Documento Relatório de Teste

Prova de Conceito – Sistema de Facilities

Ministério da Economia
Diretoria de Tecnologia da informação - DTI
Coordenação-Geral de Sistemas

Versão 1.0

Sumário

1.	**IDENTIFICAÇÃO**	2
2.	**INTRODUÇÃO**	2
3.	**ESCOPO**	2
3.1.	**TESTE DE QUALIDADE DAS FUNCIONALIDADES GERAIS MÍNIMAS**	2
3.1.1.	**FISCALIZAÇÃO TÉCNICA E ADMINSTRATIVA**	3
3.1.2.	**FUNCIONALIDADES GERAIS DA PLATAFORMA**	7
5	**RESULTADOS OBTIVOS**	10
6	**EXECUÇÃO DOS TESTES E INSPEÇÃO DE SEGURANÇA**	61
7	**CONCLUSÃO**	99

EVIDÊNCIA DE TESTE - RELATÓRIO DE TESTES

Controle de Versões			
Versão	**Data**	**Autor**	**Descrição**
1.0	21/06/2022	Wesley Martins da Silva - G4F	Criação do documento
0.2	27/06/2022	Wesley Martins da Silva - G4F	Conclusão da análise das funcionalidades do sistema
0.3	28/06/2022	Emerson Ribeiro – G4F	Conclusão da análise de segurança
1.0	28/06/2022	Ivan Carlos de Oliveira – G4F	Revisão do relatório para entrega

1. IDENTIFICAÇÃO

Número da OS:	**153/2022**
Sistema/Módulo:	**Sispred/Facilities**
Gerente de Projeto:	**Ivan Carlos de Oliveira**
Analista de Teste:	**Wesley Martins da Silva**
Analista de Segurança:	**Emerson Ferreira**

2. INTRODUÇÃO

O objetivo deste é sintetizar os resultados obtidos na execução dos serviços de Teste e Qualidade de Software e Testes de Segurança e Desempenho relativos à Prova de Conceito para contratação de pessoa jurídica para a prestação de serviços de gestão integrada de serviços prediais – facilities conforme funcionalidades mínimas e requisitos de segurança previstas na solução tecnológica descritas respectivamente nos itens 3.1 e 4.4 do Anexo VI do Termo de Referência.

3. ESCOPO

3.1. TESTE DE QUALIDADE DAS FUNCIONALIDADES GERAIS MÍNIMAS

Os serviços de teste e qualidade compreendem a execução das seguintes atividades para a soluções tecnológica apresentada pela CONTRATADA, com o objetivo de identificação de possíveis

falhas e defeitos, em conformidade com o processo licitatório abrangendo os itens 3 e 4 de avaliação elencados no Anexo VI do Termo de Referência.

3.1.1. FISCALIZAÇÃO TÉCNICA E ADMINSTRATIVA

As funcionalidades que são o foco dos testes são as descritas abaixo:

Agrupamento		Campos Necessários
1	Cadastro do contrato	Número, data de assinatura, data de início da vigência, data final da vigência, data de início da execução de acordo com o serviço, data de início de apostilamento, data final de apostilamento, data de início de aditivo, data final de aditivo.
2	Cadastro de usuário	Nome, CPF, e-mail (extensão ".gov.br"), telefone celular, perfil de acesso (gestor do contrato, fiscal administrativo, fiscal técnico, fiscal setorial, apoio à fiscalização, servidor, equipe de gerenciamento de facilities da CONTRATADA e colaboradores da CONTRATADA).
3	Cadastro de subcontratadas (Prestadores)	Nome, CNPJ, descrição do serviço, empregados alocados, representante legal, e-mail, telefone, campo para inclusão de documentos como ART, currículos, contrato social e termo de subcontratação e informações complementares dos funcionários descritas no item 2.
4	Cadastro da edificação	Identificação precisa e constantemente atualizada com os dados disponíveis, plantas, layouts, posição no prédio, utilização.
5	Cadastro de QrCodes (Cadastro de Ativo e Local)	Permitir a atuação dos fiscais para inserção de chamados e informações de forma ágil, assim como dos usuários, na fiscalização das atividades, prazos, qualidade e abertura de chamados não programados. Identificação do ambiente ou equipamento e menu de opções para chamados correlatos. Cada menu de opções deve ser avaliado de acordo com as possibilidades de cada nível de acesso dos usuários, validadas em conjunto com a fiscalização.
6	Cadastro das atividades - contratada e equipe de gestão/fiscalização (Plano de Manutenção Preventiva)	Código e nome dos serviços contemplados na contratação, conforme TR, classificação (de rotina, sob demanda, corretivos, não programada), frequência, criticidade, unidades de medida, programação da execução e datas efetivas de realização, inserção de fotos e documentos. Campos vinculados aos perfis de acesso, utilização de recursos.

7	Cadastro das atividades - abertura de chamados pelos usuários do prédio (Plano de Manutenção Preventiva)	Identificação (nome/telefone/CPF) do demandante; data e hora do registro da demanda; pavimento da demanda, quando for o caso; descrição da demanda, com possibilidade de inclusão de arquivo eletrônico com a imagem referente ao objeto da demanda; direcionamento da demanda ao perfil da fiscalização (que poderá ser delegada a seu critério/redirecionada) para análise; campo para a fiscalização aprovar/reprovar a demanda cadastrada; CPF do executor da análise da demanda cadastrada; data e hora da análise da demanda cadastrada; campo para a fiscalização justificar a aprovação e reprovação da demanda cadastrada; CPF do empregado da CONTRATADA ou da(s) subcontratada(s) que atendeu à demanda; data e hora do registro do início e término do atendimento da demanda ou de indicação de demanda não procedente, com possibilidade de registro de observações relacionadas, seja via aplicação web ou aplicativo mobile. Para demandas de mensageria/contínuo deverão haver campos para identificação do solicitante, destinatário, local de entrega, distância média estimada (ida a partir do Bloco B da Esplanada dos Ministérios), observações, horário de abertura do chamado, identificador do TaxiGov.
8	Cadastro de insumos (Produtos/Serviços)	Código, código SINAPI, nome do insumo, unidade de medida, tipo de insumo (material, mão de obra, aplicação, consumo), quantidade, custo unitário, data da cotação, registro ou protocolo na ANVISA, se tipo saneante sanitário, número do CA (Certificado de Aprovação), conforme estabelecido na NR 6, se tipo EPI, quantidade em estoque.
9	Cadastro de ferramentas (Caixa de Ferramentas)	Código, identificação do ferramental utilizado, quantidade, custo unitário.
10	Cadastro de uniformes - (A definir - Podendo ser um item da Caixa de Ferramentas)	Código, identificação dos uniformes utilizados, quantidade, custo unitário.
11	IMR - Indicador de desempenho 1 -Nível de desconformidade dos serviços (NI-DESSER) - A definir	Campo específico para descrição das notificações, responsável pela notificação, data, inserção de fotos, peso, criticidade, reincidência, disciplina, item, mecanismos de alertas, responsável pelo recebimento da notificação, manifestação, avaliação e análise final. Inserção das equações para cálculo do IMR.
12	IMR - Indicador de desempenho 2 - Nível de atendimento das solicitações no prazo (NI-TEMPO) - A definir	Tempo excedente para execução das tarefas. Inserção das equações para cálculo do IMR.

13	IMR - Indicador de desempenho 3 - Nível de redução de serviços corretivos (NI-RED CORRET) - A definir	Inserção das equações para cálculo do IMR.
14	IMR - Indicador de desempenho 4 - Nível de satisfação dos usuários (NISATIU) - A definir	Campo de identificação do avaliador, data da avaliação, identificação do serviço avaliado, nota concedida. Inserção da equação para cálculo do IMR. Campo aberto opcional.
15	IMR - Indicador de desempenho 5 - Nível de progresso de sustentabilidade (NI-PRO-SUS) - A definir	Campos de consumo mensais de água, energia e geração de resíduos, unidades. Taxa média de ocupação mensal do prédio. Inserção da equação para cálculo do IMR.
16	Cadastramento de ACT, CCT ou DCT - A definir	Nome e CNPJ da entidade sindical da CONTRATADA, nome e CNPJ da entidade sindical dos empregados de acordo com o tipo de serviço, tipo de documento (ACT, CCT ou DCT), data de início e final da vigência e respectivo registro (com possibilidade de registro e manutenção do histórico das ocorrências), data de início e final da vigência de aditivo e respectivo registro (com possibilidade de registro e manutenção do histórico das ocorrências).
17	Cadastramento de cargos dos empregados da CONTRATADA- A definir	Código e nome do cargo, código CBO do cargo.
18	Cadastramento de salário dos cargos dos empregados da CONTRATADA e da(s) subcontratada(s)- A definir	CPF e código do cargo, data de vigência e valor do salário (com possibilidade de registro e manutenção do histórico das ocorrências).
19	Cadastramento de tipos de exames médicos CONTRATADA e da(s) subcontratada(s) - A definir	CPF, código e nome dos tipos exame médicos sendo: admissional, periódico, de retorno ao trabalho, de mudança de função e demissional dos cargos dos empregados da CONTRATADA e da(s) subcontratada(s)
20	Cadastramento de senha de acesso à solução tecnológica, com possibilidade de alteração a qualquer momento, inclusive nos casos de esquecimento da senha cadastrada (Cadastro de Usuários)	Data e CPF dos usuários servidor (login) e senha, de forma criptografada, no sistema. O usuário poderá alterar sua senha de forma autônoma, na plataforma tecnológica.

22	Cadastramento dos empregados e subcontratados - A definir	CPF e nome do empregado; CI do empregado e respectivo arquivo eletrônico com a imagem do documento; CTPS do empregado e respectivo arquivo eletrônico com a imagem do documento (páginas de identificação e do contrato de trabalho com a CONTRATADA ou da(s) subcontratada(s); indicador pessoa reabilitada ou com deficiência; data de vigência e endereço, bairro, cidade, UF, CEP do empregado, com manutenção das alterações efetuadas, data de vigência e código do cargo do empregado (com possibilidade de registro e manutenção do histórico das ocorrências), datas de admissão e de demissão do empregado (com possibilidade de registro e manutenção do histórico das ocorrências), datas de início e final da alocação do empregado (com possibilidade de registro e manutenção do histórico das ocorrências), data de vigência, jornada de trabalho mensal, horário de início e de fim do trabalho e horário de início e de fim do intervalo para alimentação (com possibilidade de registro e manutenção do histórico das ocorrências).
23	Cadastramento de exames médicos dos empregados, observadas as disposições do PCMSO estabelecido pela NR 7 - A definir	CPF do empregado, data do exame, tipo e respectivo arquivo eletrônico com a imagem do documento comprobatório (com possibilidade de registro e manutenção do histórico das ocorrências).
24	Cadastramento das férias dos empregados - A definir	CPF do empregado, datas de início e final do período aquisitivo, datas de início e final das férias e respectivos arquivos eletrônicos com as imagens do aviso e do recibo de pagamento.
25	Cadastramento de comprovantes de pagamento de salário dos empregados - A definir	CPF do empregado, mês e ano do pagamento e respectivo arquivo eletrônico com a imagem do recibo de pagamento do salário (com possibilidade de registro e manutenção do histórico das ocorrências).
26	Cadastramento de comprovantes de pagamento de vale-transporte dos empregados - A definir	CPF do empregado, mês e ano do pagamento e respectivo arquivo eletrônico com a imagem do recibo de pagamento do vale-transporte (com possibilidade de registro e manutenção do histórico das ocorrências).
27	Cadastramento de comprovantes de pagamento de auxílio alimentação dos empregados - A definir	CPF do empregado, mês e ano do pagamento e respectivo arquivo eletrônico com a imagem do recibo de pagamento do auxílio alimentação (com possibilidade de registro e manutenção do histórico das ocorrências).

28	Cadastramento de comprovante de pagamento de rescisão de contrato de trabalho dos empregados - A definir	CPF do empregado, data do pagamento e respectivo arquivo eletrônico com as imagens do termo de rescisão e do recibo de pagamento.
29	Cadastramento de comprovante de recolhimento de contribuições sociais decorrentes dos pagamentos efetuados aos empregados - A definir	Mês e ano de competência e valores de recolhimento e respectivos arquivos eletrônicos com a imagem dos respectivos comprovantes de recolhimento.
30	Cadastramento das parcelas dos custos com os empregados da CONTRATADA e da(s) subcontratada(s) - A definir	Mês e ano de competência (com possibilidade de registro e manutenção do histórico das ocorrências), parcelas e valores dos custos da CONTRATADA e da(s) subcontratada(s) com os empregados alocados na execução dos serviços no mês, considerando salários, adicionais, benefícios e contribuições sociais decorrentes.

3.1.2. FUNCIONALIDADES GERAIS DA PLATAFORMA

Os requisitos que são foco dos testes são os descritos abaixo:

3.2.1 Consulta

a) A solução tecnológica deverá possibilitar consulta aos dados, informações e imagens cadastradas na base de dados, registro de inclusão e exclusão de documento, visando otimizar o desenvolvimento das atividades de gestão, controle e fiscalização contratual.

b) Possibilitar à CONTRATANTE acesso de consulta, a qualquer tempo, à réplica do banco de dados referentes ao contrato, para análise do log de eventos ou disponibilizar versão da base de dados em mídia própria à CONTRANTE ou, ainda, franquear acesso por intermédio de conexão remota pela rede de dados, com metodologia e protocolo a ser definido pela CONTRATANTE

3.2.2 Relatórios

a) A solução tecnológica deverá possibilitar consultas, emissão e impressão de relatórios, no formato PDF e XLS, com dados, informações e documentos cadastrados, registrados e armazenados a qualquer momento, assim como possibilidade de serem filtrados mensalmente. Deverão ser disponibilizados filtros para facilitar a visualização dos dados mais importantes e operacionalização do contrato.

3.2.3 Disponibilidade

a) A solução tecnológica deverá estar disponível para acesso via aplicação web e aplicativo mobile, em regime contínuo, inclusive aos sábados, domingos e feriados.

3.2.4 Manutenção da solução tecnológica

Aspectos de ordem contratual, não sendo tratados em Prova de Conceito.

3.2.5 Atualização da solução tecnológica

Aspectos de ordem contratual, não sendo tratados em Prova de Conceito.

3.2.6 Aspectos gerais

a) A solução tecnológica deverá contemplar os seguintes parâmetros:

I - permitir que os usuários efetuem consultas no sistema sobre a situação das suas solicitações;

II - operação em rede TCP/IP;

III - possuir interface gráfica de fácil utilização e ser customizada no atendimento das necessidades do contrato e da CONTRATANTE;

IV - visualização rápida dos índices/níveis e indicadores de desempenho por meio de Dashboards;

V - encaminhamento de ordem de serviço, de acordo com calendário de manutenção predial, a ser programado pela CONTRATADA;

VI - acompanhamento de todo o processo de emissão e encaminhamento das ordens de serviços;

VII - impossibilidade de o usuário gerar mais de uma OS com mesma demanda;

VIII - controle do cronograma dos serviços de rotina, não programados e sob demanda (atividades e equipamentos);

IX - controle de custos, com apropriação e cálculo automático do custo de mão de obra e dos materiais aplicados para cada Ordem de Serviço (OS), com emissão de relatórios consolidados;

X - acompanhamento e controle dos chamados (OS) de manutenção (abertura, status, solicitador, pendências, responsável), que serão realizados pela CONTRATANTE;

XI - inserção de informações e descrições da solução dada ao problema, com possibilidade de apontamentos de OS via aplicativo mobile;

XII - gerenciamento e acompanhamento das pendências dos serviços de rotina não programados e sob demanda;

XIII - gerenciamento do total de serviços de rotina não programados e sob demanda solicitados em comparação com o total de serviços realizados;

XIV - gerenciamento do tempo de realização e qualidade dos serviços de rotina não programados e sob demanda realizados;

XV - campos para inserção, gerenciamento e acompanhamento dos consumos de energia e água pela CONTRATANTE e CONTRATADA;

XVI - campos para inserção, gerenciamento e acompanhamento da produção de resíduos sólidos pela CONTRATANTE e CONTRATADA;

XVII - cadastramento dos seguintes relatórios e estudos:

- RCP - Relatório das Condições Prediais, conforme Anexo III;
- PMOC - Plano de Manutenção, Operação e Controle, conforme Anexo III;
- PIE - Prontuário de Instalações Elétricas, conforme Anexo III;

- PTA - Plano de Trabalho Anual (Plano de Gestão e Desempenho, Plano de Conservação e Limpeza, Plano de Manutenção Predial, Plano de Operação Predial);
    - Cadastramento das rotinas por serviço e tipo de serviço;
    - Horário previsto de início e final da execução do serviço; Horário de início e final da execução do serviço;
    - Código(s) e nome do(s) insumo(s) a ser(em) utilizado(s) na execução do serviço e respectiva(s) unidade(s) de medida e quantidade(s);
    - CPF do(s) empregado(s) alocado(s) na execução do serviço. Estudos de Redução de Consumo e Uso Racional e Eficiente da Água; Estudos de Redução de Consumo e Uso Racional e Eficiente de Energia; e
- Estudos de Redução de Produção e de Uso Racional e Eficiente de Resíduos Sólidos.
- XVIII - campo para upload e download de documentos, a exemplo de projetos, estudos, orçamentos e outros documentos necessários à gestão e fiscalização do objeto contratado, nas extensões compatíveis com os sistemas da CONTRATANTE.

Soluções apresentadas:

- Web: https://testes.sispred.com.br/mma/
- IOS: https://testes.sispred.com.br/mma/
- Android: https://testes.sispred.com.br/mma/

4 RECURSOS NECESSÁRIOS

4.1 Recursos Humanos:

Responsável	Papel	Responsabilidades
Ivan Carlos de Oliveira	Gerente de Projetos	Responsável pela coordenação dos testes e andamento do projeto
Wesley Martins da Silva	Especialista em Teste	Responsável pela execução dos testes funcionais previstos para o projeto
Emerson Ferreira	Especialista em Segurança	Responsável pela execução dos testes de segurança do projeto

5 RESULTADOS OBTIVOS

5.1 Requisitos de Acessibilidade

Esta atividade compreende na avaliação dos seguintes itens:

- Acesso à solução tecnológica por meio de aplicação web compatível com Google Chrome;
- Acesso à solução tecnológica por meio de aplicação web compatível com Mozilla Firefox;
- Acesso à solução tecnológica por meio de aplicação web compatível com Safari;
- Acesso à solução tecnológica por meio de aplicação web compatível com Microsoft Edge;
- Acesso à solução tecnológica por meio de aplicação web compatível com Android;
- Acesso à solução tecnológica por meio de aplicação web compatível com IOS.

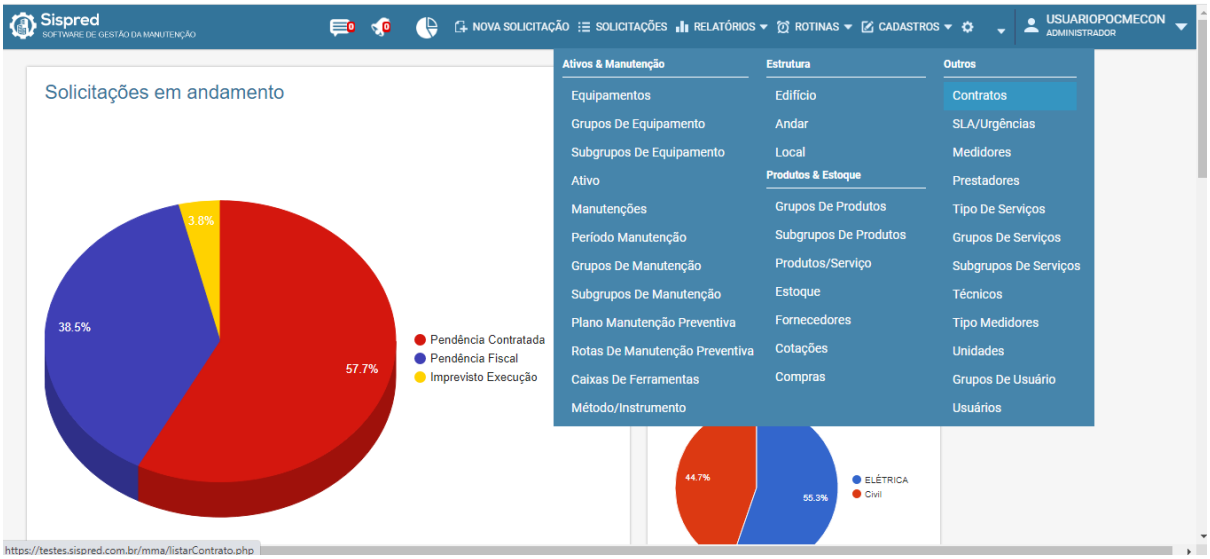
Tipo de avaliação: Conformidade
Estratégia de teste: Verificação manual
Status: **Aprovado**

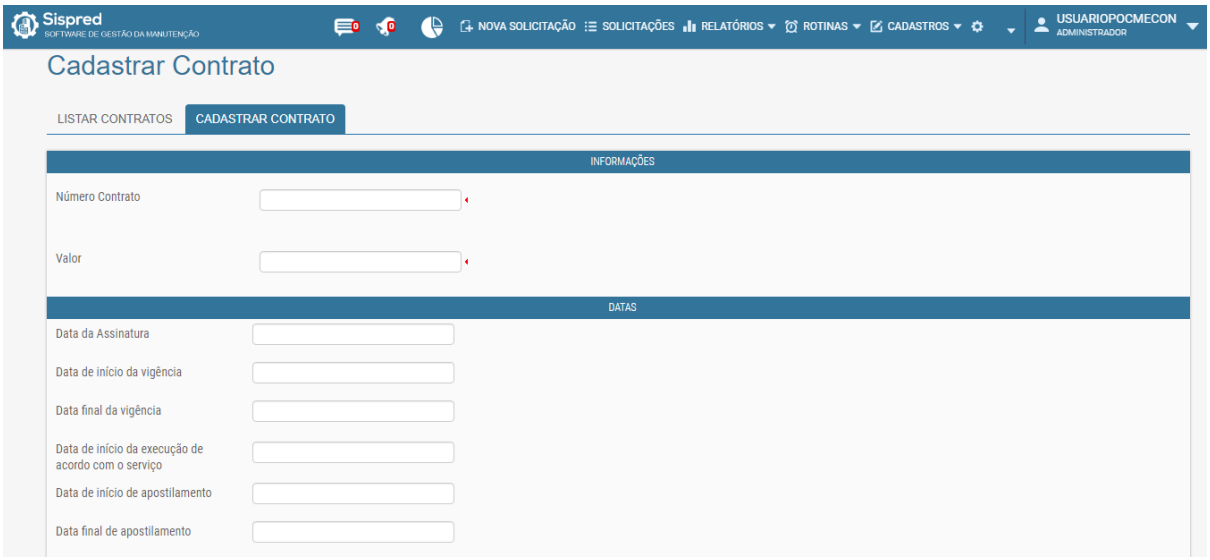
7.2 Fiscalização Técnica e Administrativa

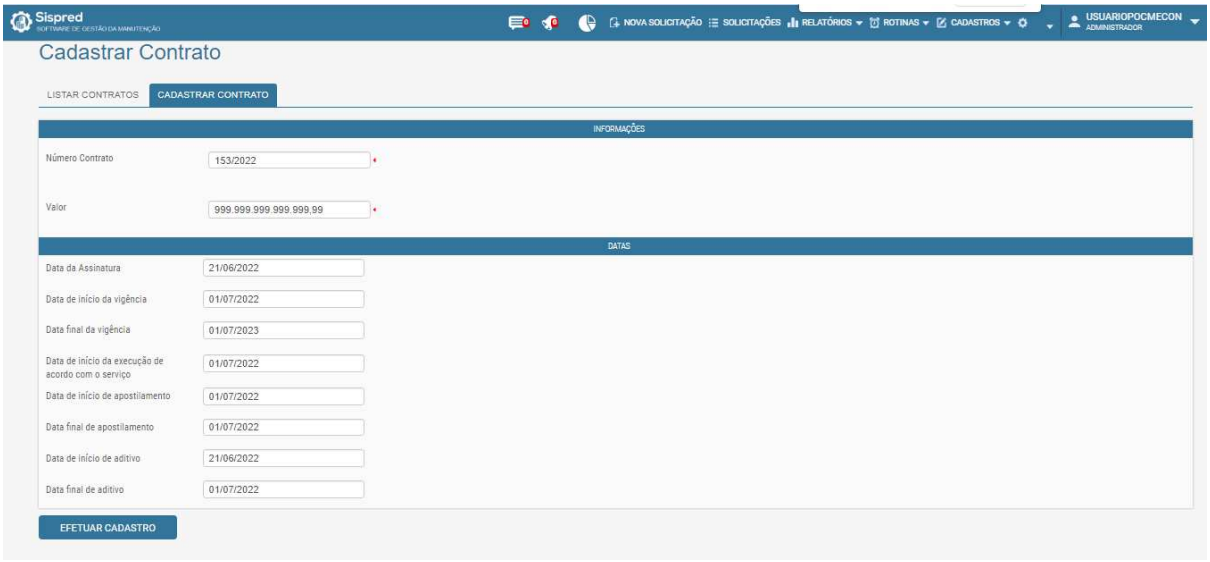
Esta atividade compreende na avaliação das funcionalidades relacionadas no item 3 Escopo:

