft .NET Framework 4. Qualquer proposta diferente deve ser submetida à CPFL para uma aprovação formal.	Módulo de Imprimido: Microsoft .NET, C#, Componentes .NET				
8	Arquitetura	Desenho geral da arquitetura	Ferramentas e formas de customizações / configurações / parametrizações: Listar quais ferramentas e formas de customizações, configurações e parametrizações.	Configuração de Database Remota através de interface Web; Configuração dos diretórios da aplicação em tabelas do Banco de Dados, executadas por scripts.				
9	Arquitetura	Desenho geral da arquitetura	Adaptabilidade, Flexibilidade e Time-to-market: Deve ser customizável e flexível através de configurações/parametrizações, sem necessidade de alteração de código. Exatidão e utilização de ferramentas de configuração/parametrização e configuração.	Configurações de planos tarifários através de interface Web; Configuração de dados de valores de produtos e descontos.				
10	Arquitetura	Desenho geral da arquitetura	Logs: Deve permitir a criação de logs, e armazenar mecanismos para seu acesso e configuração. Detalhar os tipos de logs e seus mecanismos de gerenciamento. Os logs precisam ser mantidos por pelo menos 90 dias.	Configuração do padrão de nomenclatura dos arquivos; diretório de geração; Tabelas de logs de execução, visualização dos arquivos via interface web.				
11	Arquitetura	Desenho geral da arquitetura	Escalabilidade futura do sistema: Deve ser atualizável e informado o roadmap de evolução.	Atualização e mudanças legais, regulatórias, melhores práticas de mercado e atualizações tecnológicas, como evolução de plataformas de hardware, sistemas operacionais e novos tecnologias.				
12	Arquitetura	Desenho geral da arquitetura	Deve possuir módulos de processamento batch e online. O processamento em batch não pode impactar na disponibilidade de performance de processos online.	Execução de processos de Tratamento em paralelo a administração do cliente, não deve impactar a performance.				
13	Arquitetura	Desenho geral da arquitetura	Paralelismo de processamento: Deve permitir a execução e o controle dos processos paralelos. (Distribuído e Batch)	Controle Dashboard de execução dos processos em execução. Consultas através de Web Service.				
14	Arquitetura	Desenho geral da arquitetura	Suporte a containers: A aplicação deve suportar ser executada em containers, porém não deve ser mandatória. Fica a critério da CPFL a melhor estrutura a aplicar	Suporte a Docker no outro container de mercado				
15	Arquitetura	Administração de Ambiente	Deve ser possível configurar o ambiente de aplicação. Detalhar as formas de configuração.	Configuração do pool de conexão com banco de dados, conexão com Active Directory.				
16	Arquitetura	Administração de Ambiente	Deve ser possível monitorar o ambiente da aplicação a partir de métricas definidas pela CPFL e configuração de alarmes. Detalhar as formas de monitoragem e configuração de alarmes.	Monitoragem de métricas de conexão com banco de dados, geração de alertas e envio a sistema de monitoramento através de um protocolo padronizado.				
17	Arquitetura	Administração de Ambiente	Deve ser possível monitorar o ambiente da aplicação remotamente, via protocolos padrão de mercado. Detalhar a lista de protocolos disponíveis para monitoragem remota.	Monitoragem de eventos de falhas externas, utilizando protocolos de mercado (SNMP, SMTP, etc.).				
18	Integração	Interoperabilidade e Integração	Integração SOAP: Deve seguir os padrões de mercado e não consistibilidade para comunicação com soluções ESB (Enterprise Service Bus) ou especial, compatibilizado com SOAP 1.1, SOAP 1.2 e serviços SOAP Restless.					
19	Integração	Interoperabilidade e Integração	Integração especificação de todos os tipos/formulário de integração entre os sistemas.	Ex: Integração pontual para replicação de informações.				
20	Integração	Interoperabilidade e Integração	Deve possuir controle para que transações não sejam processadas em duplicidade.					
21	Integração	Interoperabilidade e Integração	Deve permitir o monitoramento e análise de problemas relacionados às transações.					
22	Integração	Interoperabilidade e Integração	Deve seguir os padrões de OASIS e W3C para desenvolvimento de Web Services. Fornecer a lista de especificações suportadas (SOAP).					
23	Integração	Interoperabilidade e Integração	Deve possuir capacidade para utilizar um service registry para consultar os serviços através de protocolos ISO (Universal Description Discovery and Integration)					
24	Integração	Interoperabilidade e Integração	Exatidão e protocolos REST					
25	Integração	Interoperabilidade e Integração	Exatidão e estruturas de microserviços					