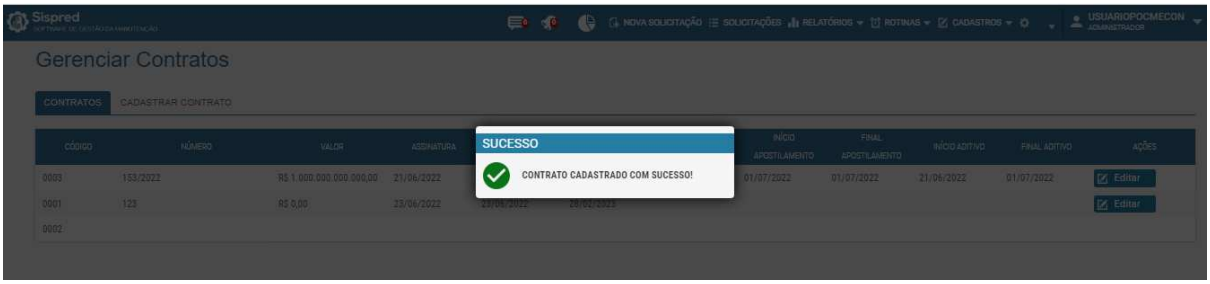
1 – Cadastro de Contratos

Trilha de Navegação: Menu Principal -> Cadastros -> Outros -> Contratos -> Cadastrar Contrato


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Solicitações em andamento
3.8%
38.5%
57.7%
Pendência Contratada
Pendência Fiscal
Imprevisto Execução
Ativos & Manutenção
Equipamentos
Grupos De Equipamento
Subgrupos De Equipamento
Ativo
Manutenções
Período Manutenção
Grupos De Manutenção
Subgrupos De Manutenção
Plano Manutenção Preventiva
Rotas De Manutenção Preventiva
Caixas De Ferramentas
Método/Instrumento
Estrutura
Edifício
Andar
Local
Produtos & Estoque
Grupos De Produtos
Subgrupos De Produtos
Produtos/Serviço
Estoque
Fornecedores
Cotações
Compras
Outros
Contratos
SLA/Urgências
Medidores
Prestadores
Tipo De Serviços
Grupos De Serviços
Subgrupos De Serviços
Técnicos
Tipo Medidores
Unidades
Grupos De Usuário
Usuários
44.7%
55.3%
ELÉTRICA
Civil
https://testes.sispred.com.br/mma/listarContrato.php


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Cadastrar Contrato
LISTAR CONTRATOS
CADASTRAR CONTRATO
INFORMAÇÕES
Número Contrato
Valor
DATAS
Data da Assinatura
Data de início da vigência
Data final da vigência
Data de início da execução de acordo com o serviço
Data de início de apostilamento
Data final de apostilamento



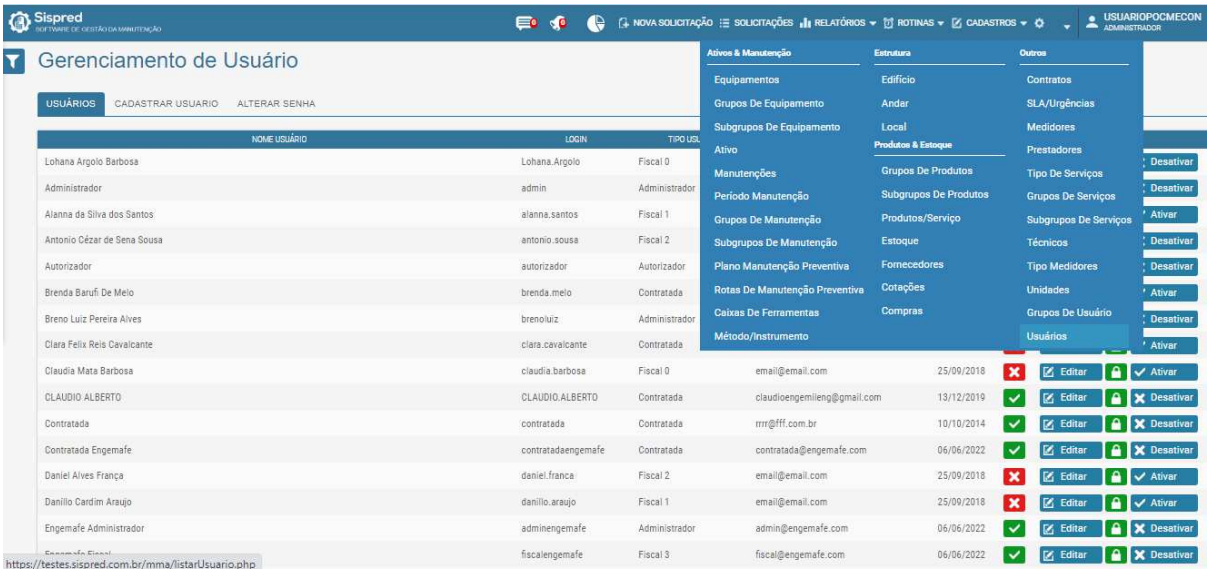


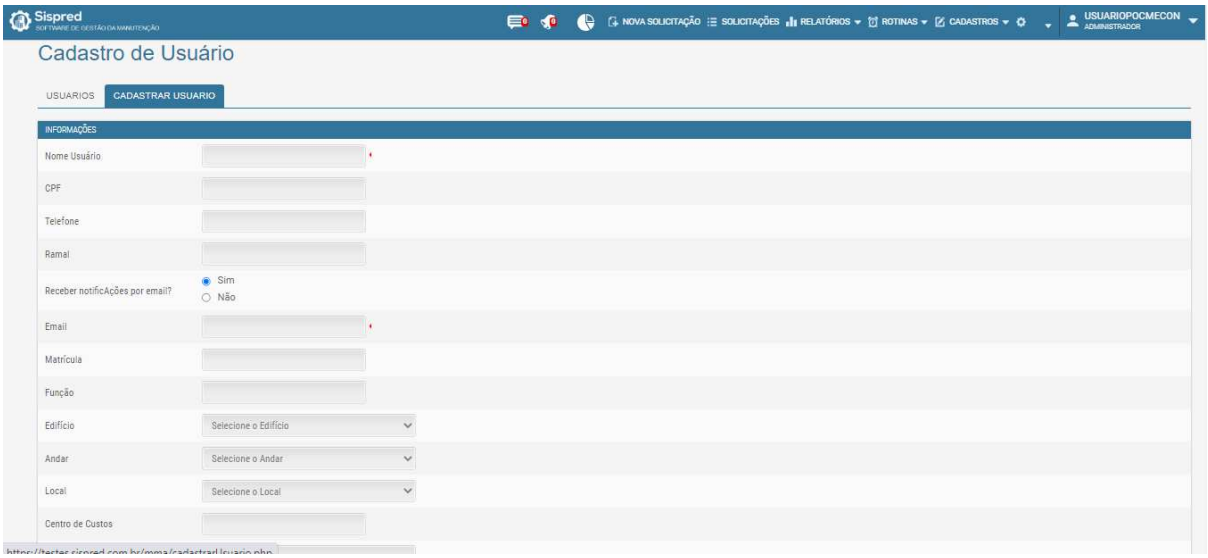
Status: **Aderente com ressalvas**

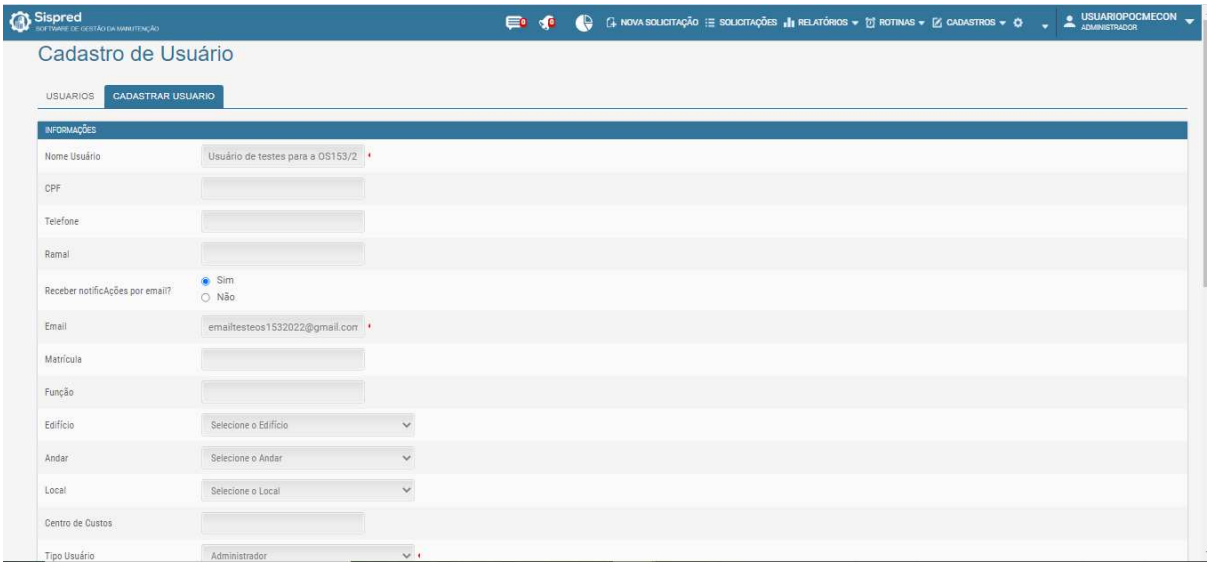
Sugestão de melhoria/ajustes: Sistema permite cadastrar vários contratos com os mesmos valores e não formata as datas quando é digitado manualmente, gerando um bug na funcionalidade.

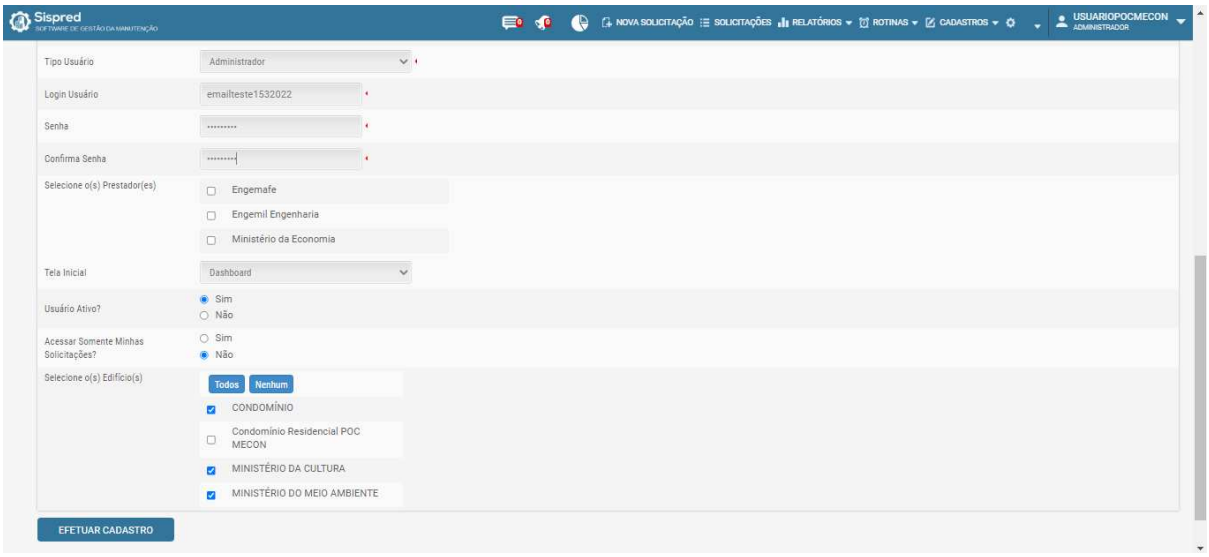
2 – Cadastro de Usuário

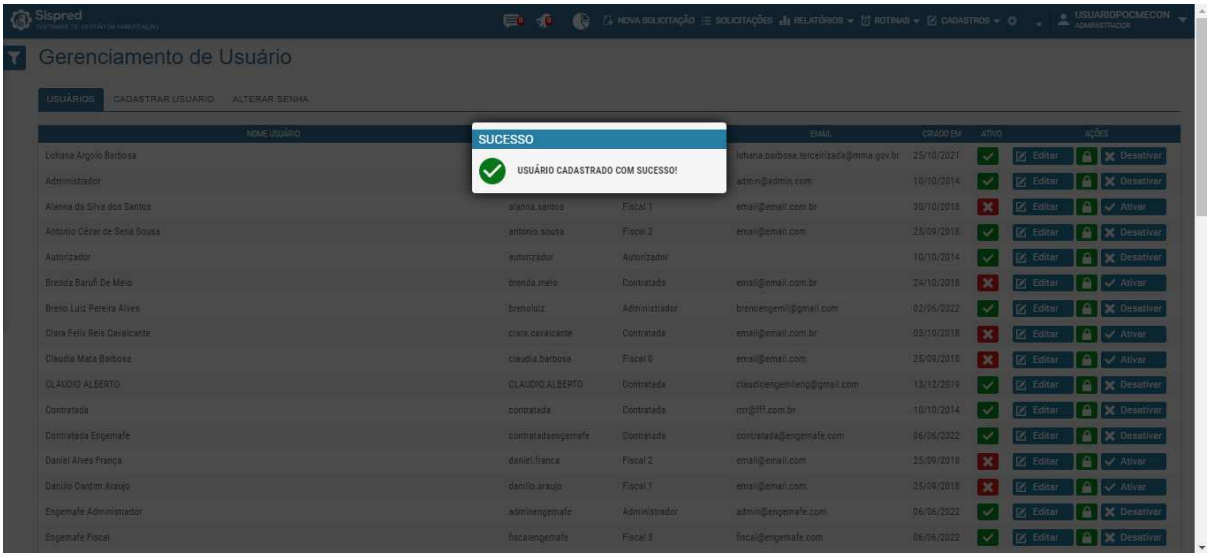
Trilha de Navegação: Menu Principal -> Cadastros -> Outros -> Usuários -> Cadastrar Usuário

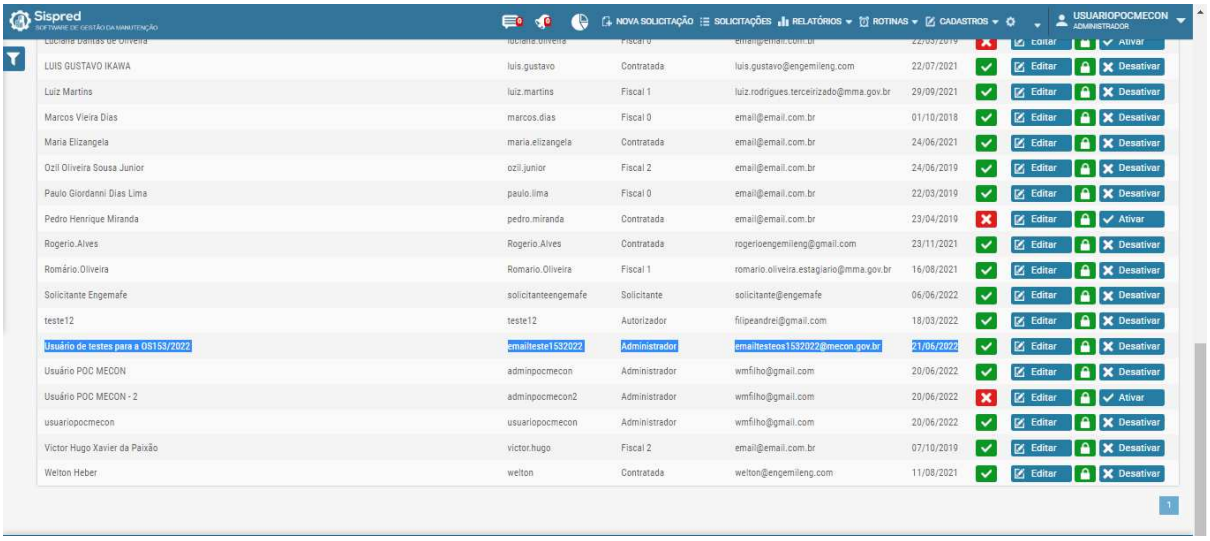





Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Cadastro de Usuário
USUARIOS
CADASTRAR USUARIO
INFORMAÇÕES
Nome Usuário
Usuário de testes para a OS153/2
CPF
Telefone
Ramal
Receber notificAções por email?
Sim
Não
Email
emailtesteos1532022@gmail.com
Matrícula
Função
Edifício
Selecione o Edifício
Andar
Selecione o Andar
Local
Selecione o Local
Centro de Custos
Tipo Usuário
Administrador


Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Tipo Usuário
Administrador
Login Usuário
emailteste1532022
Senha
Confirma Senha
Selecione o(s) Prestador(es)
Engemafe
Engemil Engenharia
Ministério da Economia
Tela Inicial
Dashboard
Usuário Ativo?
Sim
Não
Acessar Somente Minhas Solicitações?
Sim
Não
Selecione o(s) Edifício(s)
Todos
Nenhum
CONDOMÍNIO
Condomínio Residencial POC MECON
MINISTÉRIO DA CULTURA
MINISTÉRIO DO MEIO AMBIENTE
EFETUAR CADASTRO



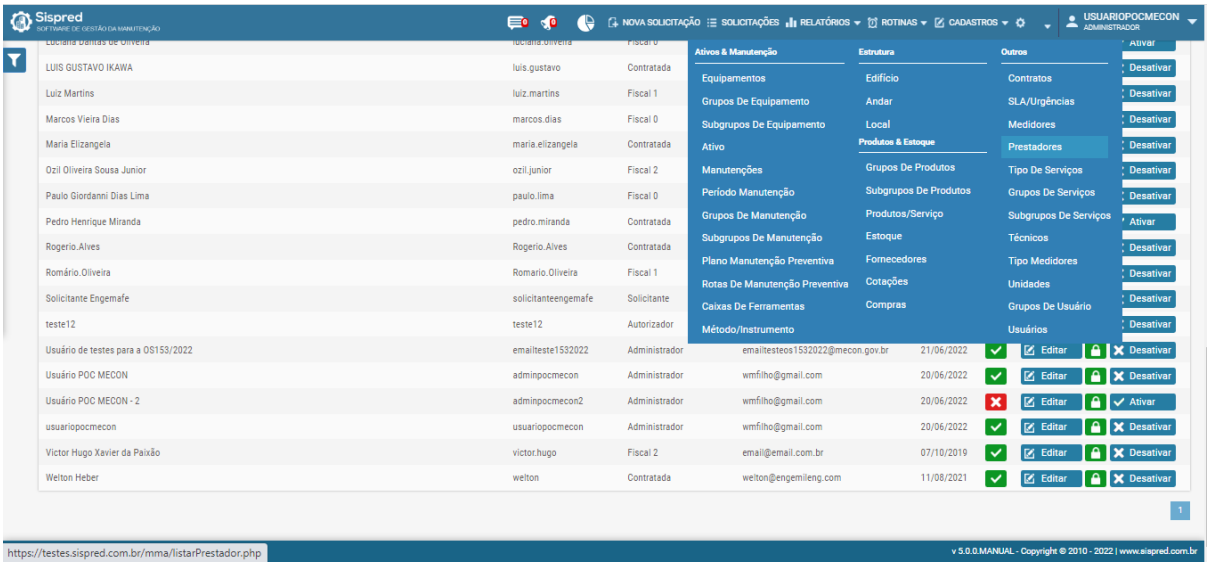


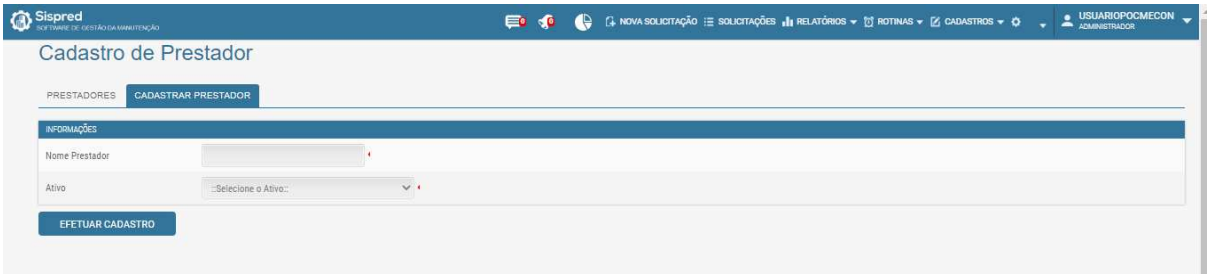
Status: Aderente com ressalvas

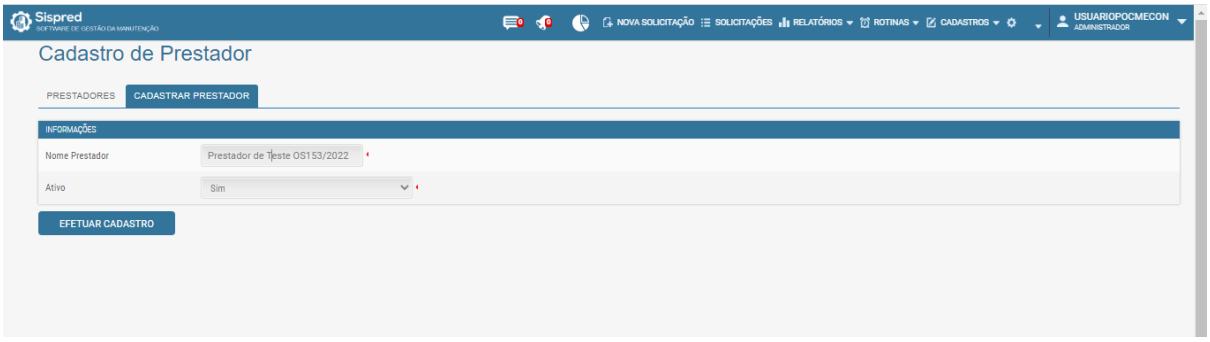
Sugestão de melhoria/ajuste: Os novos cadastros no Grupo de Usuários, apresenta os valores desalinhados e permite o cadastro de vários tipos de usuários repetidos.

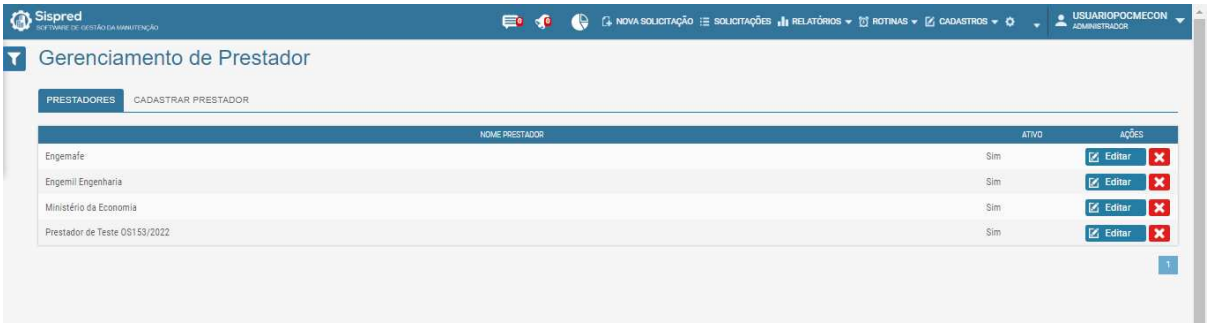
3 – Cadastro de Subcontratadas

Trilha de Navegação: Menu Principal -> Cadastros -> Outros -> Prestadores -> Cadastrar Prestador





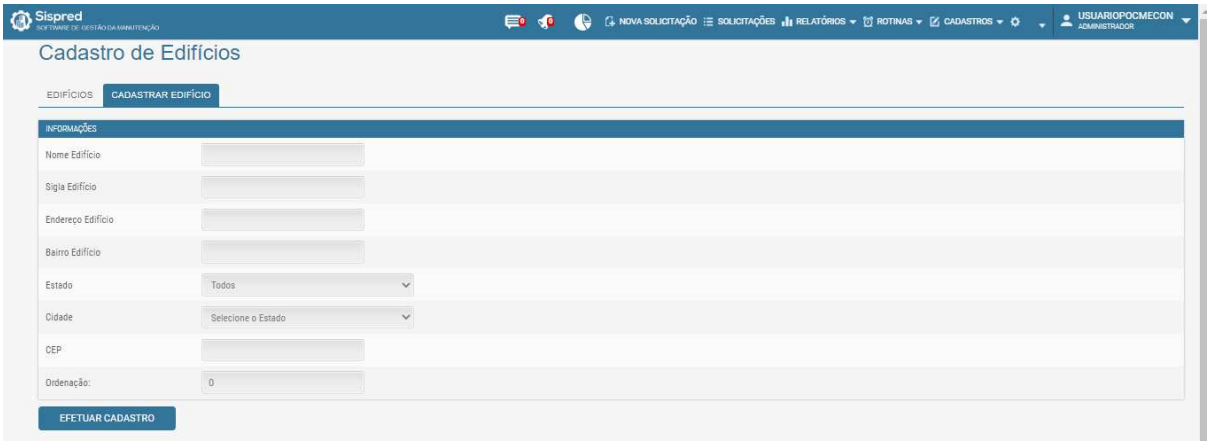


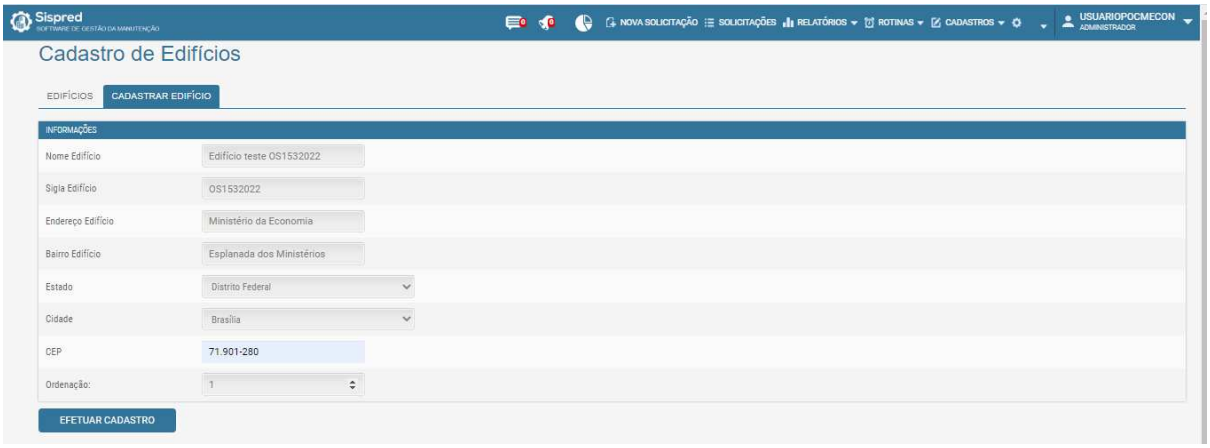


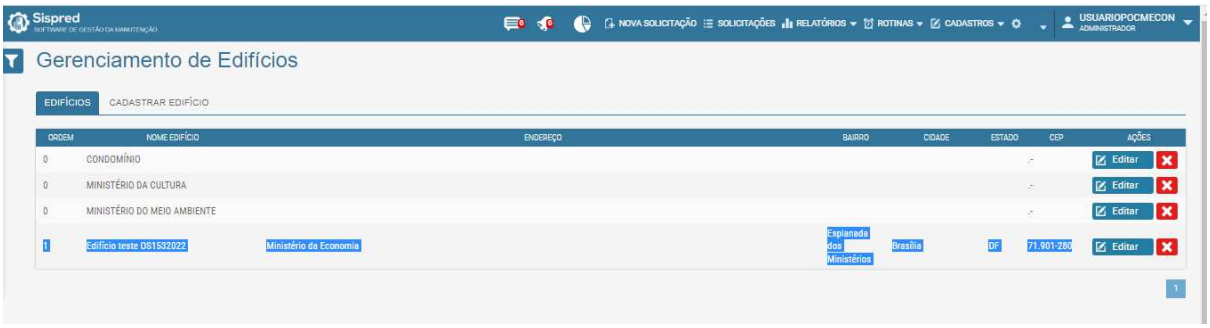
Status: **Não aderente**. No cadastro de prestadores, não é possível cadastras as seguintes informações: CNPJ, descrição do serviço, empregados alocados, representante legal, e-mail, telefone, campo para inclusão de documentos como ART, currículos, contrato social e termo de subcontratação e informações complementares dos funcionários.

4 – Cadastro da Edificação

Trilha de Navegação: Menu Principal -> Cadastros -> Estrutura -> Edifício -> Cadastrar Edifício



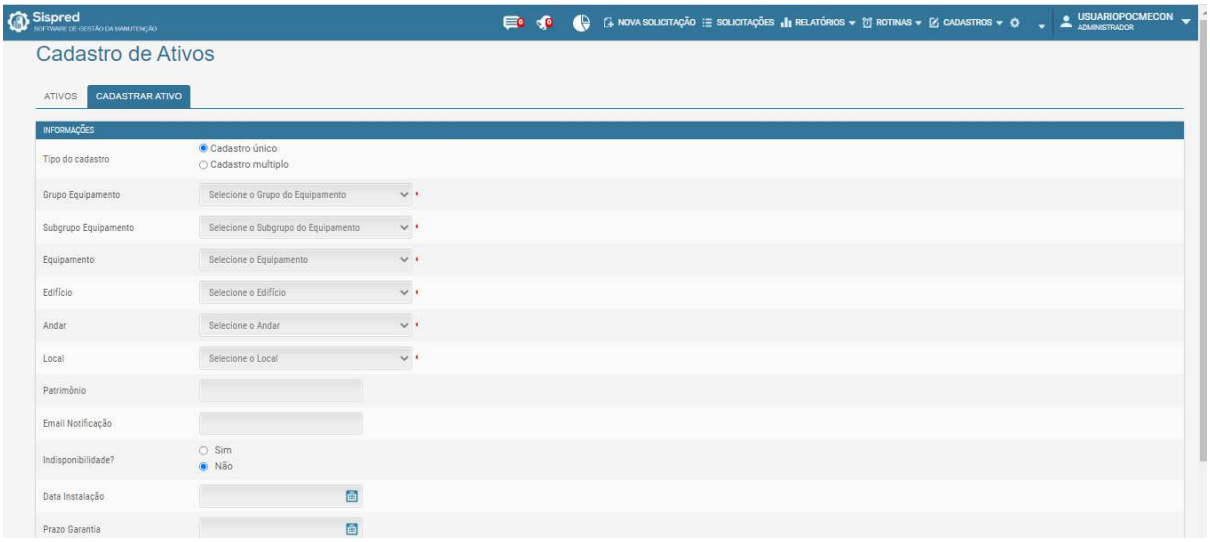


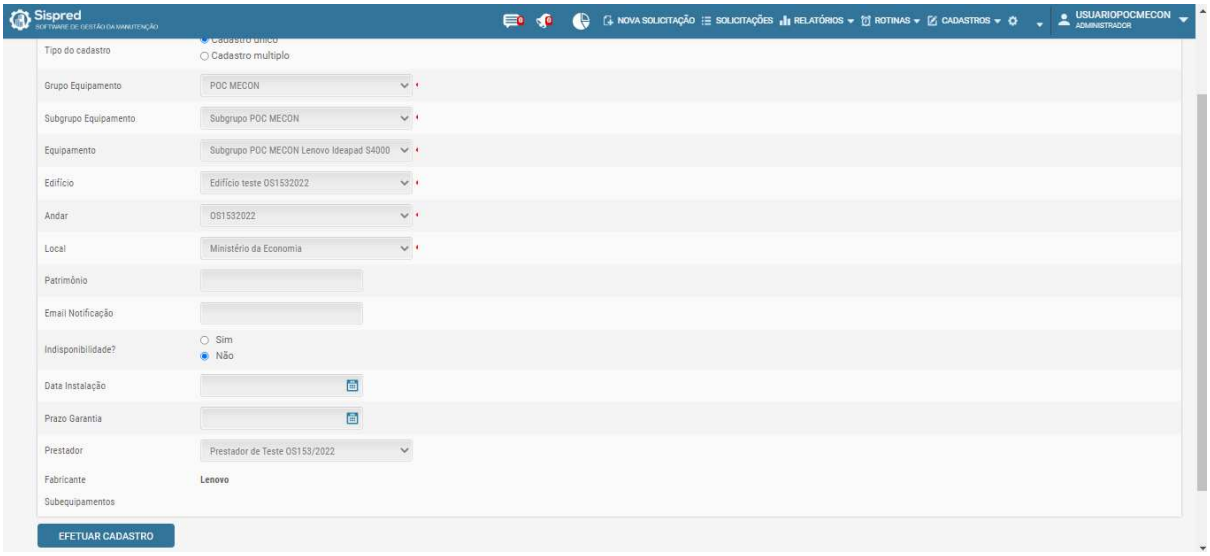


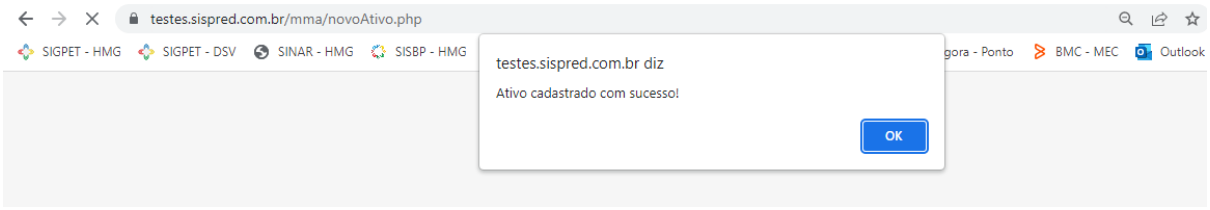
Status: Aderente com ressalvas.
Sugestão de melhoria/ajustes: No cadastro de edificação, não apresenta os campos para inclusão de plantas, layouts e utilização.

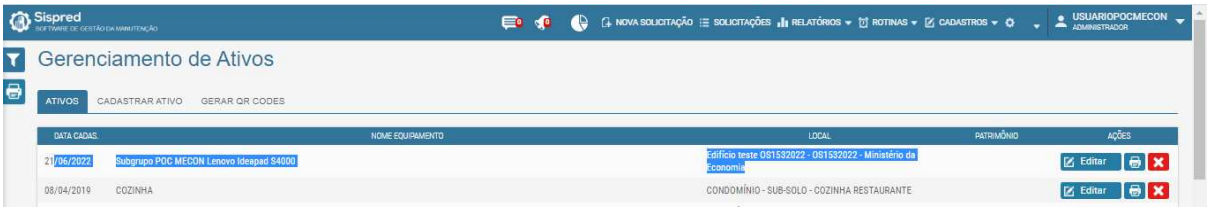
5 – Cadastro de QR Codes

Trilha de Navegação: Menu Principal -> Cadastros -> Ativos & Manutenção -> Ativo -> Cadastrar Ativo -> Gerar QR Codes ou Menu Principal -> Cadastros -> Estrutura -> Local -> Gerar QR Codes







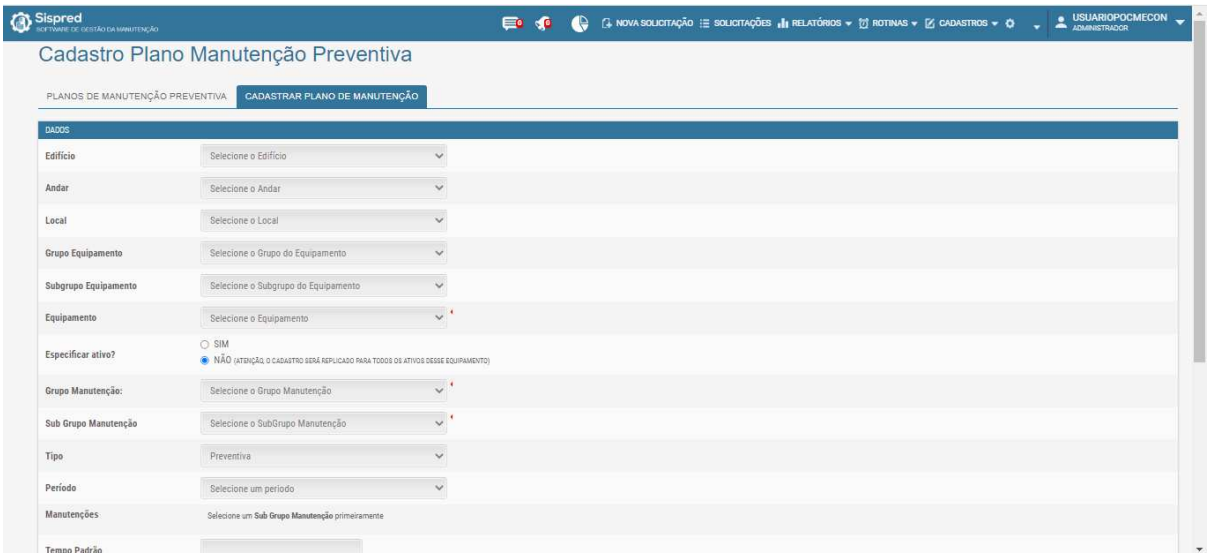


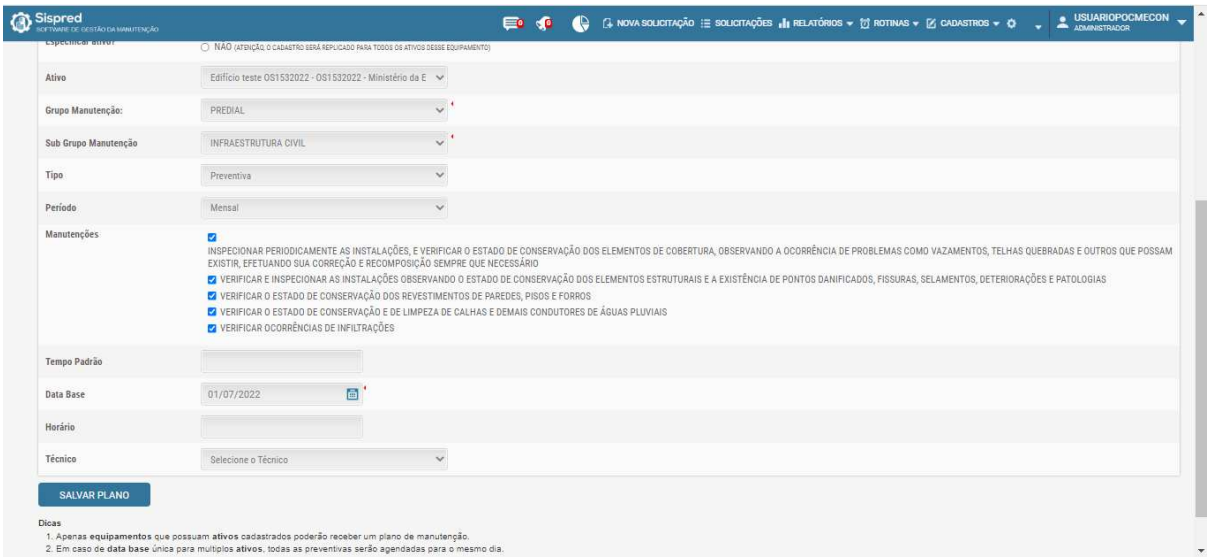
Status: Aderente com ressalvas.

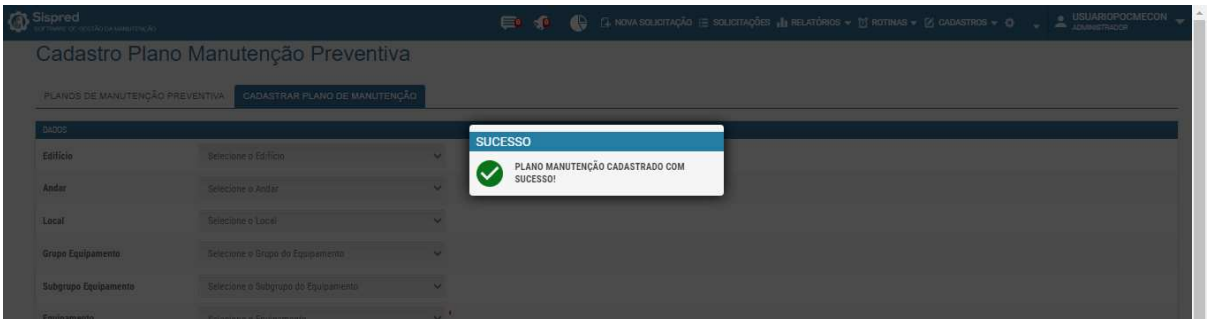
Sugestão de melhoria: Melhorar a usabilidade do sistema de forma mais intuitiva. De repente apresentar a geração do QRCodes dentro da funcionalidade de Solicitação.

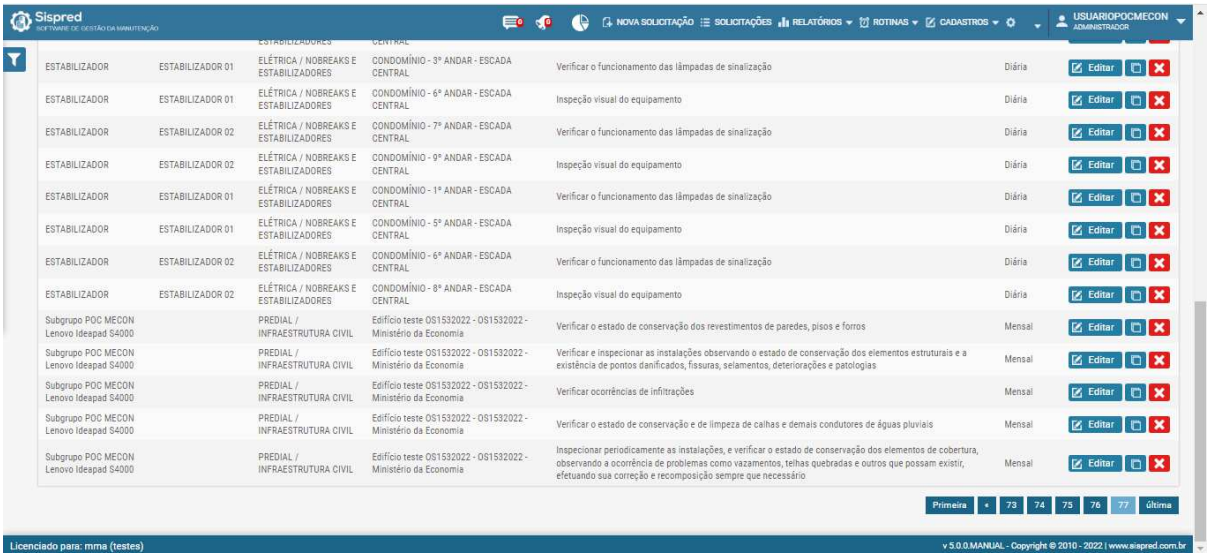
6 – Cadastro das atividades - contratada e equipe de gestão/fiscalização

Trilha de Navegação: Menu Principal -> Cadastros -> Ativos & Manutenção -> Plano Manutenção Preventiva -> Cadastrar Plano de Manutenção




Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Ativo
Edifício teste OS1532022 - OS1532022 - Ministério da E
Grupo Manutenção:
PREDIAL
Sub Grupo Manutenção
INFRAESTRUTURA CIVIL
Tipo
Preventiva
Período
Mensal
Manutenções
INSPECIONAR PERIODICAMENTE AS INSTALAÇÕES, E VERIFICAR O ESTADO DE CONSERVAÇÃO DOS ELEMENTOS DE COBERTURA, OBSERVANDO A OCORRÊNCIA DE PROBLEMAS COMO VAZAMENTOS, TELHAS QUEBRADAS E OUTROS QUE POSSAM EXISTIR, EFETUANDO SUA CORREÇÃO E RECOMPOSIÇÃO SEMPRE QUE NECESSÁRIO
VERIFICAR E INSPECIONAR AS INSTALAÇÕES OBSERVANDO O ESTADO DE CONSERVAÇÃO DOS ELEMENTOS ESTRUTURAIS E A EXISTÊNCIA DE PONTOS DANIFICADOS, FISSURAS, SELAMENTOS, DETERIORAÇÕES E PATOLOGIAS
VERIFICAR O ESTADO DE CONSERVAÇÃO DOS REVESTIMENTOS DE PAREDES, PISOS E FORROS
VERIFICAR O ESTADO DE CONSERVAÇÃO E DE LIMPEZA DE CALHAS E DEMAIS CONDUTORES DE ÁGUAS PLUVIAIS
VERIFICAR OCORRÊNCIAS DE INFILTRAÇÕES
Tempo Padrão
Data Base
01/07/2022
Horário
Técnico
Selecione o Técnico
SALVAR PLANO
Dicas
1. Apenas equipamentos que possuam ativos cadastrados poderão receber um plano de manutenção.
2. Em caso de data base única para múltiplos ativos, todas as preventivas serão agendadas para o mesmo dia.

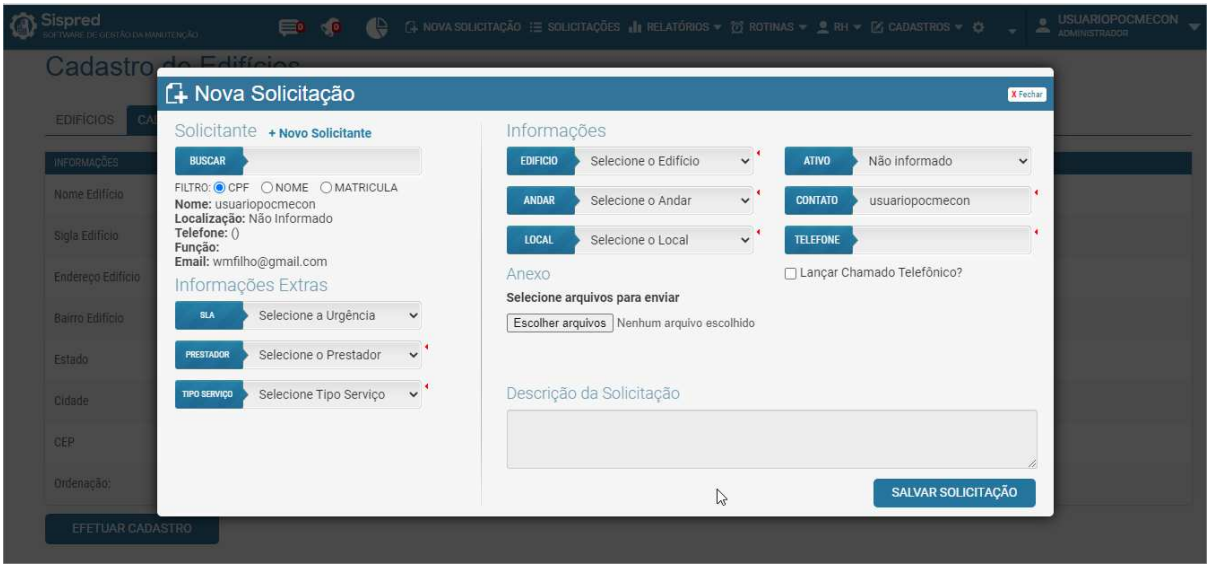

Sispred
Cadastro Plano Manutenção Preventiva
PLANOS DE MANUTENÇÃO PREVENTIVA
CADASTRAR PLANO DE MANUTENÇÃO
DADOS
SUCESSO
PLANO MANUTENÇÃO CADASTRADO COM SUCESSO!
Edifício
Andar
Local
Grupo Equipamento
Subgrupo Equipamento

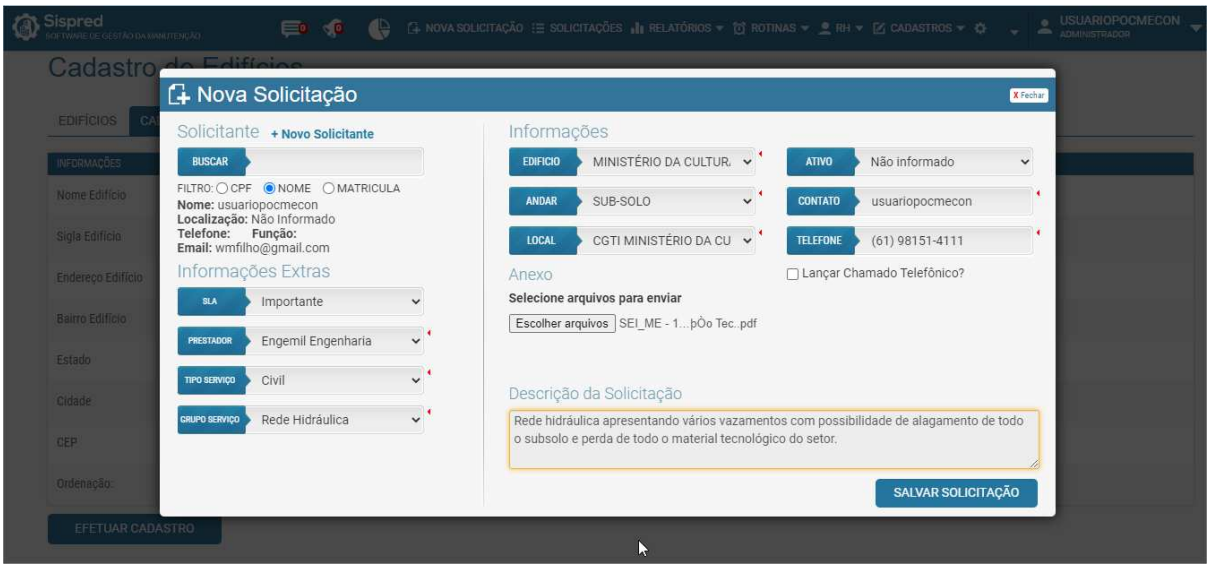

Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
ESTABILIZADOR ESTABILIZADOR 01 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 3º ANDAR - ESCADA CENTRAL Verificar o funcionamento das lâmpadas de sinalização Diária Editar
ESTABILIZADOR ESTABILIZADOR 01 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 6º ANDAR - ESCADA CENTRAL Inspeção visual do equipamento Diária Editar
ESTABILIZADOR ESTABILIZADOR 02 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 7º ANDAR - ESCADA CENTRAL Verificar o funcionamento das lâmpadas de sinalização Diária Editar
ESTABILIZADOR ESTABILIZADOR 02 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 9º ANDAR - ESCADA CENTRAL Inspeção visual do equipamento Diária Editar
ESTABILIZADOR ESTABILIZADOR 01 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 1º ANDAR - ESCADA CENTRAL Verificar o funcionamento das lâmpadas de sinalização Diária Editar
ESTABILIZADOR ESTABILIZADOR 01 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 5º ANDAR - ESCADA CENTRAL Inspeção visual do equipamento Diária Editar
ESTABILIZADOR ESTABILIZADOR 02 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 6º ANDAR - ESCADA CENTRAL Verificar o funcionamento das lâmpadas de sinalização Diária Editar
ESTABILIZADOR ESTABILIZADOR 02 ELÉTRICA / NOBREAKS E ESTABILIZADORES CONDOMÍNIO - 8º ANDAR - ESCADA CENTRAL Inspeção visual do equipamento Diária Editar
Subgrupo POC MECON Lenovo Ideapad S4000 PREDIAL / INFRAESTRUTURA CIVIL Edifício teste OS1532022 - OS1532022 - Ministério da Economia Verificar o estado de conservação dos revestimentos de paredes, pisos e forros Mensal Editar
Subgrupo POC MECON Lenovo Ideapad S4000 PREDIAL / INFRAESTRUTURA CIVIL Edifício teste OS1532022 - OS1532022 - Ministério da Economia Verificar e inspecionar as instalações observando o estado de conservação dos elementos estruturais e a existência de pontos danificados, fissuras, selamentos, deteriorações e patologias Mensal Editar
Subgrupo POC MECON Lenovo Ideapad S4000 PREDIAL / INFRAESTRUTURA CIVIL Edifício teste OS1532022 - OS1532022 - Ministério da Economia Verificar ocorrências de infiltrações Mensal Editar
Subgrupo POC MECON Lenovo Ideapad S4000 PREDIAL / INFRAESTRUTURA CIVIL Edifício teste OS1532022 - OS1532022 - Ministério da Economia Verificar o estado de conservação e de limpeza de calhas e demais condutores de águas pluviais Mensal Editar
Subgrupo POC MECON Lenovo Ideapad S4000 PREDIAL / INFRAESTRUTURA CIVIL Edifício teste OS1532022 - OS1532022 - Ministério da Economia Inspecionar periodicamente as instalações, e verificar o estado de conservação dos elementos de cobertura, observando a ocorrência de problemas como vazamentos, telhas quebradas e outros que possam existir, efetuando sua correção e recomposição sempre que necessário Mensal Editar
Primeira 73 74 75 76 77 última
Licenciado para: mma (testes)
v 5.0.0.MANUAL - Copyright © 2010 - 2022 | www.sispred.com.br

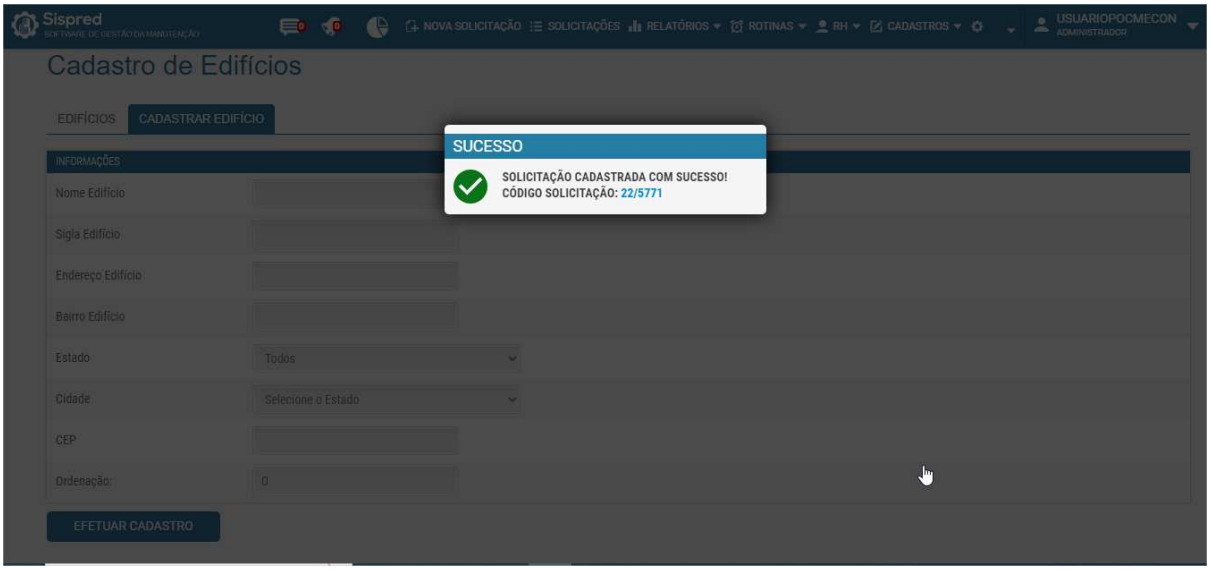
Status: **Não aderente**. No cadastro das atividades, conforme informado na análise do item 7, a funcionalidade de Solicitações precisa ser ajustada para uma futura avaliação e aderência ao edital.