 Segurança em Projetos Assunto: Requisitos Não Funcionais - Gestão		O-Fore do Escopo 1-Dentro do Escopo	O-Atende ao Escopo 2-Atende Totalmente	O-Atende 1-Atende Parcialmente 2-Atende Totalmente	O-Atende 1-Atende Parcialmente 2-Atende Totalmente	O-Atende 1-Atende Parcialmente 2-Atende Totalmente	O-Atende 1-Atende Parcialmente 2-Atende Totalmente	O-Atende 1-Atende Parcialmente 2-Atende Totalmente
ID	Fronte	Matriz Requisitos	Requisito	Escopo	Atendimento	Atendimento	Atendimento	Atendimento
1	Treinamento	Documentos e Manuais	Os treinamentos deverão ser conduzidos, bem como o material disponibilizado em Português. Deixar os treinamentos disponíveis e as metodologias.					
2	Treinamento	Documentos e Manuais	Os treinamentos deverão ocorrer em português, nas dependências da CPFL, em Campinas em horário comercial.					
3	Treinamento	Documentos e Manuais	Detalhar e os materiais de treinamento poderão ser modificados para atender as especificidades da CPFL.					
4	Treinamento	Documentos e Manuais	A proponente deve informar os tipos de manuais impressos e/ou eletrônicos que acompanharão os treinamentos.					
5	Treinamento	Documentos e Manuais	O PROPONENTE deve encaminhar o conteúdo programático dos treinamentos que serão ministrados na CPFL.					
6	Treinamento	Conteúdo dos Treinamentos	O conteúdo do treinamento deverá ser customizado para atender os públicos e o novo modelo operacional. O treinamento deve ser preferencialmente hands-on.					
7	Treinamento	Conteúdo dos Treinamentos	O formador deve considerar para cada frente do projeto, no mínimo, os seguintes treinamentos:					
8	Treinamento	Conteúdo dos Treinamentos	1) Usuários/Analistas de Negócio;					
9	Treinamento	Conteúdo dos Treinamentos	O PROPONENTE deve considerar treinamento técnico suficiente para a operação diária do sistema, visando capacitar a realizar a gestão dos processos das aplicações, realizar suporte básico aos usuários e checar o perfeito funcionamento das rotinas e dos processos implementados/modificados.					
10	Treinamento	Conteúdo dos Treinamentos	O PROPONENTE deve utilizar o ambiente de Qualidade configurado, customizado e com os dados históricos migrados para execução do treinamento, para que deve ser hands-on.					
11	Treinamento	Conteúdo dos Treinamentos	Estimativa que cerca de 30 pessoas com esse perfil serão treinadas.					
12	Treinamento	Conteúdo dos Treinamentos	Após o treinamento será preenchido uma avaliação de reação pela equipe da CPFL, tendo que a índice de aprovação deve ser superior a 80%.					
13	Testes	Metodologia	O proponente é responsável por apresentar padrões e metodologias de testes que possam exatamente, incluindo e não incluindo a funcionalidades existentes, novos funcionalidades requeridas, testes de stress, backup/recover.					
14	Testes	Metodologia	O formador deverá seguir sua metodologia de testes para o plano de teste da CPFL.					
15	Testes	Testes Unitários	O formador é responsável pela execução dos testes unitários em todos os sistemas implementados/modificados durante o projeto.					
16	Testes	Testes Unitários	O formador deverá apresentar o plano e testes unitários, bem como todos os resultados de testes para a aprovação da CPFL.					
17	Testes	Testes Unitários	Deverá ser apresentado as evidências de sucesso dos testes unitários para aprovação da CPFL.					
18	Testes	Testes Integrados TI	O formador é responsável pela execução de um ciclo de testes integrados de TI em todos os sistemas implementados/modificados durante o projeto, visando minimizar os erros de integração entre os sistemas.					
19	Testes	Testes Integrados TI	Esses testes vão também validar a conectividade entre as soluções integradas.					
20	Testes	Testes Integrados TI	O formador deverá apresentar o plano e testes integrados de TI, bem como todos os resultados de testes para a aprovação da CPFL.					
21	Testes	Testes Integrados TI	O formador deverá informar no cronograma Macro e detalhado o período de testes de integração de TI.					
22	Testes	Testes Integrados TI	Deverá ser apresentado as evidências de sucesso dos testes integrados de TI para aprovação da CPFL.					
23	Testes	Testes Integrados TI	Realizar homologação de testes em conjunto com o Prioritador.					
24	Testes	Testes de Stress	O formador é responsável pela execução de um ciclo de testes de Stress em todos os sistemas implementados/modificados durante o projeto, visando minimizar os erros de integração entre os sistemas.					
25	Testes	Testes de Stress	Esses testes vão também validar a conectividade entre as soluções integradas.					
26	Testes	Testes de Stress	O formador deverá apresentar o plano e testes de Stress, bem como todos os resultados de testes para a aprovação da CPFL.					
27	Testes	Testes de Stress	O formador deverá informar no cronograma Macro e detalhado o período de testes de stress.					
28	Testes	Testes de Stress	Deverá ser apresentado as evidências de sucesso dos testes de Stress para aprovação da CPFL.					
29	Testes	Testes de Stress	Esses testes serão acompanhados e definidos em conjunto com a equipe de TI de CPFL.					
30	Testes	Testes de Stress	O PROPONENTE será responsável por executar um ciclo de testes de stress em cada funcionalidade ou subconjunto de funcionalidades a ser testado.					