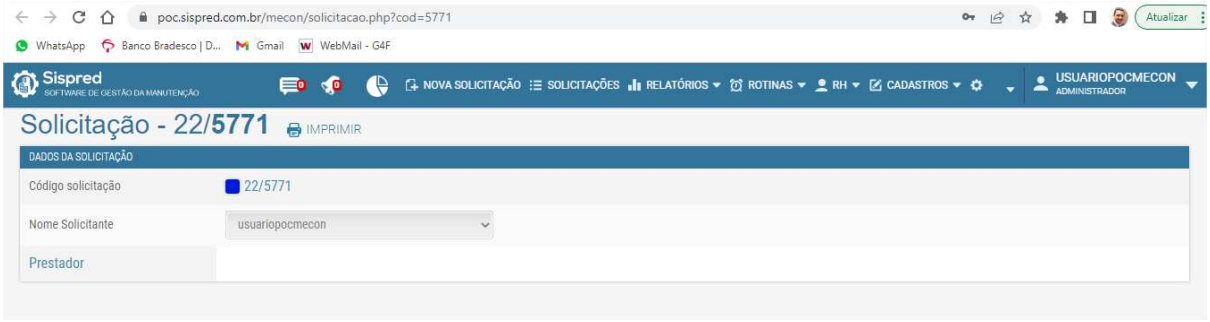
7 – Cadastro das atividades - abertura de chamados pelos usuários do prédio

Trilha de Navegação: Menu Principal -> Nova Solicitação -> Solicitações





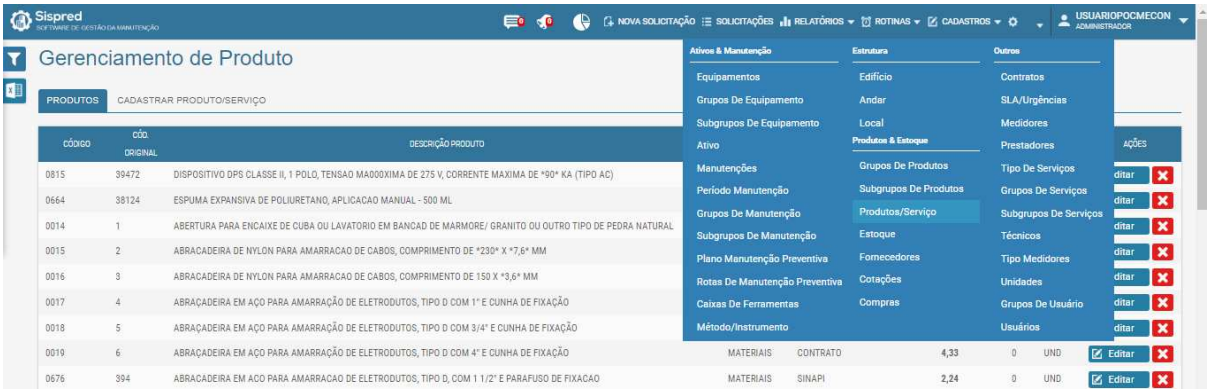


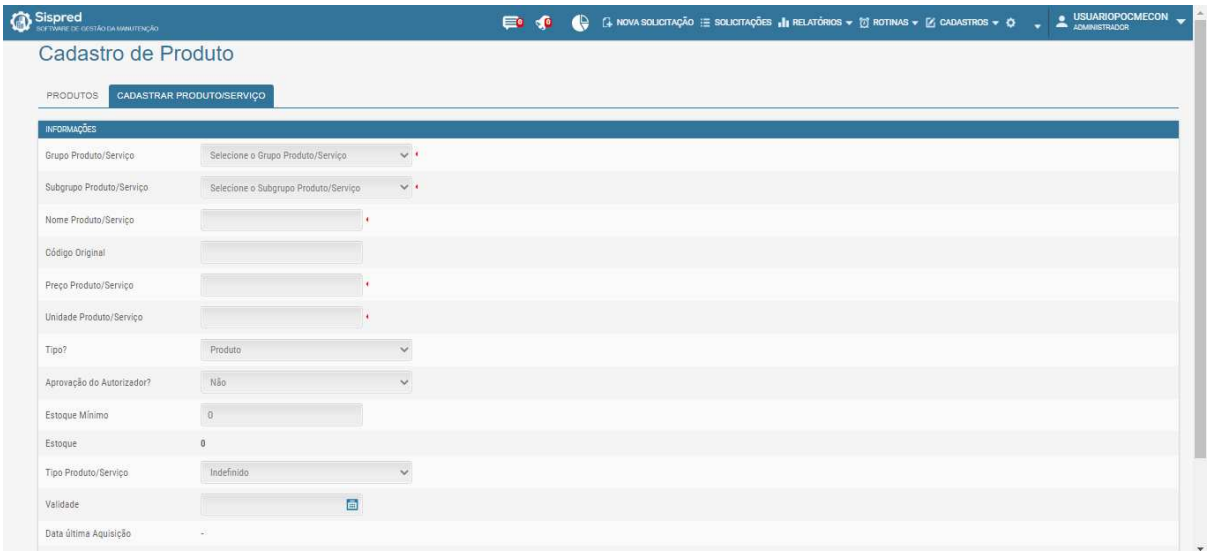


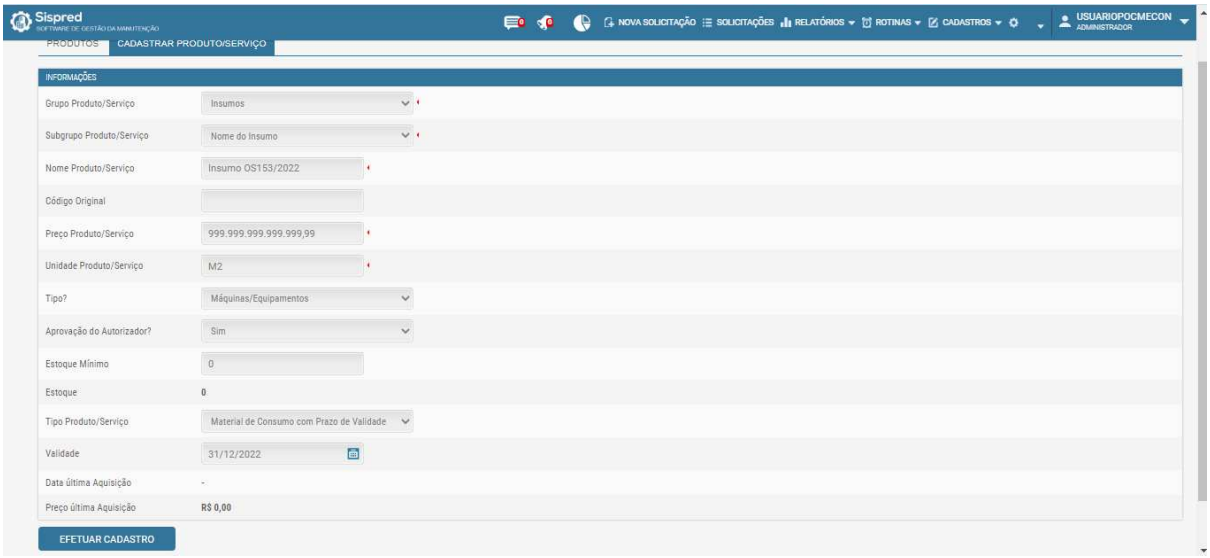
Status: **Não aderente**. No cadastro das atividades, após o cadastro da solicitação/chamado, não foi possível validar toda a funcionalidade e verificar a aderência e todos os campos conforme solicitados na TR. O sistema apresenta erro e não carrega toda a página para evolução do chamado. Funcionalidade necessita ser ajustada para uma futura avaliação e aderência ao edital.

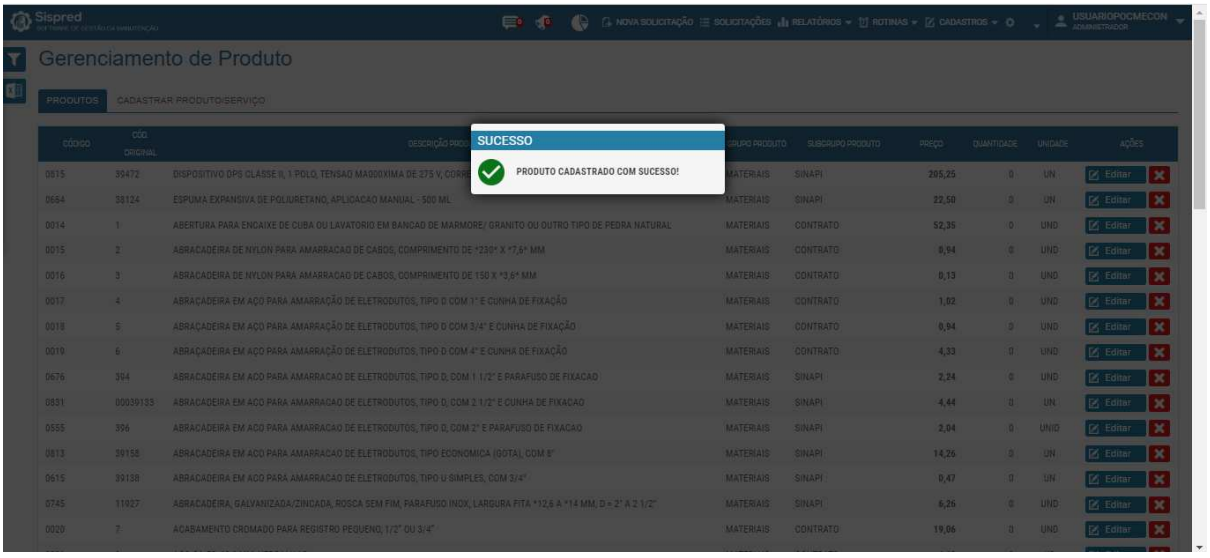
8 – Cadastro de Insumos

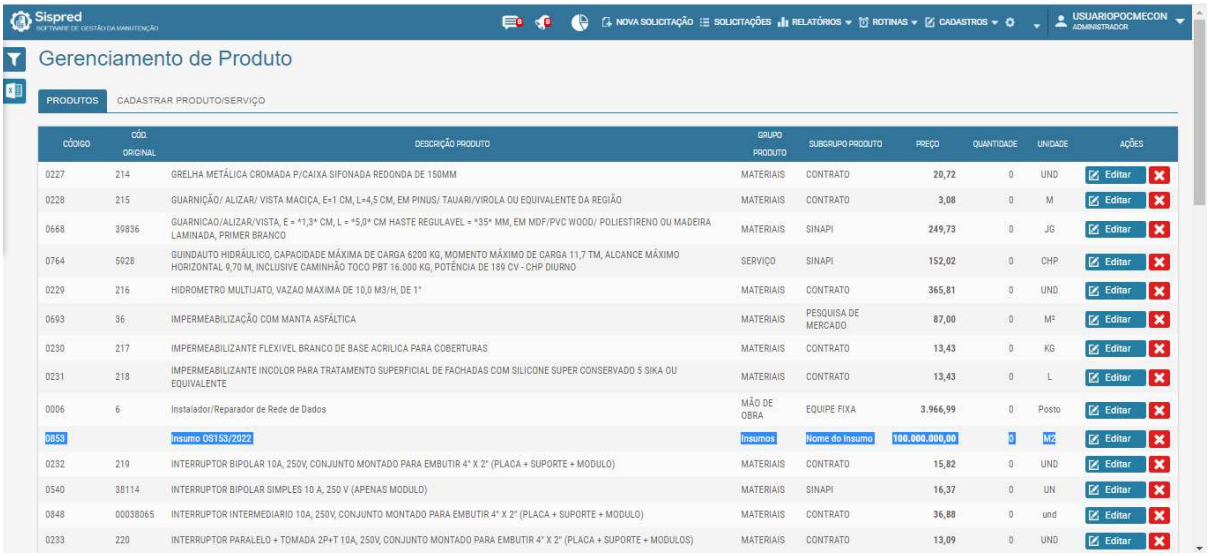
Trilha de Navegação: Menu Principal -> Cadastros -> Produtos & Estoque -> Produtos/Serviço -> Cadastrar Produto/Serviço






Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
PRODUTOS
CADASTRAR PRODUTO/SERVIÇO
INFORMAÇÕES
Grupo Produto/Serviço
Insumos
Subgrupo Produto/Serviço
Nome do Insumo
Nome Produto/Serviço
Insumo OS153/2022
Código Original
Preço Produto/Serviço
999.999.999.999.999,99
Unidade Produto/Serviço
M2
Tipo?
Máquinas/Equipamentos
Aprovação do Autorizador?
Sim
Estoque Mínimo
0
Estoque
0
Tipo Produto/Serviço
Material de Consumo com Prazo de Validade
Validade
31/12/2022
Data última Aquisição
-
Preço última Aquisição
R$ 0,00
EFETUAR CADASTRO

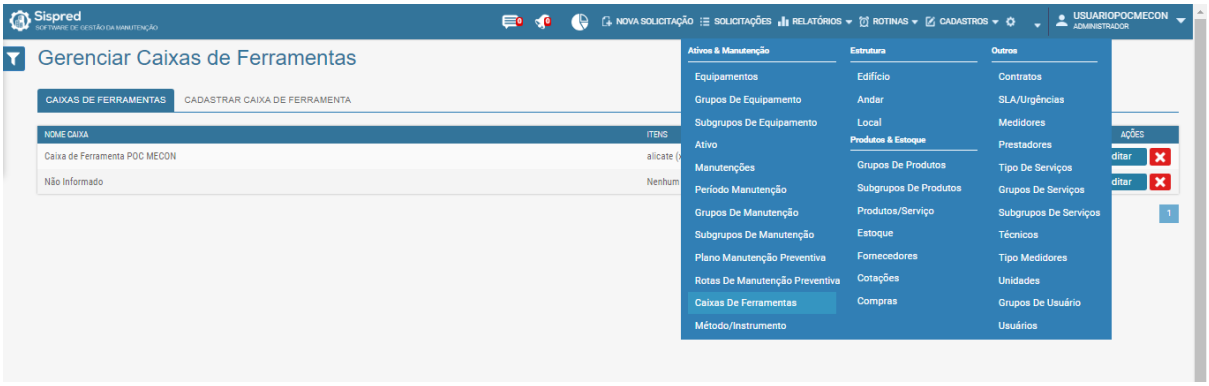

Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Gerenciamento de Produto
PRODUTOS
CADASTRAR PRODUTO/SERVIÇO
SUCESSO
PRODUTO CADASTRADO COM SUCESSO!

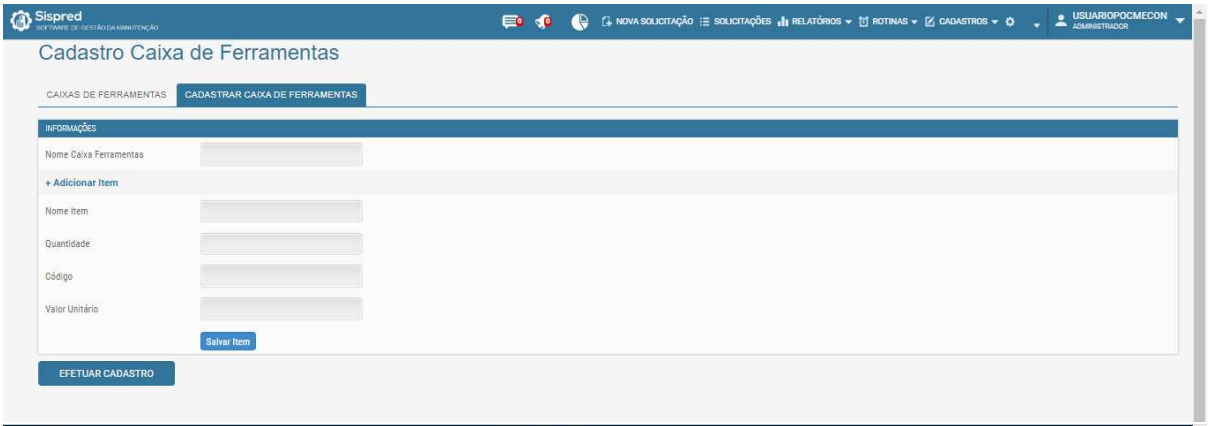


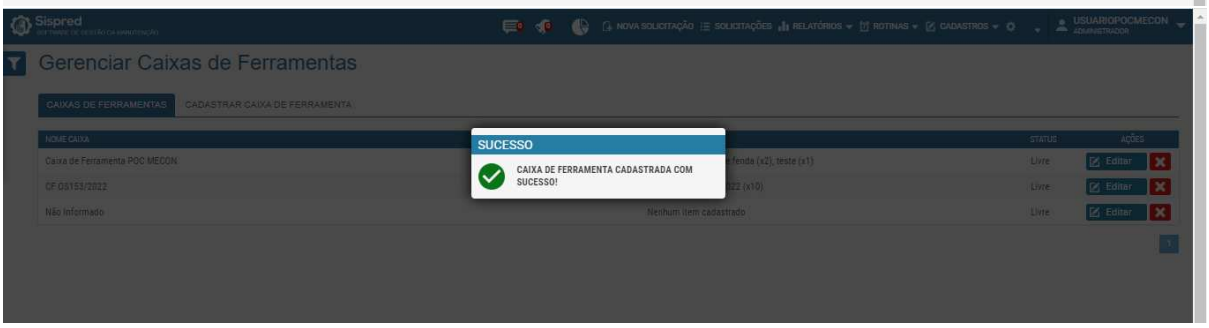
Status: Aderente.

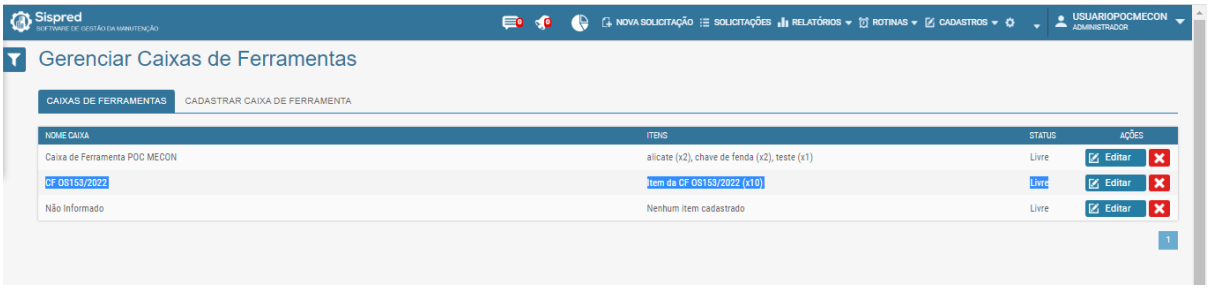
9 – Cadastro de Ferramentas

Trilha de Navegação: Menu Principal -> Cadastros -> Ativos & Manutenção -> Caixas de Ferramentas -> Cadastrar Caixa de Ferramenta





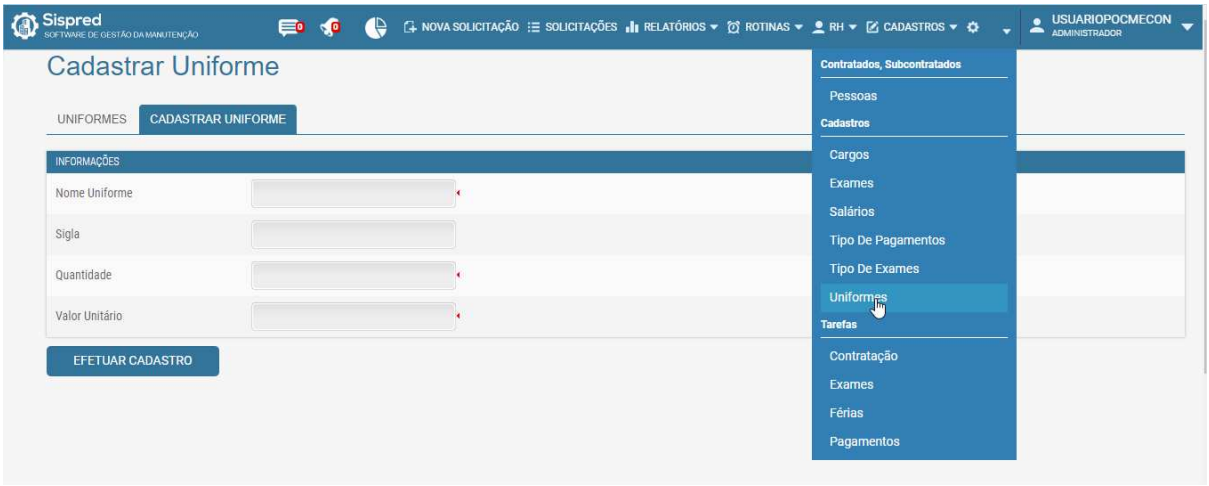


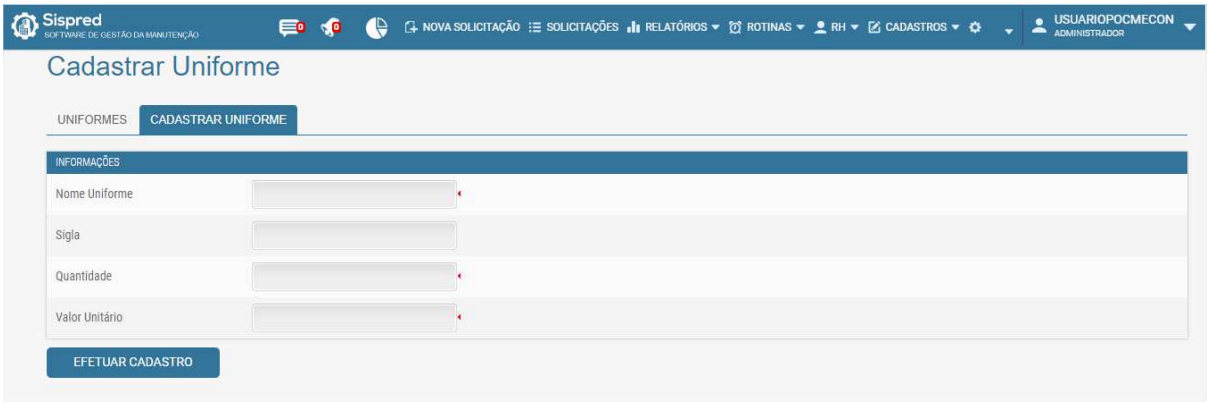


Status: Aderente

10 – Cadastro de Uniformes

Trilha de Navegação: Menu Principal -> RH -> Cadastros -> Uniformes -> Cadastrar Uniforme

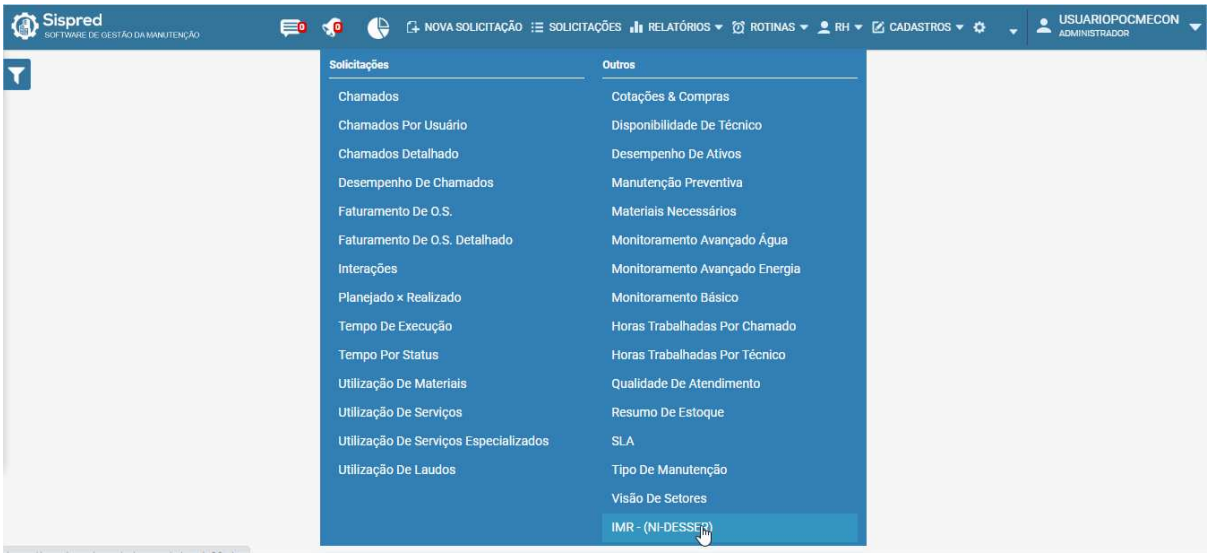


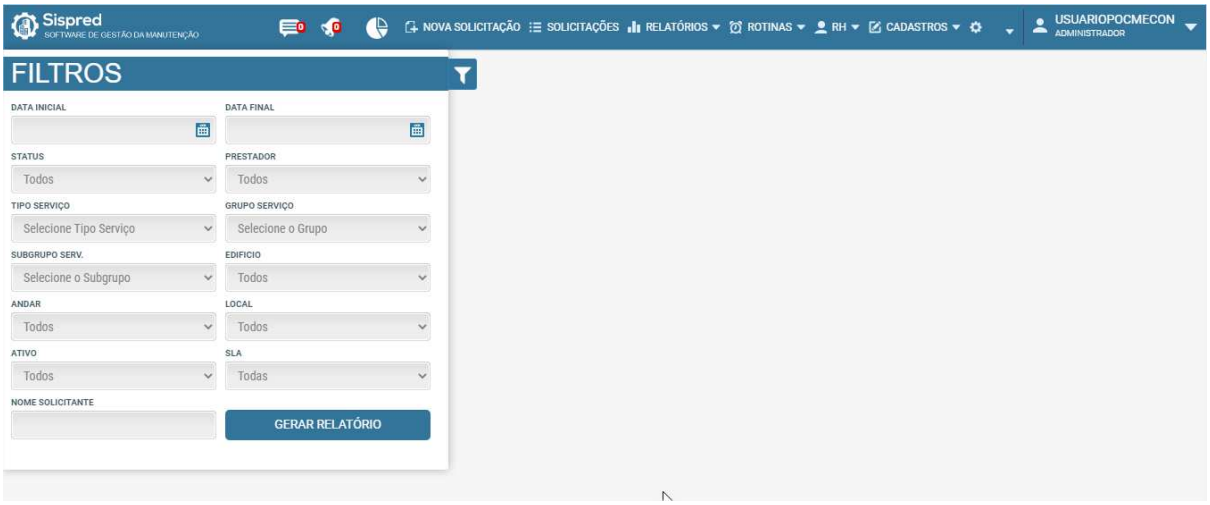


Status: **Não aderente.** No cadastro de uniformes, não apresenta campo para o cadastro do código do uniforme cadastrado, bem como o controle dos uniformes utilizados. A listagem dos uniformes cadastrados apresenta as informações invertidas necessitando de ajustes funcionais.

11 - IMR - Indicador de desempenho 1 -Nível de desconformidade dos serviços (NI-DESSER)

Trilha de Navegação: Menu Principal -> Relatórios -> Outros -> IMR – (NI-DESSER)

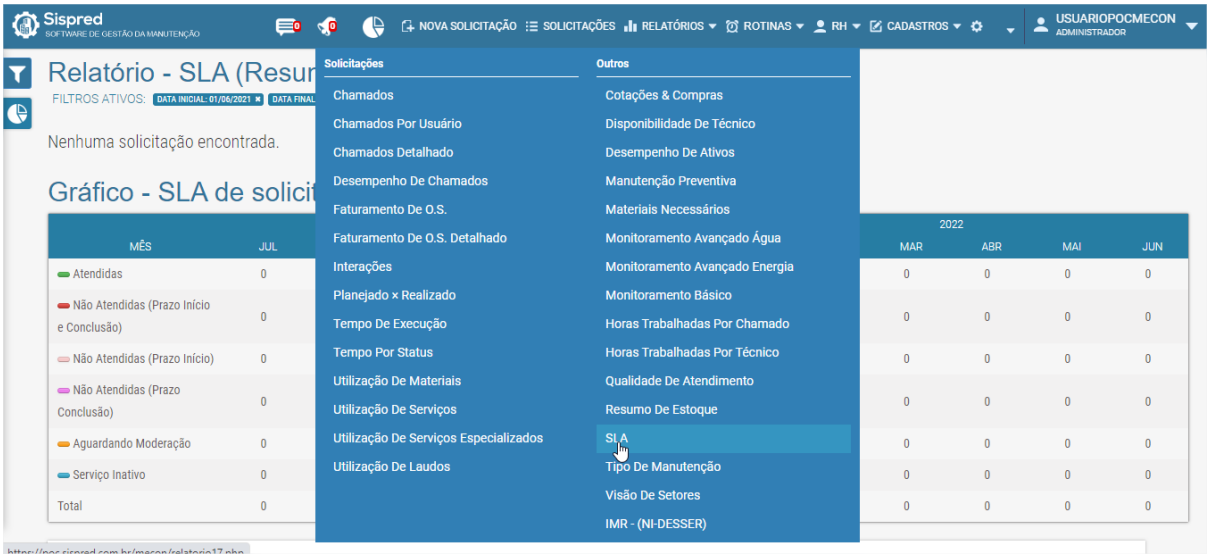




Status: **Não aderente.** Devido a disponibilização da funcionalidade somente no último dia da prova de conceito, o sistema não traz informações disponíveis para a geração de relatório e validação da aderência de todas as informações solicitadas no edital.

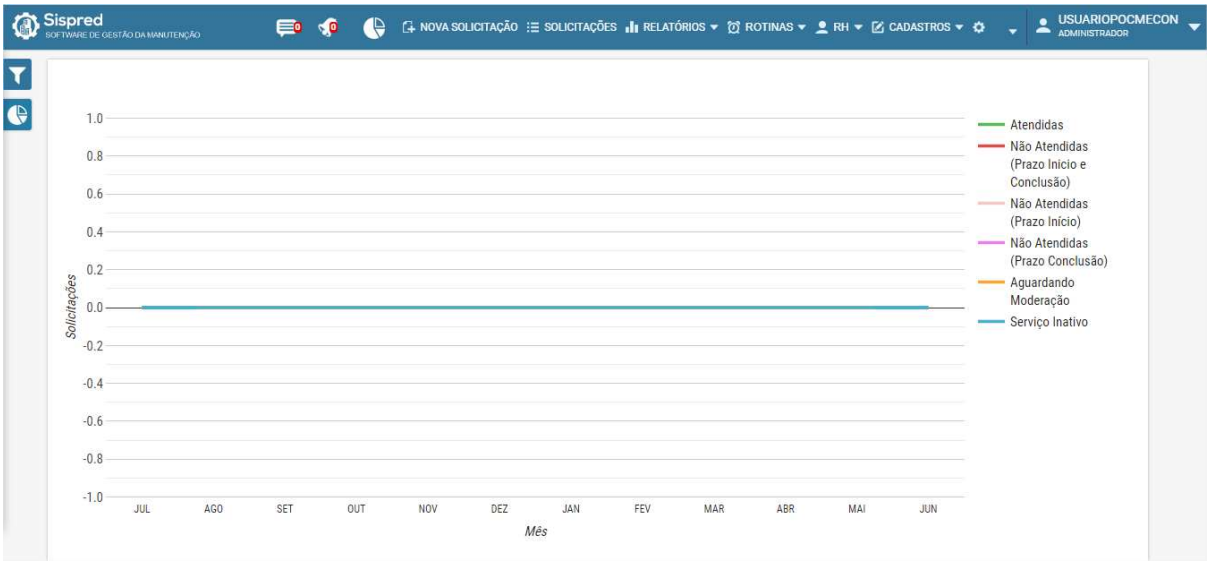
12 - IMR - Indicador de desempenho 2 - Nível de atendimento das solicitações no prazo (NI-TEMPO)

Trilha de Navegação: Menu Principal -> Relatórios -> Outros -> SLA




Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
FILTROS
EXIBIR
Solicitações por período
STATUS
Todos
DATA INICIAL
01/06/2021
PRESTADOR
Todos
DATA FINAL
24/06/2022
TIPO SERVIÇO
Selecione Tipo Serviço
GRUPO SERVIÇO
Selecione o Grupo
SUBGRUPO SERV.
Selecione o Subgrupo
EDIFICIO
Todos
ANDAR
Todos
LOCAL
Todos
ATIVO
Todos
SLA
Todas
SITUAÇÃO DE SLA
Todas
OPERADOR
Todos
SALVAR FILTRO?
GERAR RELATÓRIO
LIMPAR FILTROS
Relatório - SLA (Resumo)
Gráfico - SLA de solicitações encerradas
2021
2022
OUT NOV DEZ JAN FEV MAR ABR MAI JUN

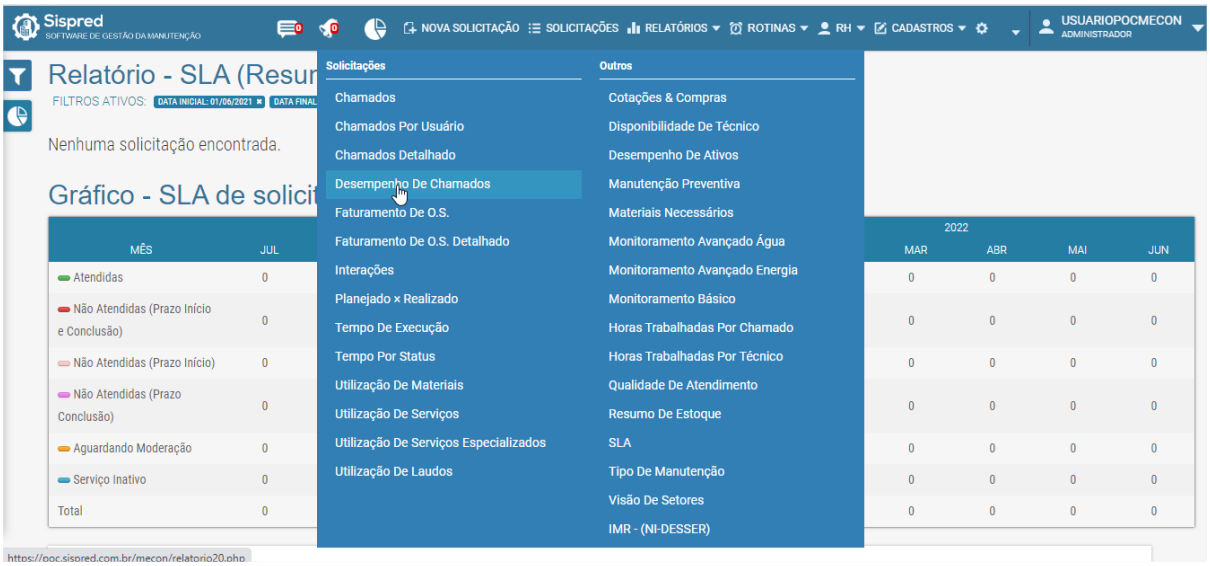

Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Relatório - SLA (Resumo)
FILTROS ATIVOS: DATA INICIAL: 01/06/2021 DATA FINAL: 24/06/2022
Nenhuma solicitação encontrada.
Gráfico - SLA de solicitações encerradas
2021
2022
MÊS JUL AGO SET OUT NOV DEZ JAN FEV MAR ABR MAI JUN
Atendidas
Não Atendidas (Prazo Início e Conclusão)
Não Atendidas (Prazo Início)
Não Atendidas (Prazo Conclusão)
Aguardando Moderação
Serviço Inativo
Total



Status: **Não aderente.** Devido a disponibilização da funcionalidade somente no último dia da prova de conceito, o sistema não traz informações disponíveis para a geração de relatório e validação da aderência de todas as informações solicitadas no edital.

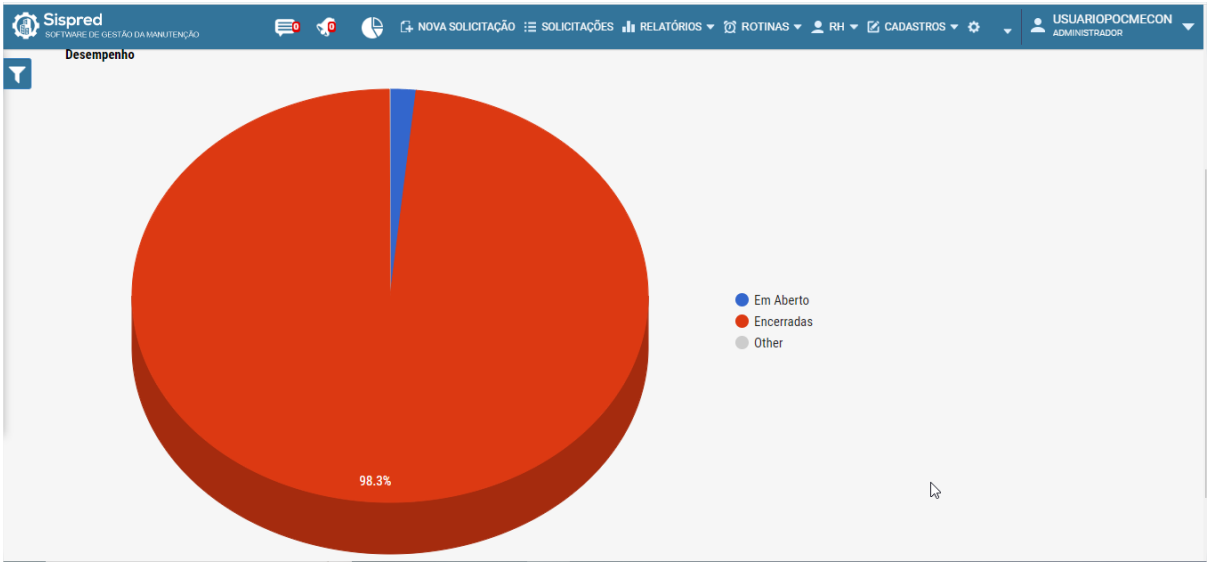
13 - IMR - Indicador de desempenho 3 - Nível de redução de serviços corretivos (NI-RED CORRET)

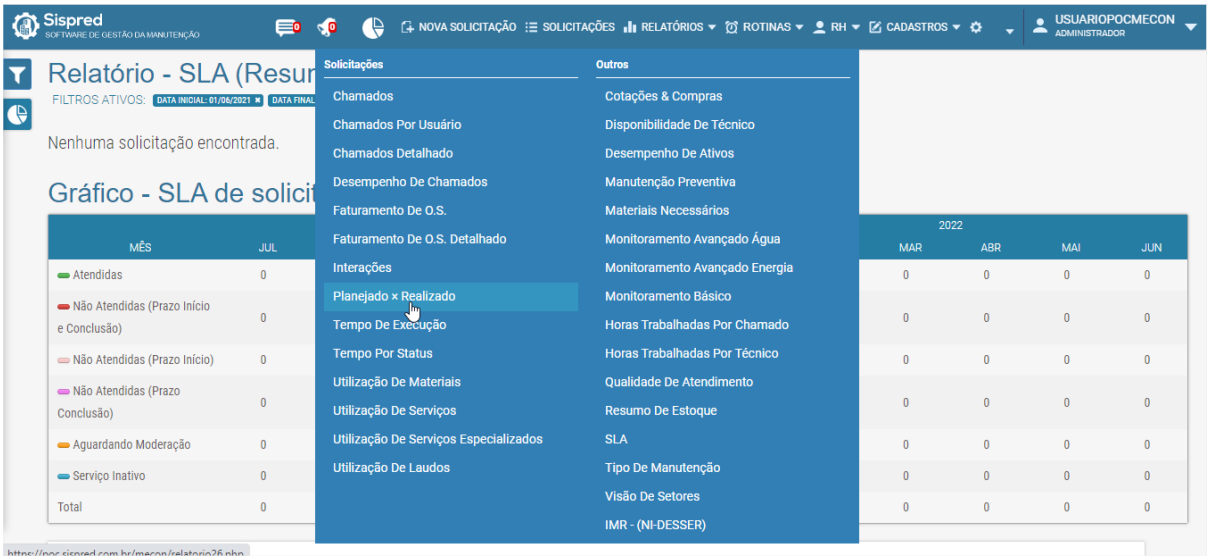
Trilha de Navegação: Menu Principal -> Relatórios -> Solicitações -> Desempenho De Chamados e Planejado X Realizado

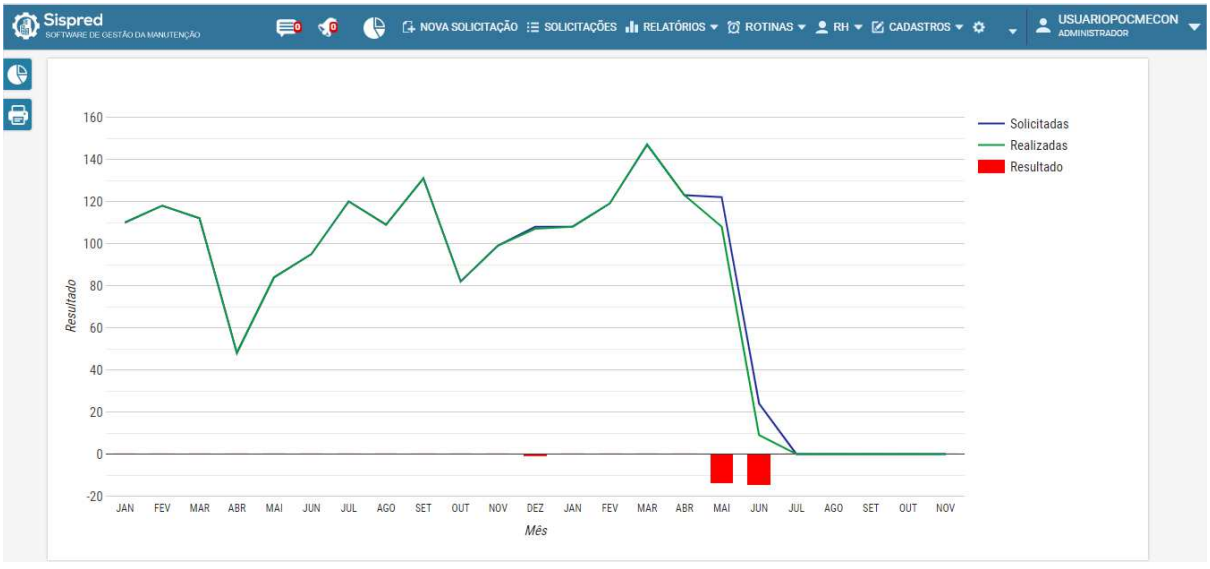



Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
FILTROS
Relatório - Desempenho de Chamados
DATA INICIAL
01/01/2021
DATA FINAL
STATUS
Todos
PRESTADOR
Todos
TIPO SERVIÇO
Selecione Tipo Serviço
GRUPO SERVIÇO
Selecione o Grupo
SUBGRUPO SERV.
Selecione o Subgrupo
EDIFICIO
Todos
ANDAR
Todos
LOCAL
Todos
ATIVO
Todos
OPERADOR
Todos
SLA
Todas
GERAR RELATÓRIO


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Relatório - Desempenho de Chamados
INFORMAÇÕES
Em Aberto 1860
Encerradas 1829
Canceladas 1
Taxa de cancelamento 0.1%
Taxa de encerramento 98.3%


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Desempenho
98.3%
Em Aberto
Encerradas
Other

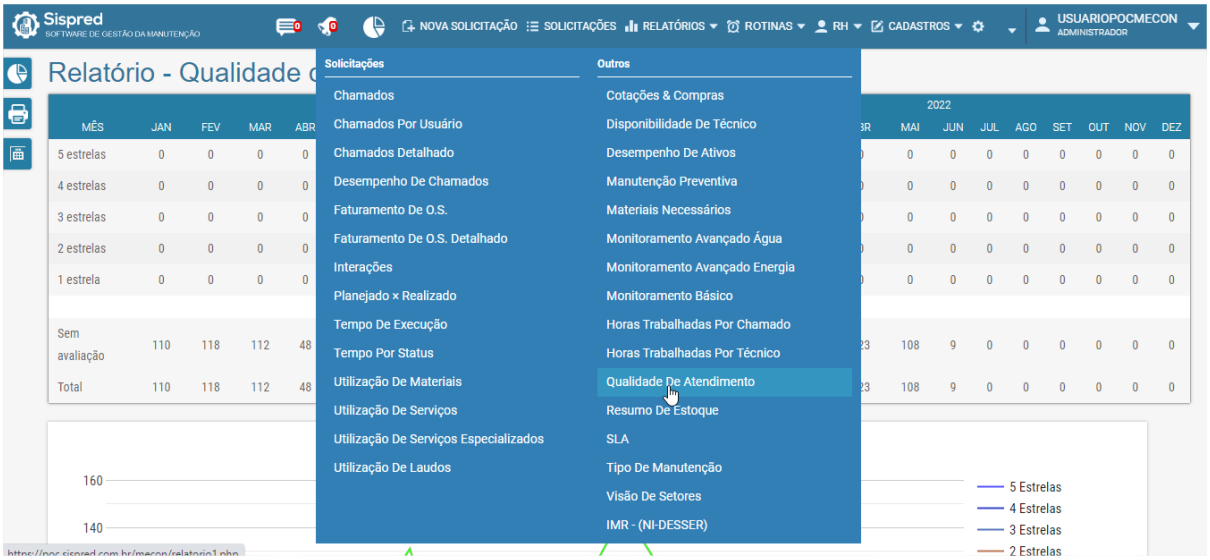


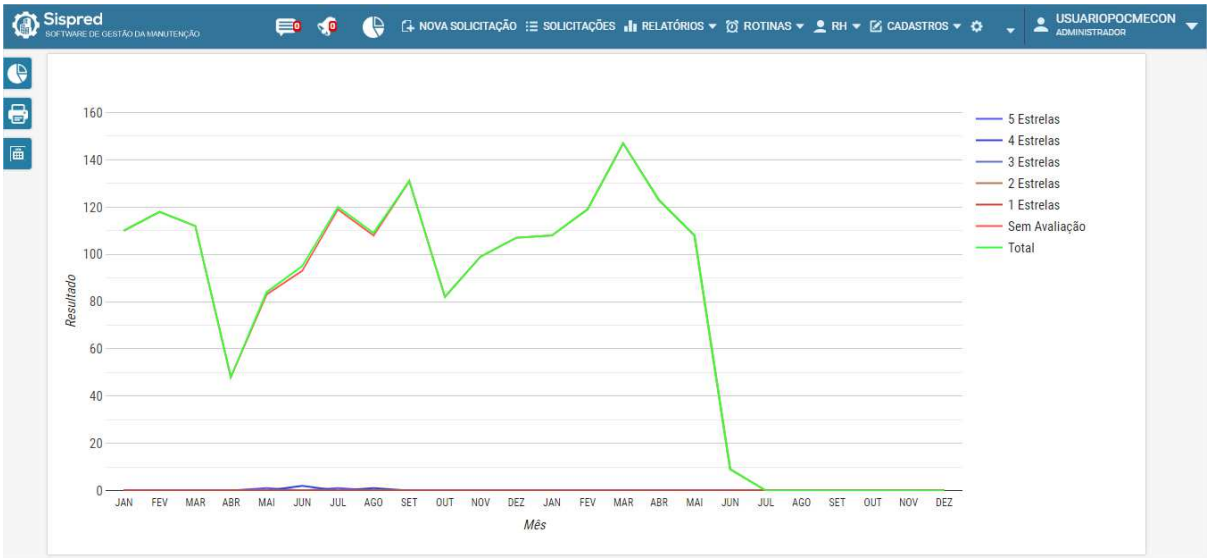


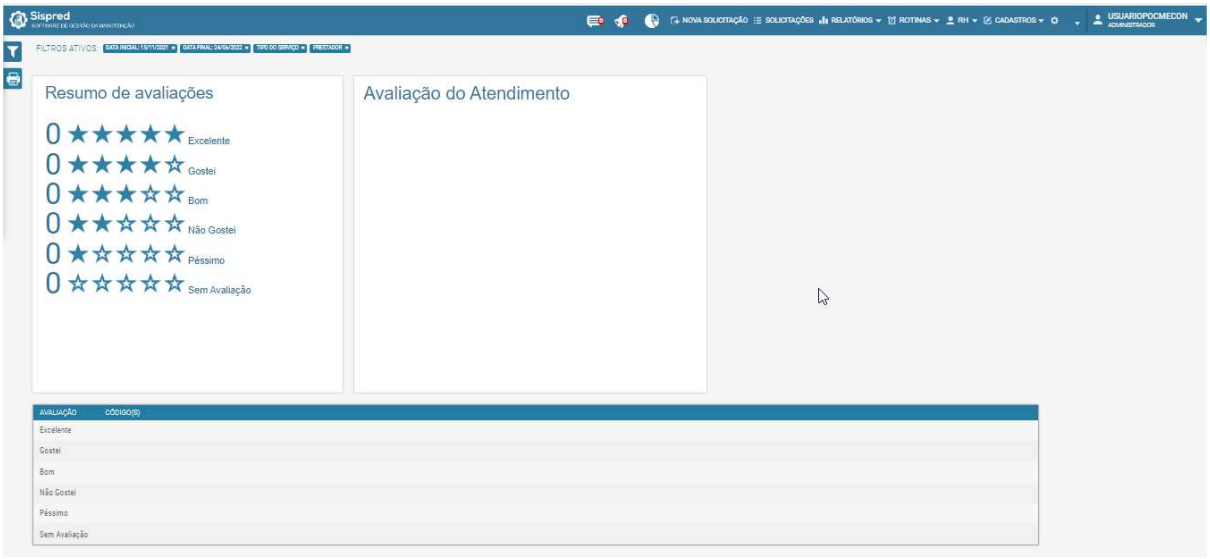
Status: **Não aderente.** Não foi possível identificar a inserção das equações de cálculo do IMR de forma a qualificar os indicadores de desempenho e nível de redução de serviços corretivos.