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	41 de 42

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Tecnologia de Informação
	Título do Documento:	Requisitos de Segurança para Projetos

	Matriz de Conformidade: Requisitos Não Funcionais
Requisitos obrigatórios a serem observados: Escopo: se o atendimento do requisito está incluído ou fora do escopo da solução proposta. 0 - Fora do Escopo 1 - Dentro do Escopo A CPFL entende que todos os requisitos fazem parte do escopo, porém a proponente pode indicar através desse item os requerimentos em que ela considera não aderente ao projeto.	
Modo de Atendimento: como o requerimento é atendido pela solução. Existem 4 modos de atendimento. 0 - Não Atendido - (Requerimento está fora do escopo ou não atendido); 1 - Customização/código - (Atendimento do requerimento demanda customização ou criação de programas/códigos externos ao sistema); 2 - Configuração/script - (Atendimento do requerimento demanda criação de configurações ou scripts usando funcionalidade/scripts do próprio sistema); 3 - Funcionalidades nativas - (Atendimento via funcionalidade nativa sem necessidade de configuração ou customização)	
Esforço: quantidade de horas estimadas para realização do atendimento (via configuração/script ou customização/código). 0 - Nenhum 1 - Pequeno (Até 40 horas) 2 - Médio (Entre 41 e 80 horas) 3 - Grande (Mais de 80 horas)	
Observação: Alguns requisitos se referem a solicitações de informações ou detalhamentos. Nesses casos a proponente deverá preencher a matriz de requisito com código "2 - Atende Totalmente" e a informação deve ser disponibilizada em um capítulo único e específico da Proposta Técnica. Caso a informação não seja disponibilizada, a matriz de requisito deve ser preenchida como "0 - Não Atendido". Os itens "Modo de Atendimento" e "Esforço" não devem ser preenchidos quando os requisitos se referem a solicitações de informações ou detalhamentos.	

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Rocha

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não Aplicável	Não Aplicável	Documento em versão inicial
1.0	20/06/2022	Atualização de requisitos de segurança para projetos

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19271	Instrução	1.0	Raphael Basseto	23/06/2022	42 de 42