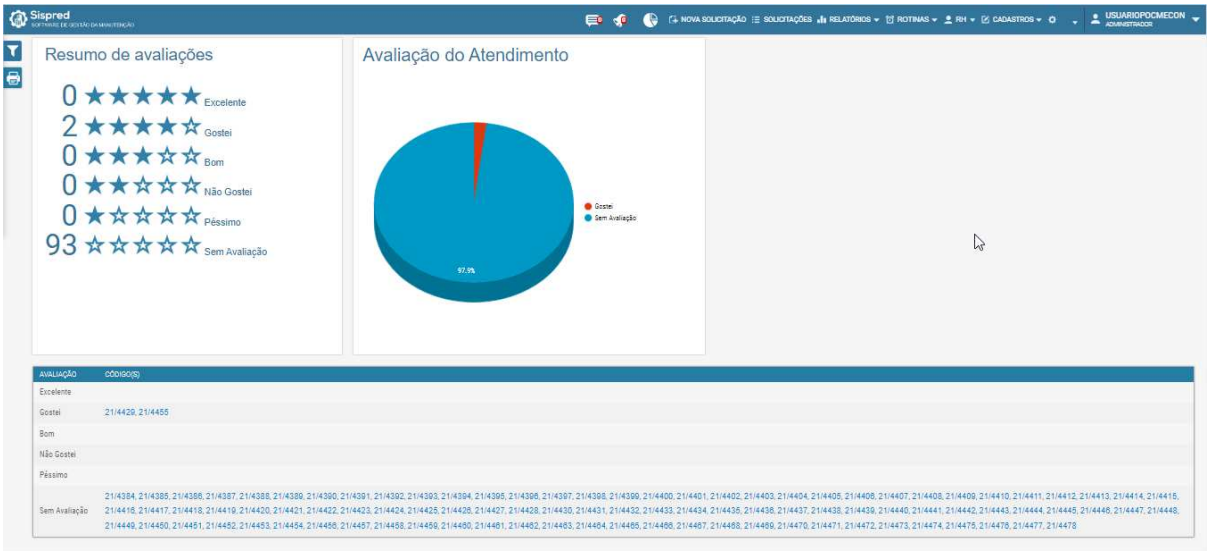
14 - IMR - Indicador de desempenho 4 - Nível de satisfação dos usuários (NISATIU)

Trilha de Navegação: Menu Principal -> Relatórios -> Outros -> Qualidade De Atendimento




Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
160
140
120
100
80
60
40
20
0
Resultado
JAN FEV MAR ABR MAI JUN JUL AGO SET OUT NOV DEZ JAN FEV MAR ABR MAI JUN JUL AGO SET OUT NOV DEZ
Mês
5 Estrelas
4 Estrelas
3 Estrelas
2 Estrelas
1 Estrelas
Sem Avaliação
Total

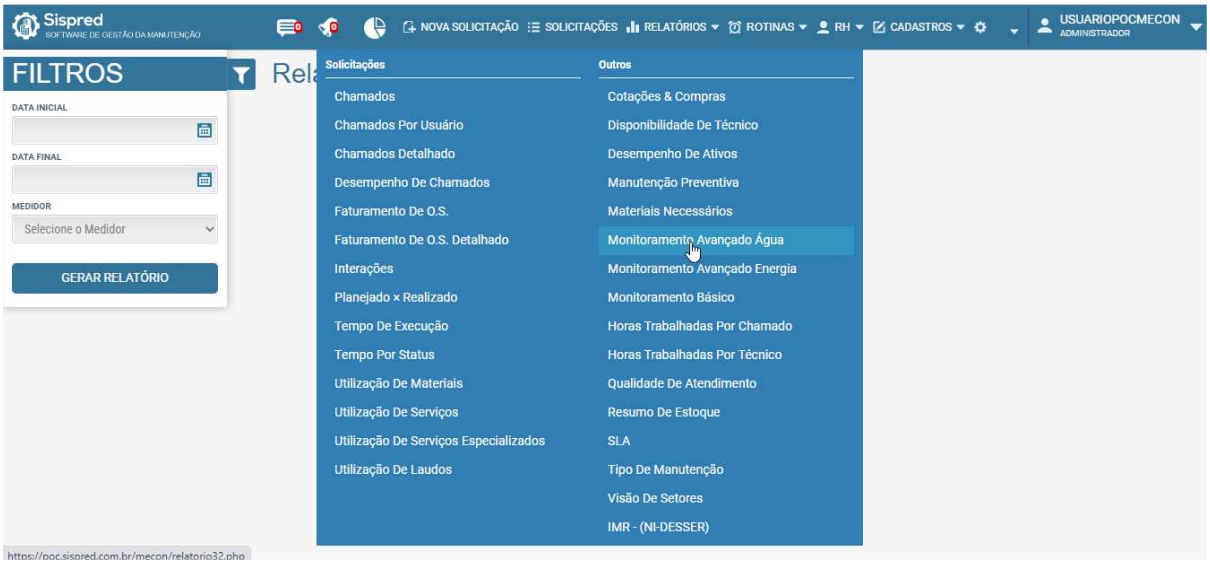

Sispred
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
FILTROS ATIVOS:
Resumo de avaliações
0 Excelente
0 Gostei
0 Bom
0 Não Gostei
0 Péssimo
0 Sem Avaliação
Avaliação do Atendimento
AVALIAÇÃO
CÓDIGO(S)
Excelente
Gostei
Bom
Não Gostei
Péssimo
Sem Avaliação



Status: **Não aderente.** Não foi possível identificar as informações referentes a identificação do avaliador, data da avaliação, identificação do serviço avaliado, nota concedida e a inserção das equações de cálculo do IMR de forma a qualificar os indicadores de desempenho e nível de satisfação dos usuários.

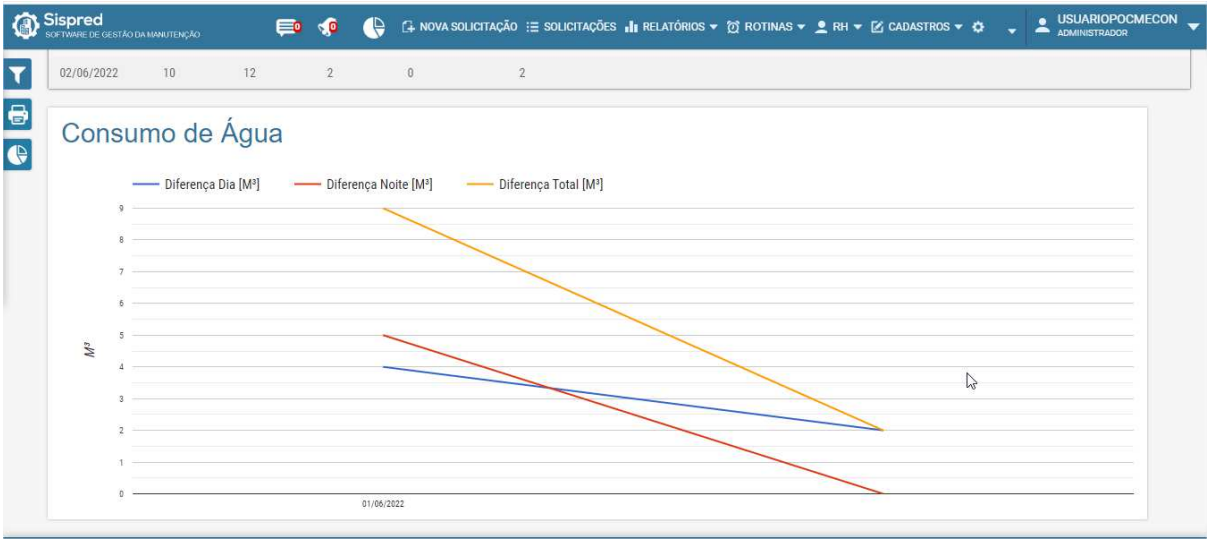
15 - IMR - Indicador de desempenho 5 - Nível de progresso de sustentabilidade (NI-PRO-SUS)

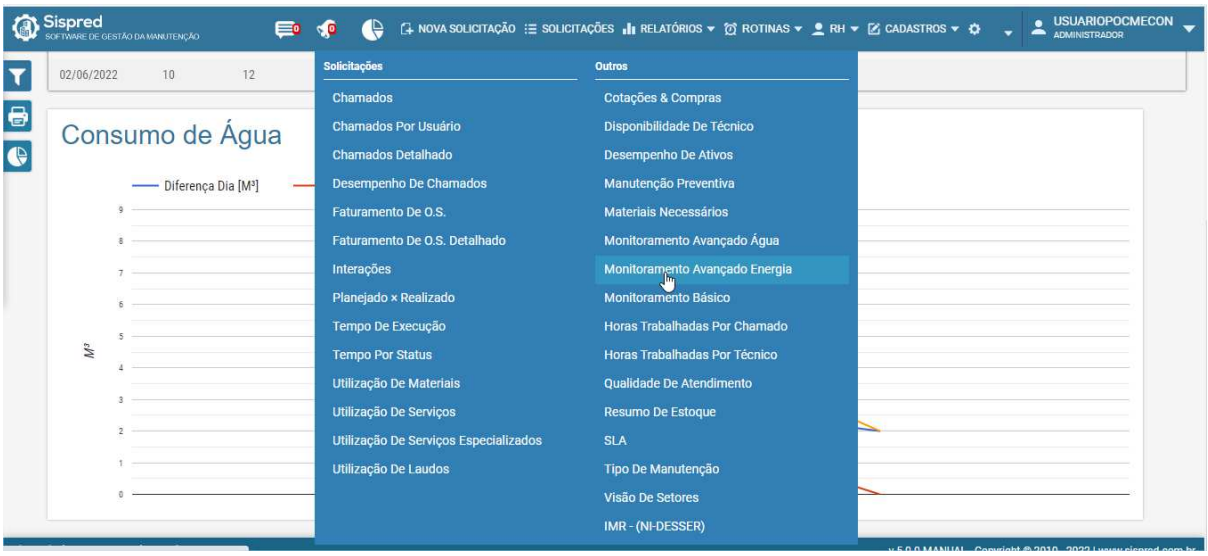
Trilha de Navegação: Menu Principal -> Relatórios -> Outros -> Monitoramento Avançado Água e Monitoramento Avançado Energia

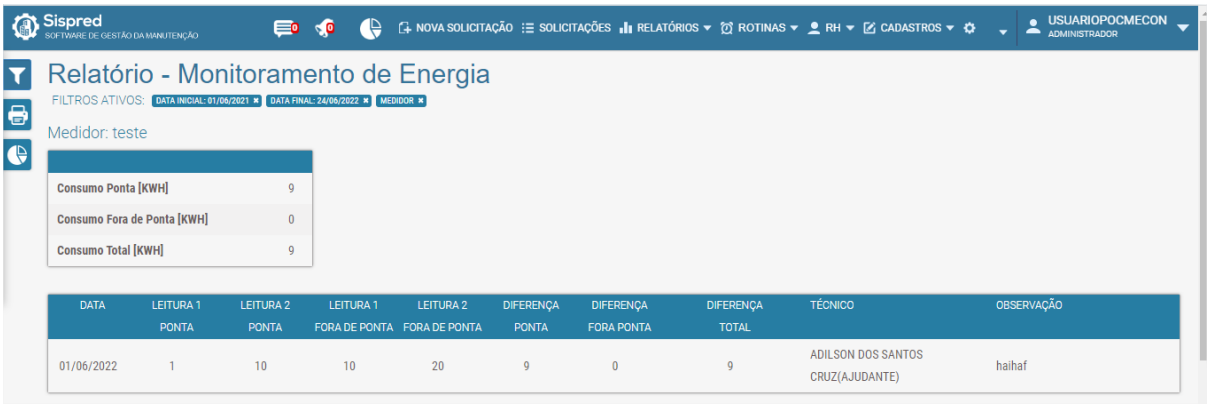


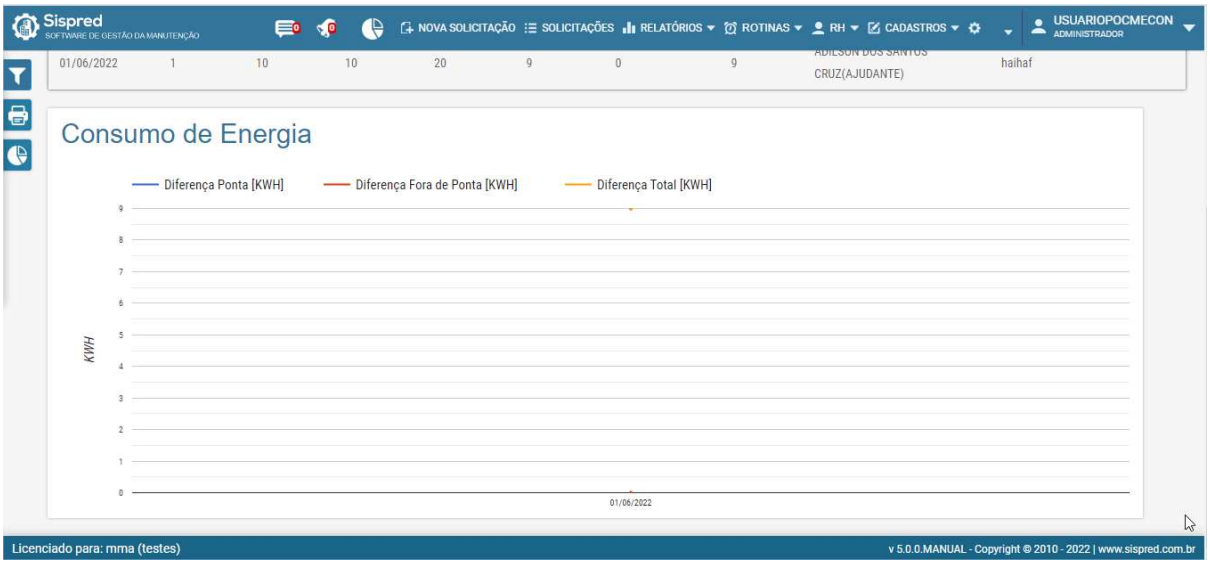

Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
FILTROS
Relatório - Monitoramento de Água
DATA INICIAL
01/06/2021
DATA FINAL
24/06/2022
MEDIDOR
teste
GERAR RELATÓRIO


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Relatório - Monitoramento de Água
FILTROS ATIVOS:
DATA INICIAL: 01/06/2021
DATA FINAL: 24/06/2022
MEDIDOR
Medidor: teste
Consumo Dia [M³] 6
Consumo Noite [M³] 5
Consumo Total [M³] 11
DATA
LEITURA MANHÃ
LEITURA TARDE
DIFERENÇA DIA
DIFERENÇA NOITE
DIFERENÇA TOTAL
TÉCNICO
OBSERVAÇÃO
01/06/2022 1 5 4 5 9 Glaugelio Aquino dos Santos (Pintor) fjisdjfoi
02/06/2022 10 12 2 0 2


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
02/06/2022 10 12 2 0 2
Consumo de Água
Diferença Dia [M³]
Diferença Noite [M³]
Diferença Total [M³]
M³
9
8
7
6
5
4
3
2
1
0
01/06/2022


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
02/06/2022
10
12
Consumo de Água
Diferença Dia [M³]
M³
Solicitações
Chamados
Chamados Por Usuário
Chamados Detalhado
Desempenho De Chamados
Faturamento De O.S.
Faturamento De O.S. Detalhado
Interações
Planejado x Realizado
Tempo De Execução
Tempo Por Status
Utilização De Materiais
Utilização De Serviços
Utilização De Serviços Especializados
Utilização De Laudos
Outros
Cotações & Compras
Disponibilidade De Técnico
Desempenho De Ativos
Manutenção Preventiva
Materiais Necessários
Monitoramento Avançado Água
Monitoramento Avançado Energia
Monitoramento Básico
Horas Trabalhadas Por Chamado
Horas Trabalhadas Por Técnico
Qualidade De Atendimento
Resumo De Estoque
SLA
Tipo De Manutenção
Visão De Setores
IMR - (NI-DESSER)


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
Relatório - Monitoramento de Energia
FILTROS ATIVOS: DATA INICIAL: 01/06/2021 DATA FINAL: 24/06/2022 MEDIDOR
Medidor: teste
Consumo Ponta [KWH] 9
Consumo Fora de Ponta [KWH] 0
Consumo Total [KWH] 9
DATA
LEITURA 1 PONTA
LEITURA 2 PONTA
LEITURA 1 FORA DE PONTA
LEITURA 2 FORA DE PONTA
DIFERENÇA PONTA
DIFERENÇA FORA PONTA
DIFERENÇA TOTAL
TÉCNICO
OBSERVAÇÃO
01/06/2022
1
10
10
20
9
0
9
ADILSON DOS SANTOS CRUZ(AJUDANTE)
haihaf


Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
01/06/2022 1 10 10 20 9 0 9 CRUZ(AJUDANTE) haihaf
Consumo de Energia
Diferença Ponta [KWH]
Diferença Fora de Ponta [KWH]
Diferença Total [KWH]
KWH
01/06/2022
Licenciado para: mma (testes)
v 5.0.0.MANUAL - Copyright © 2010 - 2022 | www.sispred.com.br

Status: **Não aderente.** Não foi possível identificar as informações referentes aos consumos mensais de geração de resíduos e unidades. Taxa média de ocupação mensal do prédio e a inserção das equações de cálculo do IMR de forma a qualificar os indicadores de desempenho e nível de progresso de sustentabilidade.

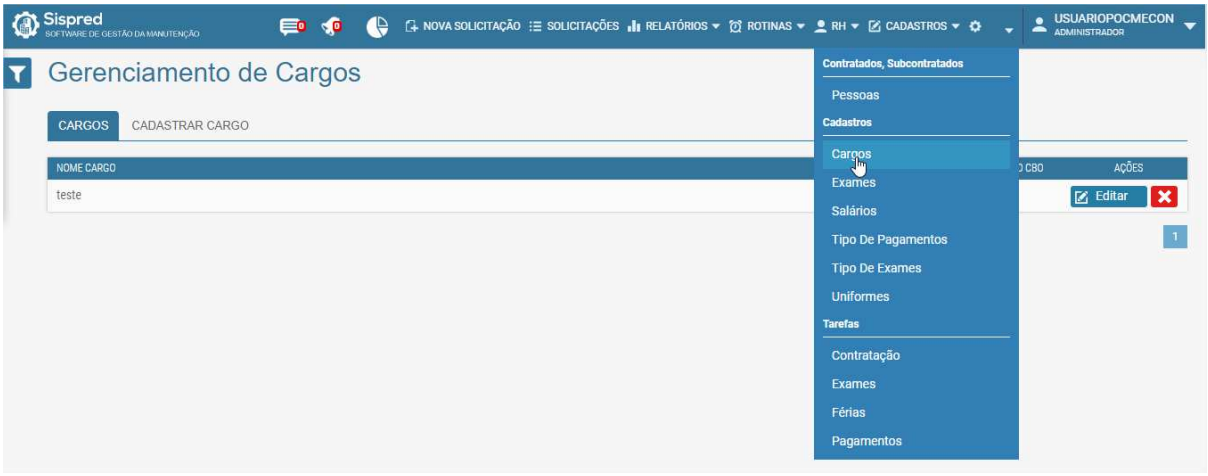
16 - Cadastramento de ACT, CCT ou DCT

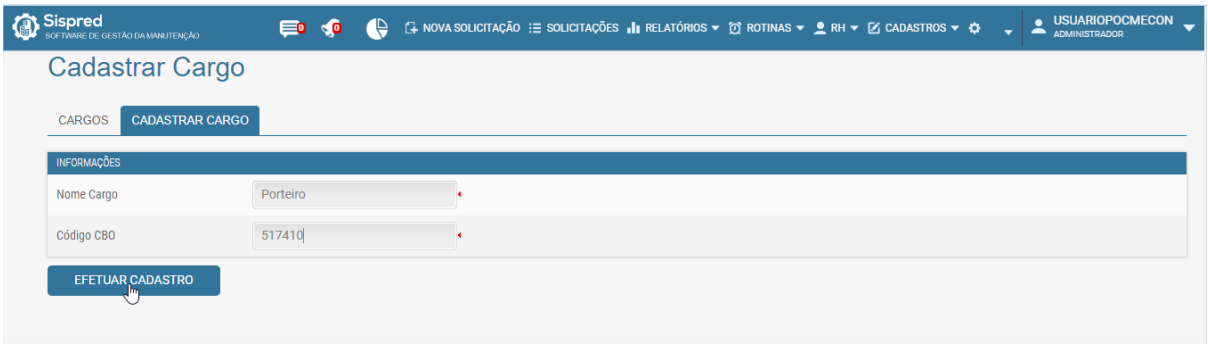
Trilha de Navegação: Menu Principal -> RH -> Cadastros

Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

17 - Cadastramento de cargos dos empregados da CONTRATADA

Trilha de Navegação: Menu Principal -> RH -> Cadastros -> Cargos -> Cadastrar Cargo

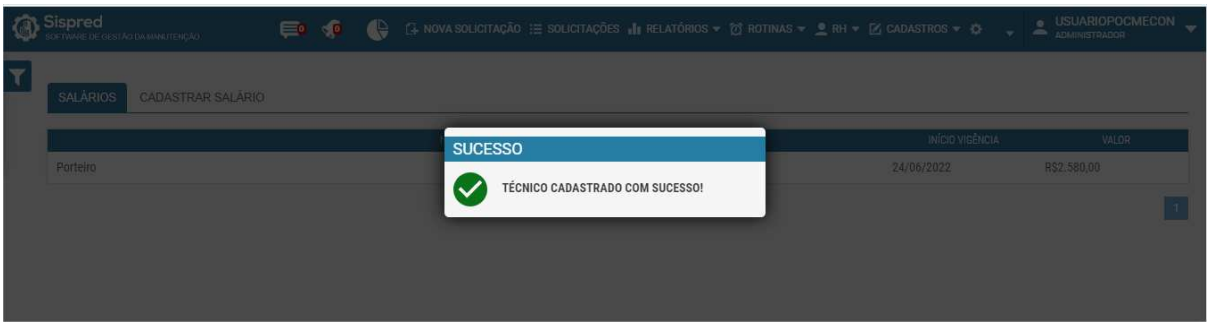




Status: **Aderente com ressalvas.**
Sugestão de melhoria/ajuste: Após a geração do Cargo do funcionário, deverá ser gerado o código de cadastro do cargo.

18 - Cadastramento de salário dos cargos dos empregados da CONTRATADA e da(s) subcontratada(s)

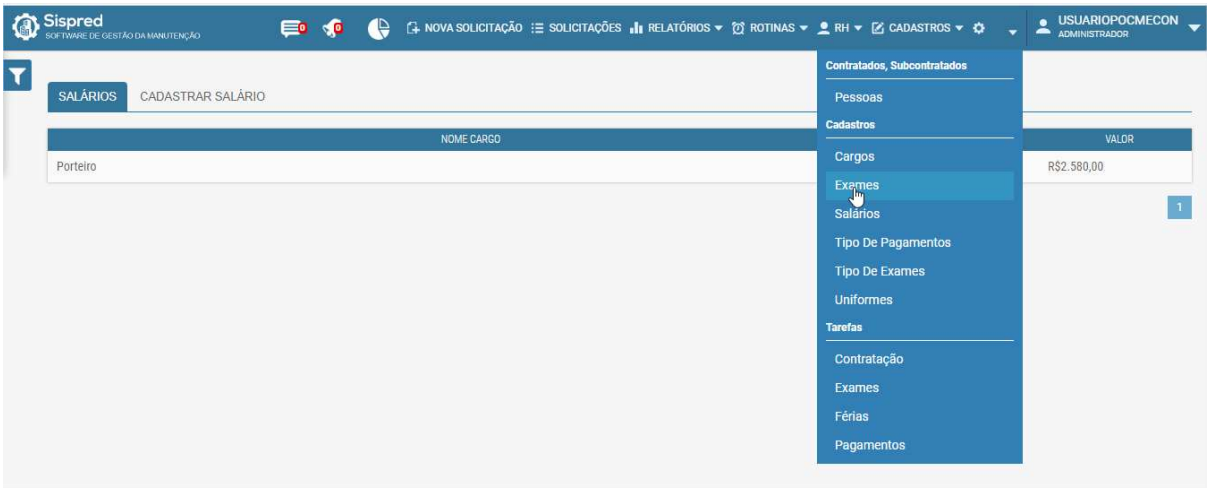
Trilha de Navegação: Menu Principal -> RH -> Cadastros -> Salários -> Cadastrar Salário

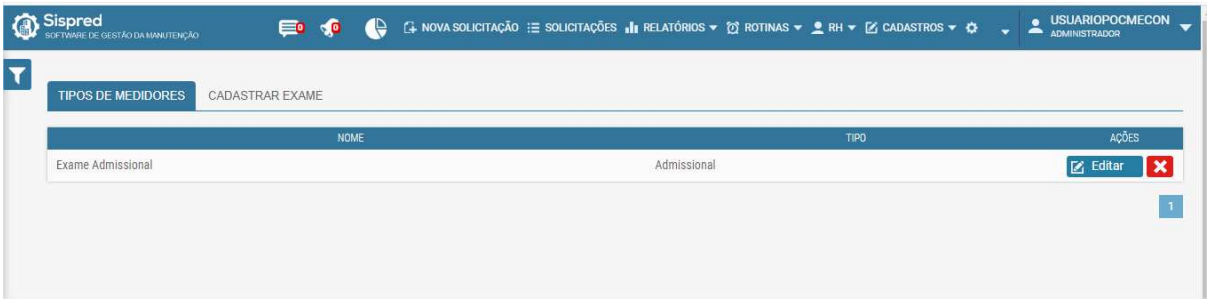


Status: Aderente com ressalvas.
Sugestão de melhoria/ajuste: Após a geração do Cargo do funcionário, deverá ser gerado o código de cadastro do cargo.

19 - Cadastramento de tipos de exames médicos CONTRATADA e da(s) subcontratada(s)

Trilha de Navegação: Menu Principal -> RH -> Cadastros -> Exames -> Cadastrar Exame



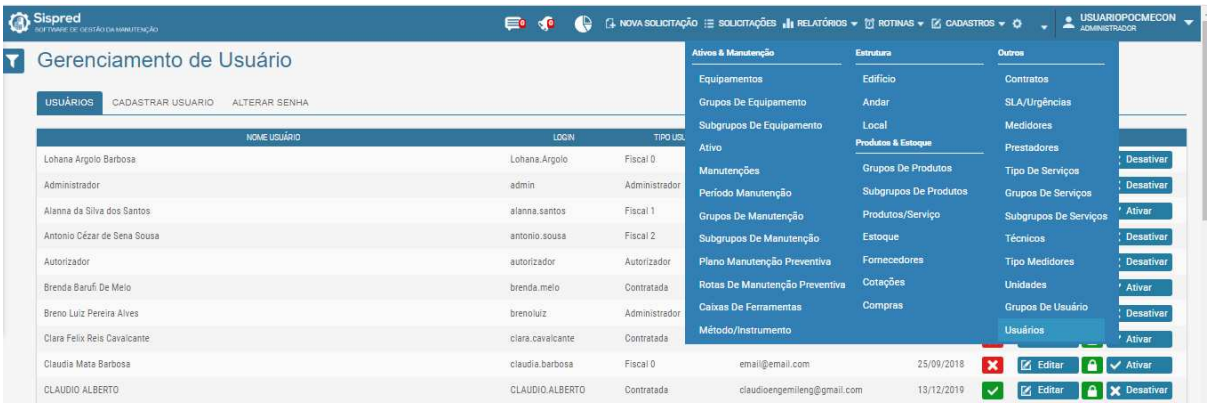


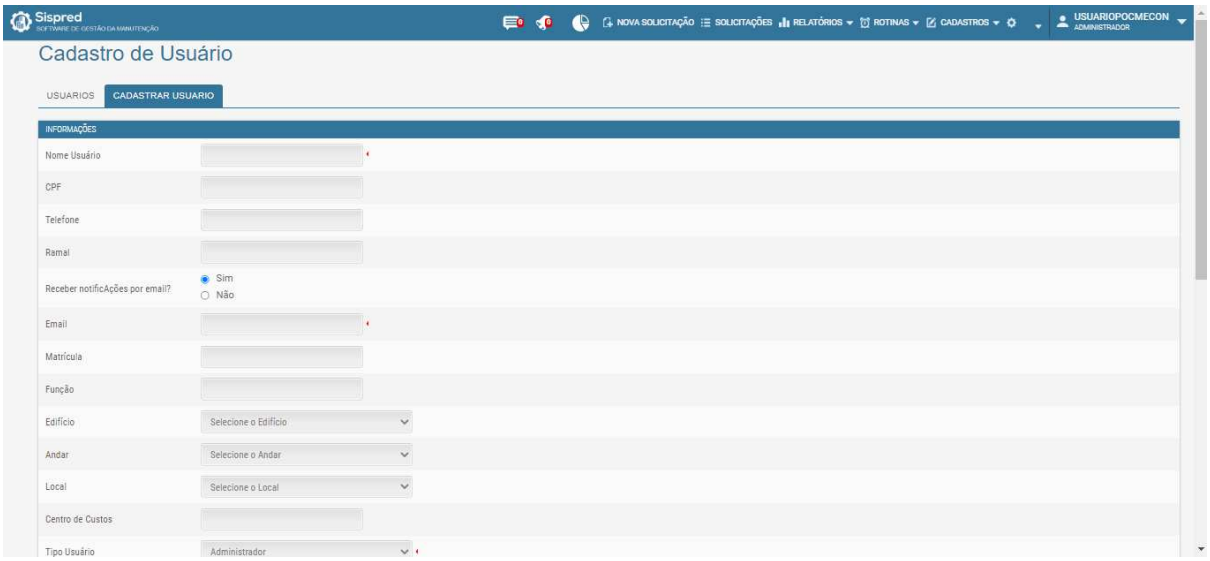
Status: Aderente com ressalvas.

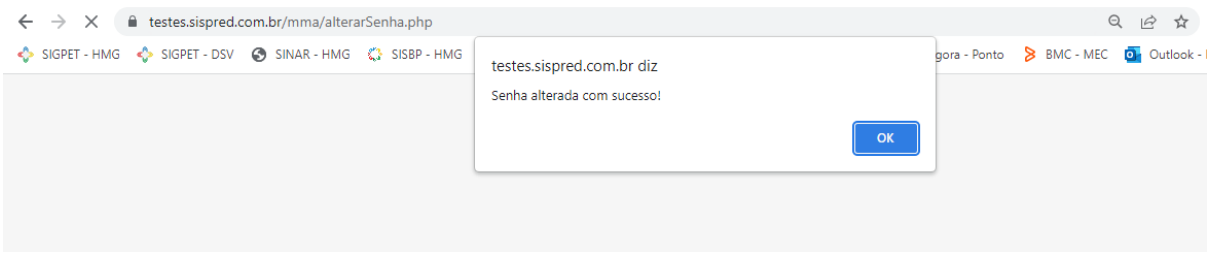
Sugestão de melhoria/ajuste: Após a geração do exame do funcionário, deverá ser gerado o código de cadastro do exame e vinculo ao CPF do funcionário que irá realizar o exame.

20 – Cadastramento de senha de acesso à solução tecnológica, com possibilidade de alteração a qualquer momento, inclusive nos casos de esquecimento da senha cadastrada

Trilha de Navegação: Menu Principal -> Cadastros -> Outros -> Usuários -> Alterar Senha



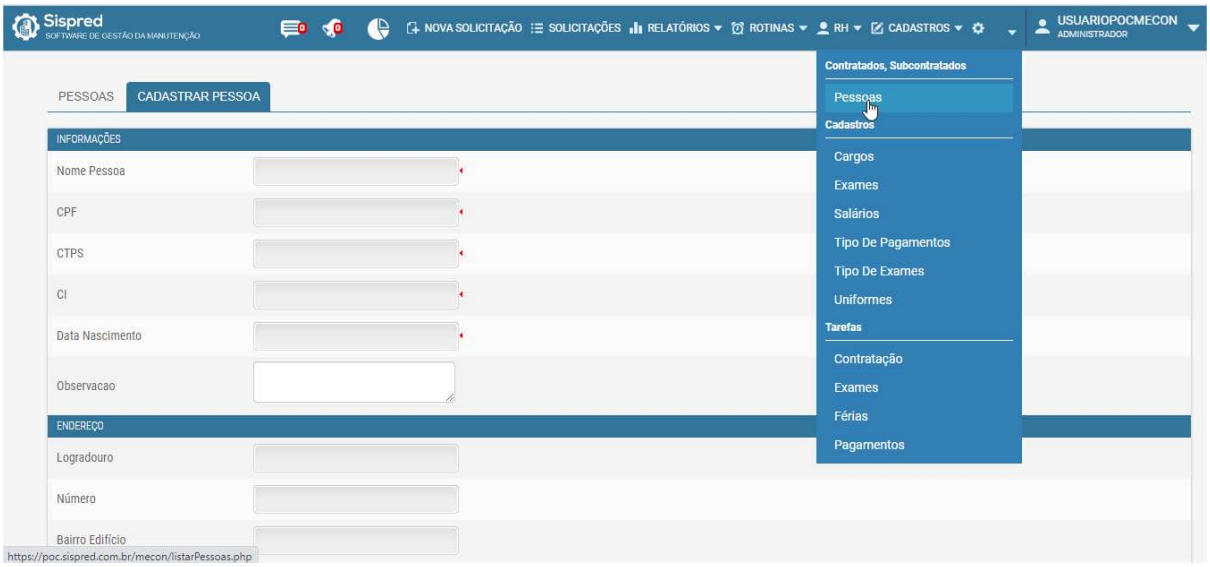


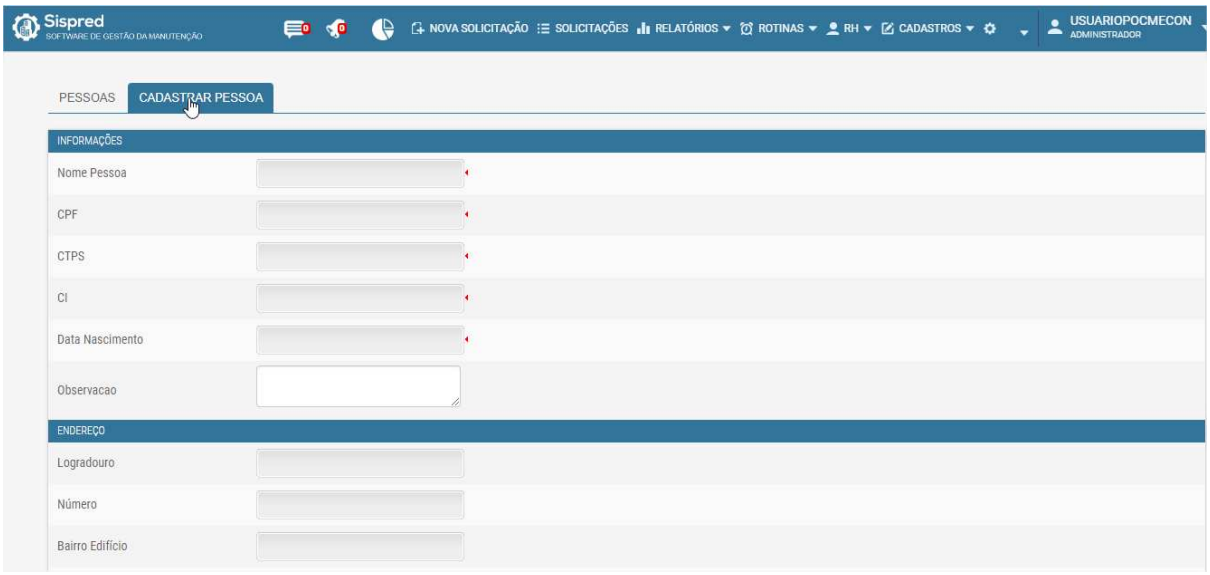


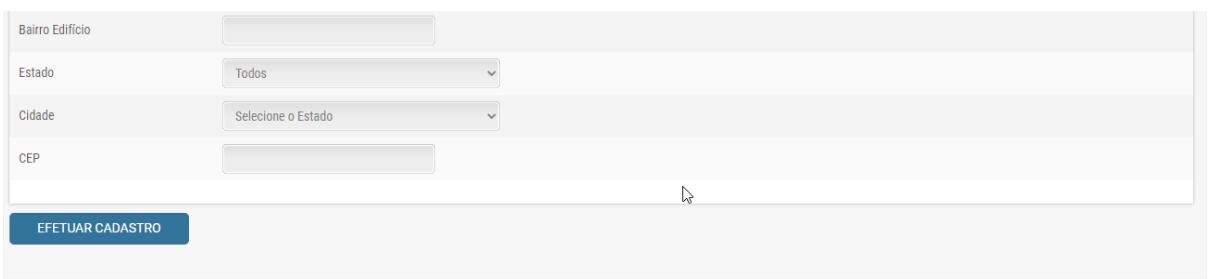
Status: **Aderente**

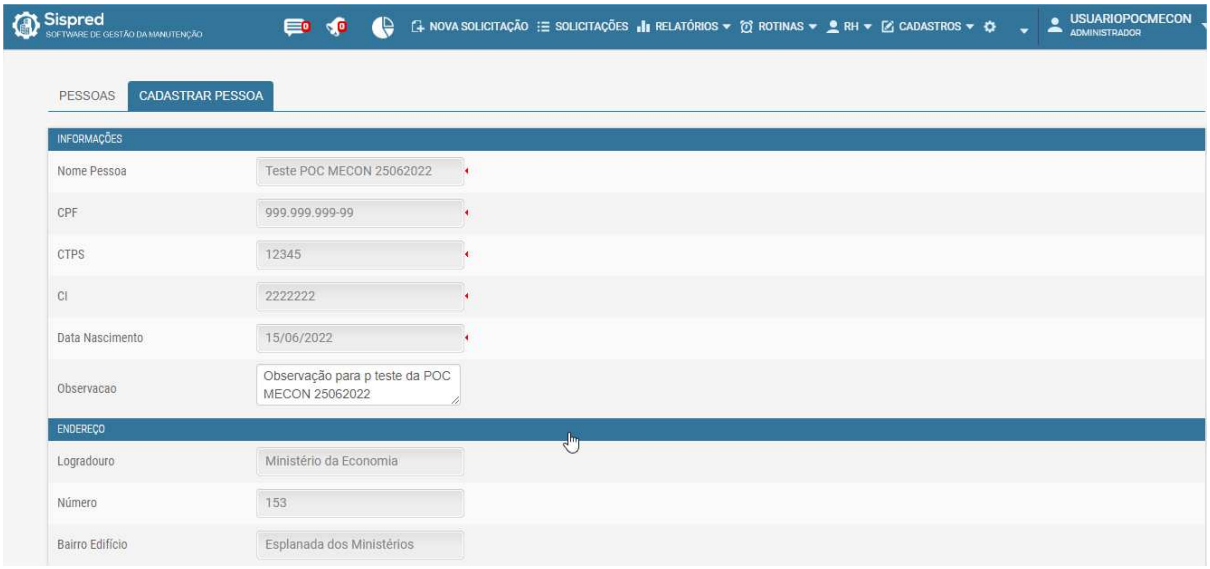
22 - Cadastramento dos empregados e subcontratados

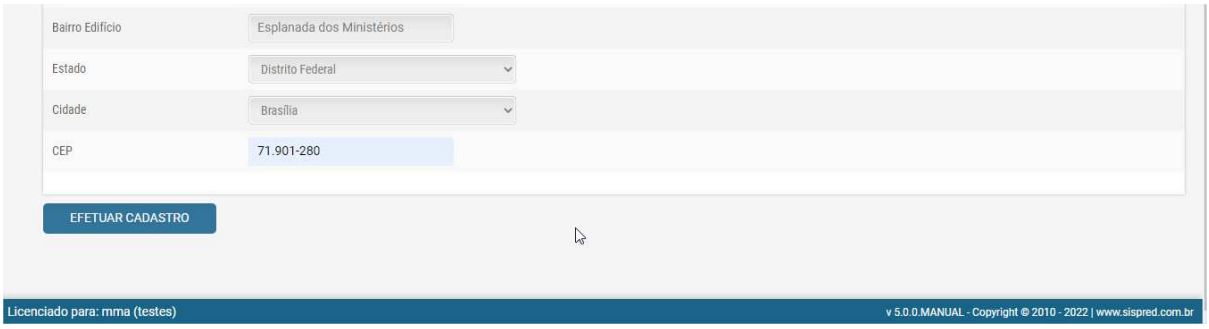
Trilha de Navegação: Menu Principal -> RH -> Contratados, Subcontratados -> Pessoas -> Cadastrar Pessoas

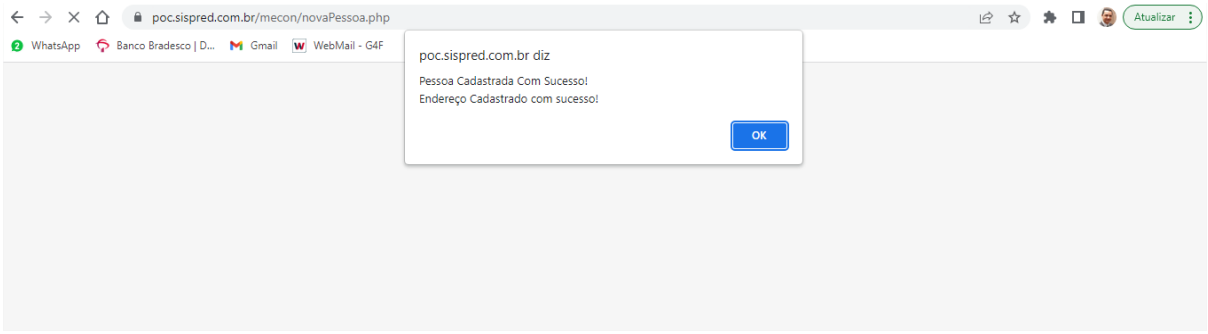


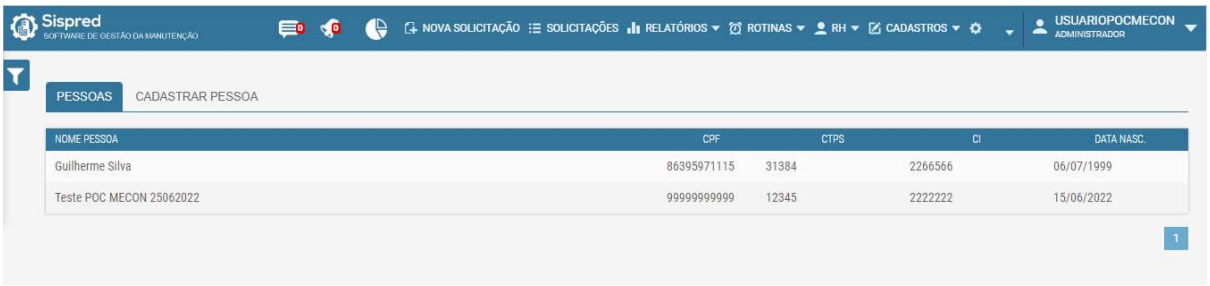





Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
PESSOAS
CADASTRAR PESSOA
INFORMAÇÕES
Nome Pessoa
Teste POC MECON 25062022
CPF
999.999.999-99
CTPS
12345
CI
2222222
Data Nascimento
15/06/2022
Observacao
Observação para p teste da POC MECON 25062022
ENDEREÇO
Logradouro
Ministério da Economia
Número
153
Bairro Edifício
Esplanada dos Ministérios


Bairro Edifício
Esplanada dos Ministérios
Estado
Distrito Federal
Cidade
Brasília
CEP
71.901-280
EFETUAR CADASTRO
Licenciado para: mma (testes)
v 5.0.0.MANUAL - Copyright © 2010 - 2022 | www.sispred.com.br

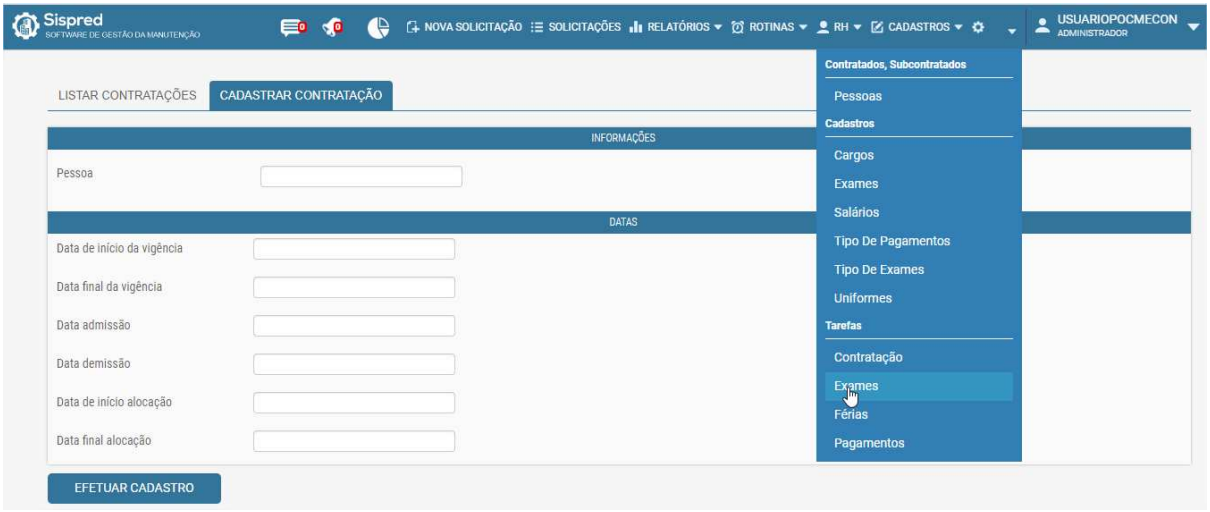

poc.sispred.com.br/mecon/novaPessoa.php
Atualizar
WhatsApp
Banco Bradesco | D...
Gmail
WebMail - G4F
poc.sispred.com.br diz
Pessoa Cadastrada Com Sucesso!
Endereço Cadastrado com sucesso!
OK

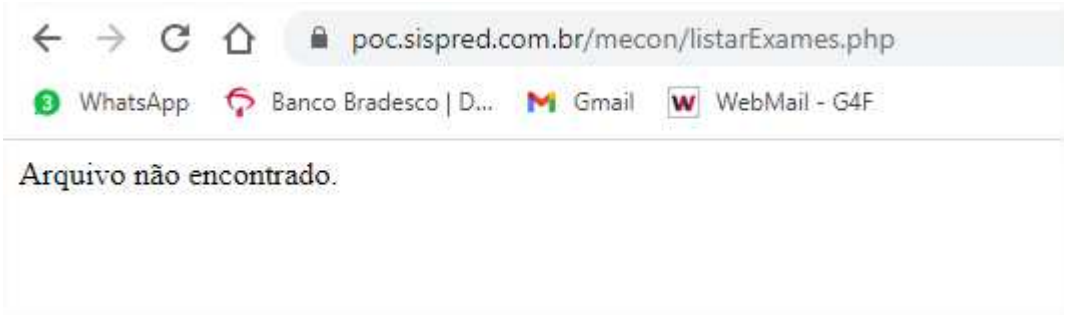

Sispred
SOFTWARE DE GESTÃO DA MANUTENÇÃO
NOVA SOLICITAÇÃO
SOLICITAÇÕES
RELATÓRIOS
ROTINAS
RH
CADASTROS
USUARIOPOCMECON
ADMINISTRADOR
PESSOAS
CADASTRAR PESSOA
NOME PESSOA
CPF
CTPS
CI
DATA NASC.
Guilherme Silva
86395971115
31384
2266566
06/07/1999
Teste POC MECON 25062022
99999999999
12345
2222222
15/06/2022
1

Status: **Não aderente.** No cadastro de Empregados e Subcontratos, não possui local/campo para o cadastramento dos arquivos/imagens dos documentos de CI e CTPS, indicador pessoa reabilitada ou com deficiência; data de vigência; manutenção das alterações efetuadas; datas de admissão e de demissão do empregado (com possibilidade de registro e manutenção do histórico das ocorrências), datas de início e final da alocação do empregado (com possibilidade de registro e manutenção do histórico das ocorrências), data de vigência, jornada de trabalho mensal, horário de início e de fim do trabalho e horário de início e de fim do intervalo para alimentação (com possibilidade de registro e manutenção do histórico das ocorrências).

23 - Cadastramento de exames médicos dos empregados, observadas as disposições do PCMSO estabelecido pela NR 7

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Exames

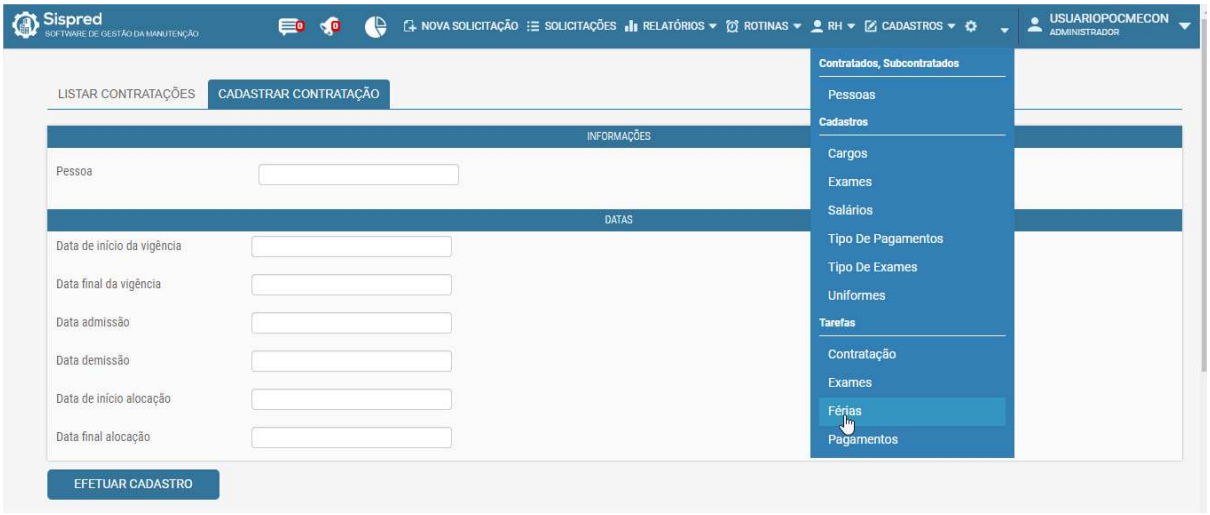


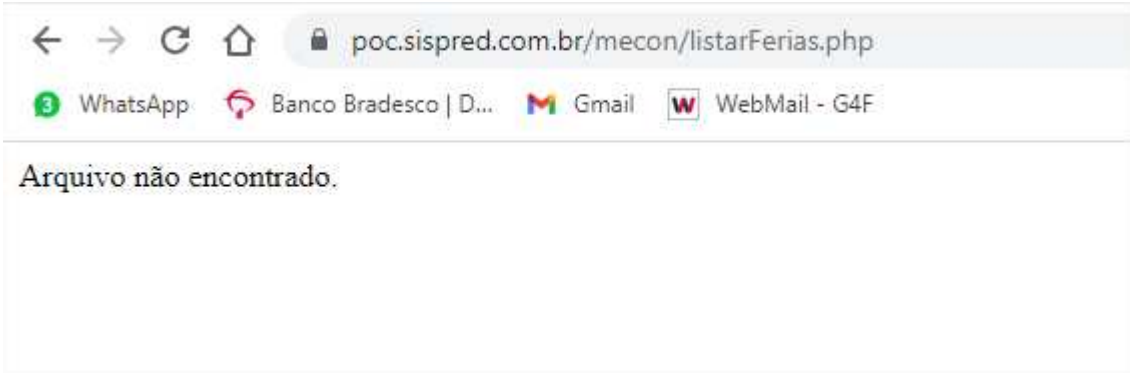


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

24 - Cadastramento das férias dos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Férias

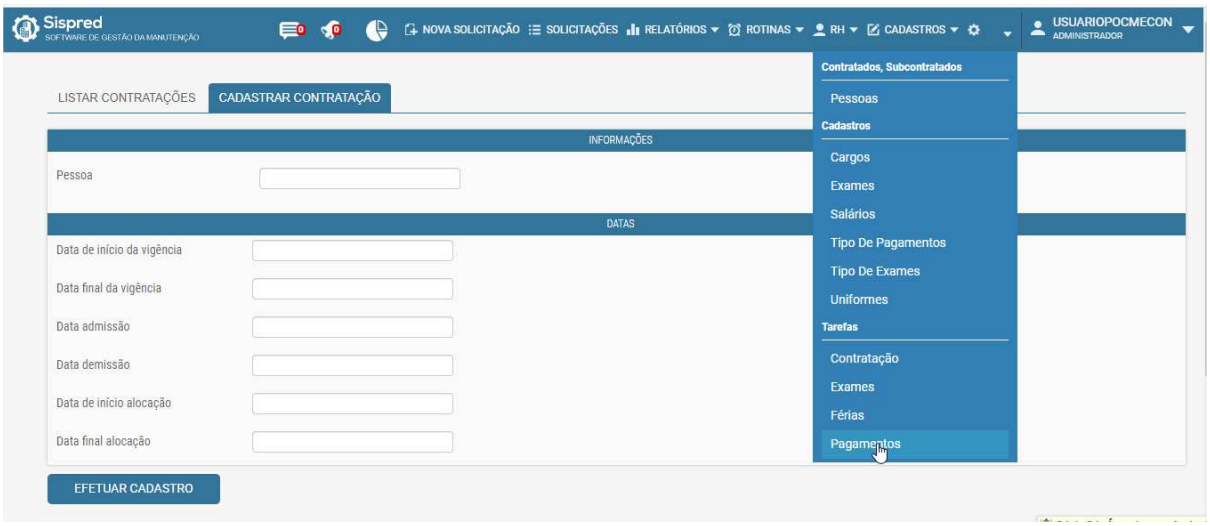


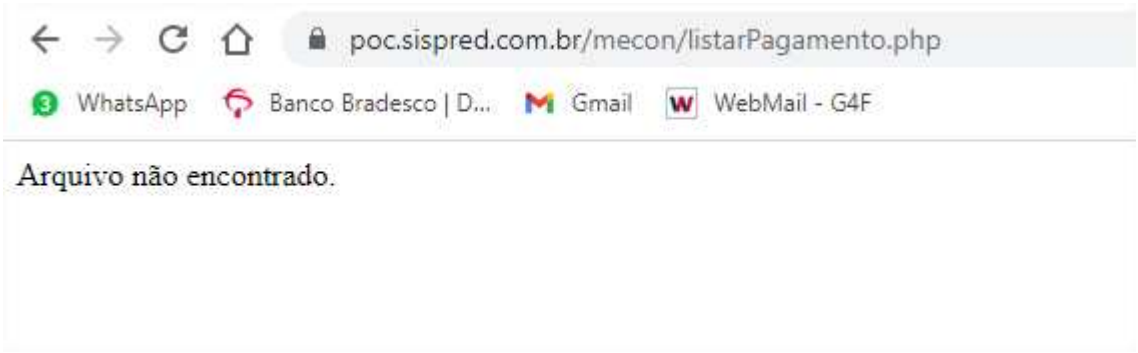


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

25 - Cadastramento de comprovantes de pagamento de salário dos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos

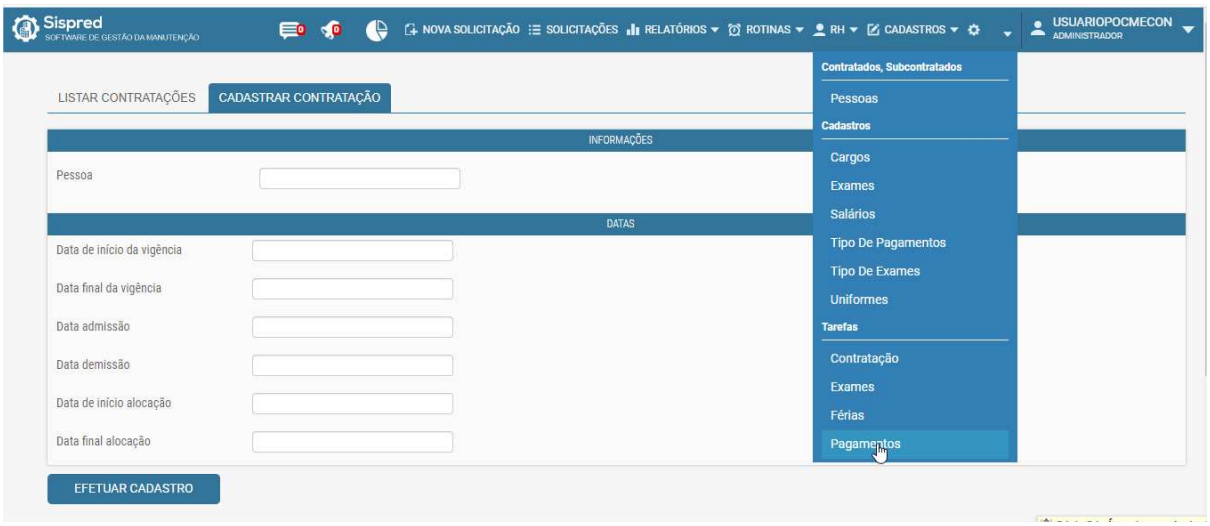


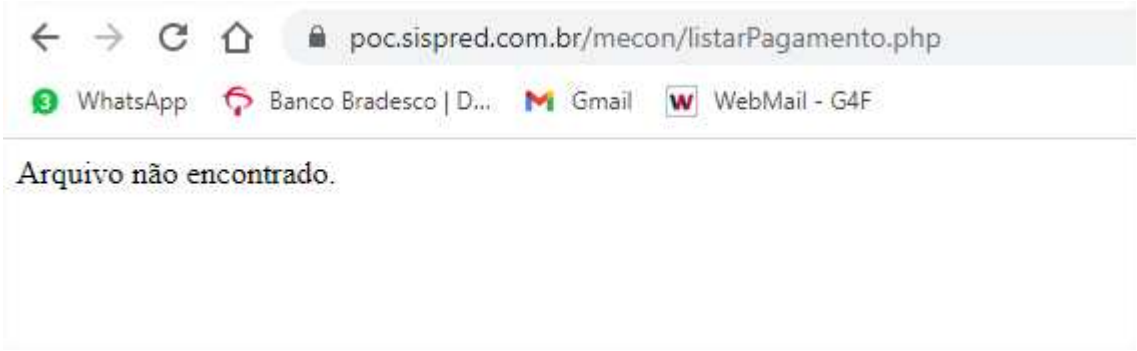


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

26 - Cadastramento de comprovantes de pagamento de vale-transporte dos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos

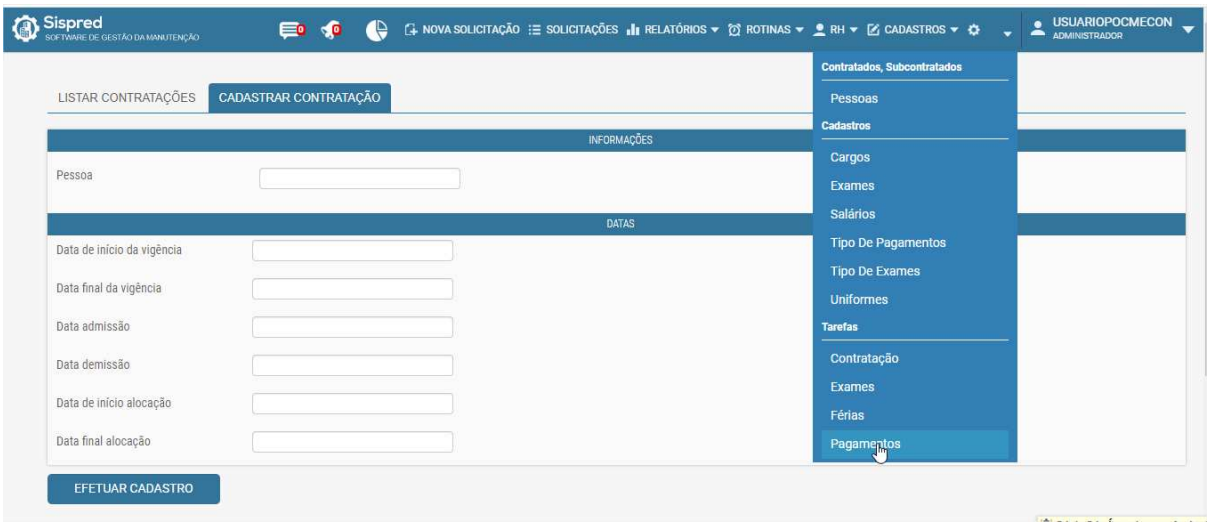


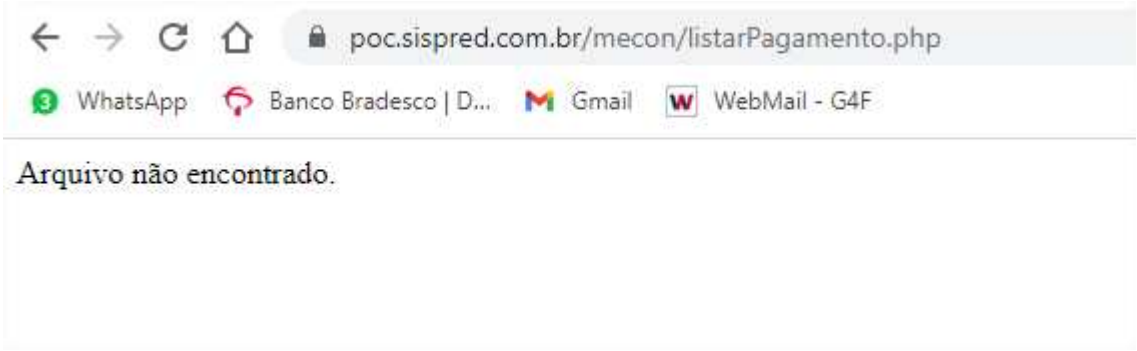


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

27 - Cadastramento de comprovantes de pagamento de auxílio alimentação dos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos

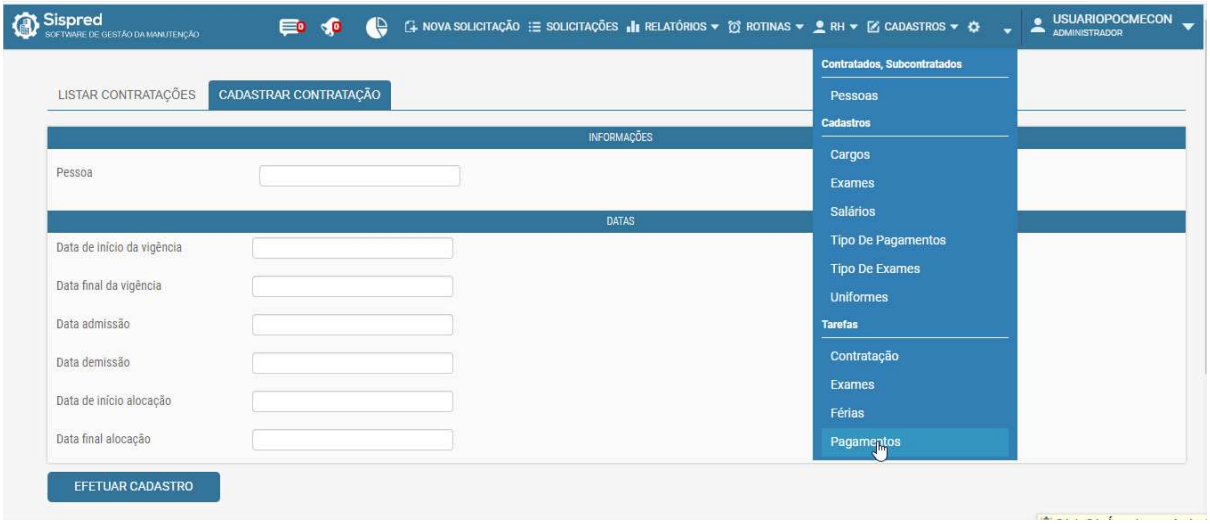


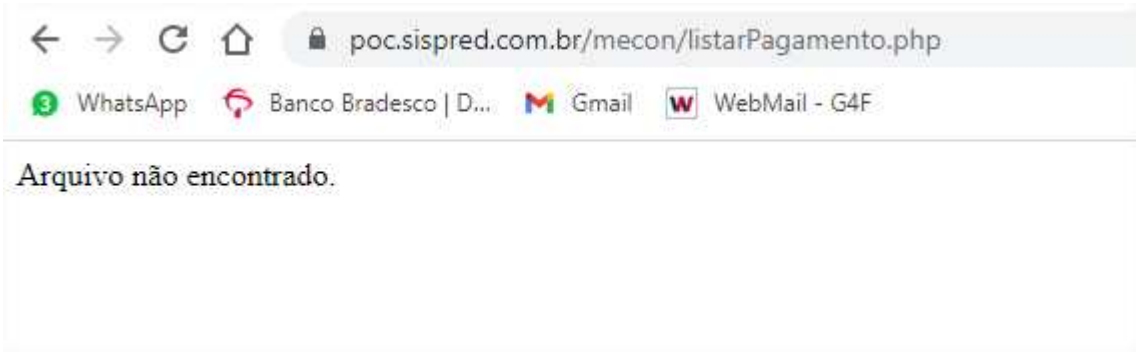


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

28 - Cadastramento de comprovante de pagamento de rescisão de contrato de trabalho dos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos

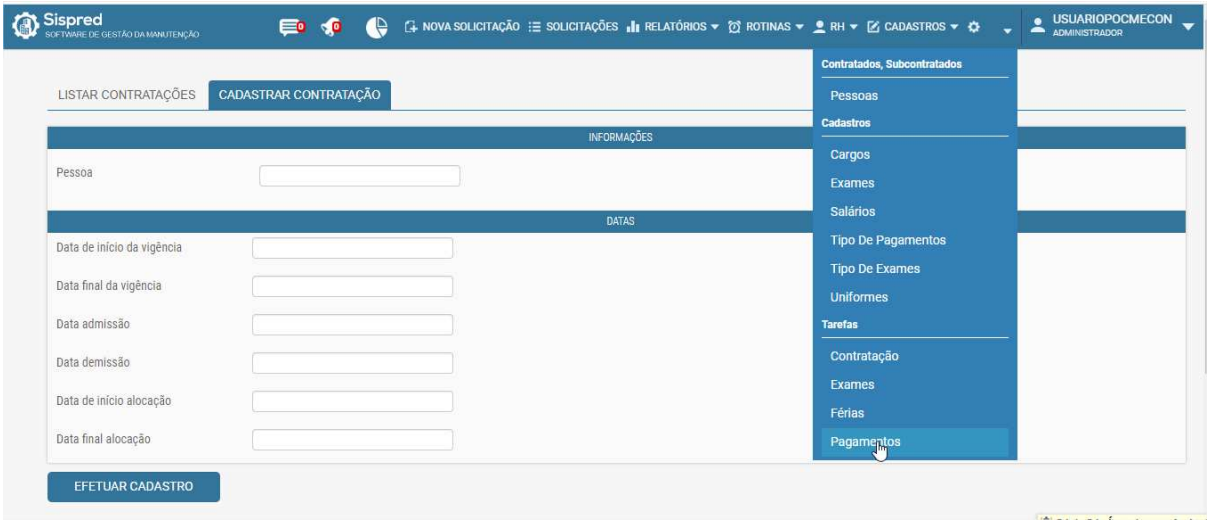


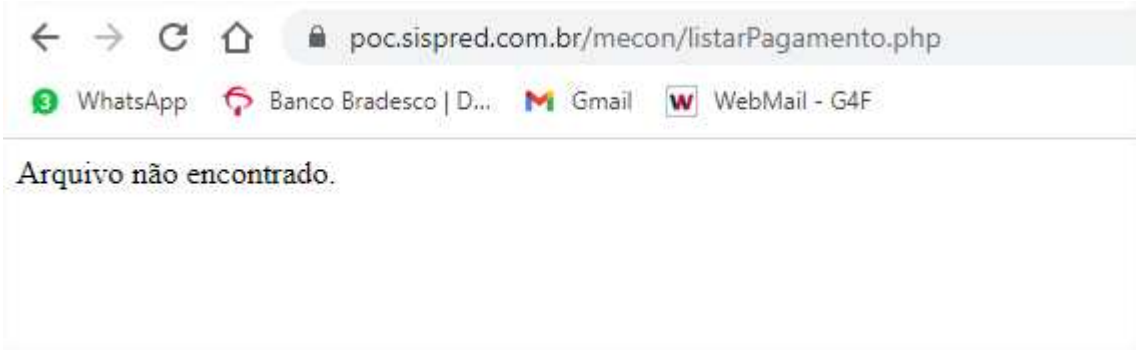


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

29 - Cadastramento de comprovante de recolhimento de contribuições sociais decorrentes dos pagamentos efetuados aos empregados

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos

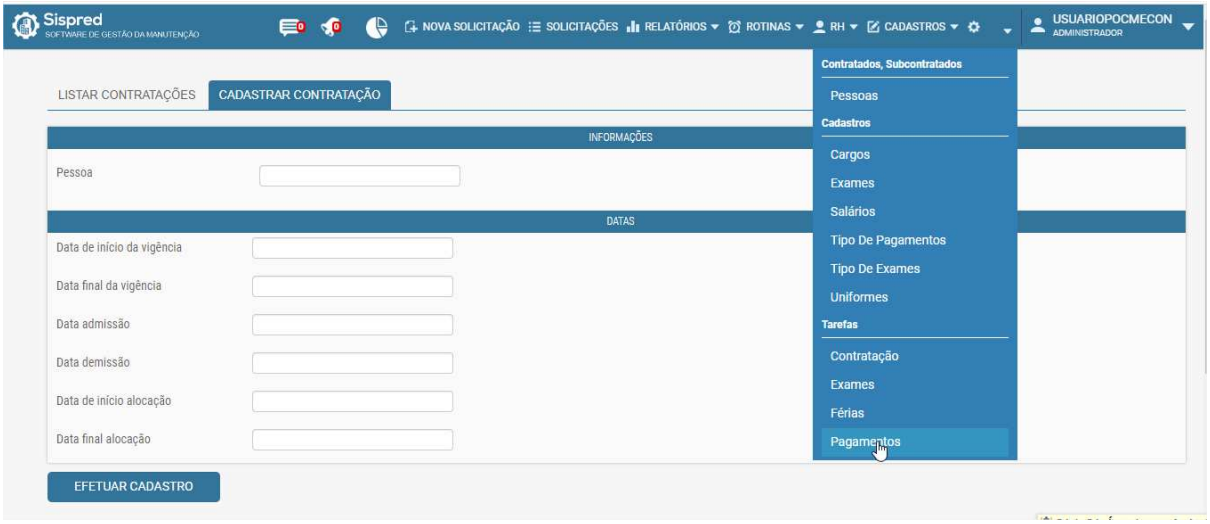


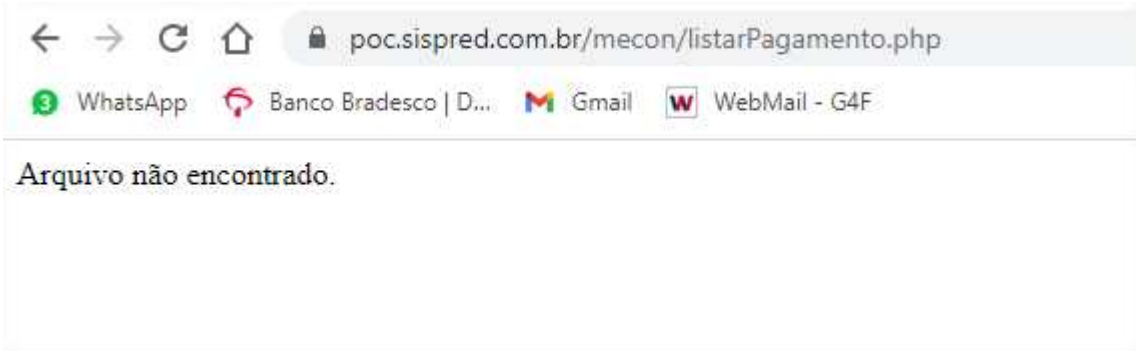


Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

30 - Cadastramento das parcelas dos custos com os empregados da CONTRATADA e da(s) subcontratada(s)

Trilha de Navegação: Menu Principal -> RH -> Tarefas -> Pagamentos





Status: **Não aderente. Observação: Funcionalidade não identificada no sistema.**

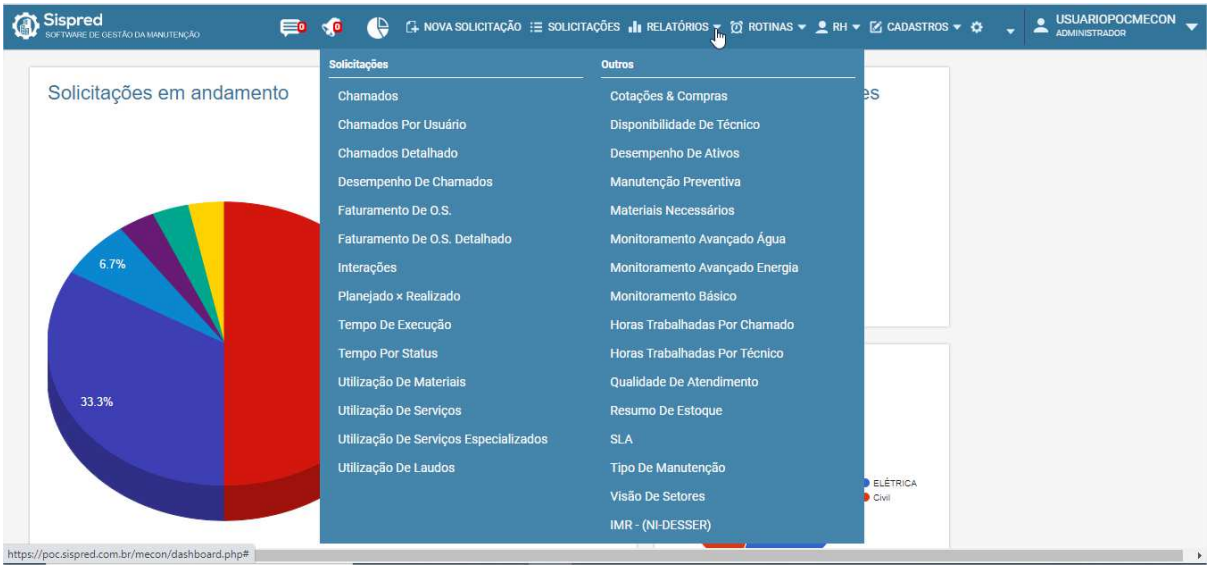
3.2. Funcionalidades gerais da plataforma tecnológica

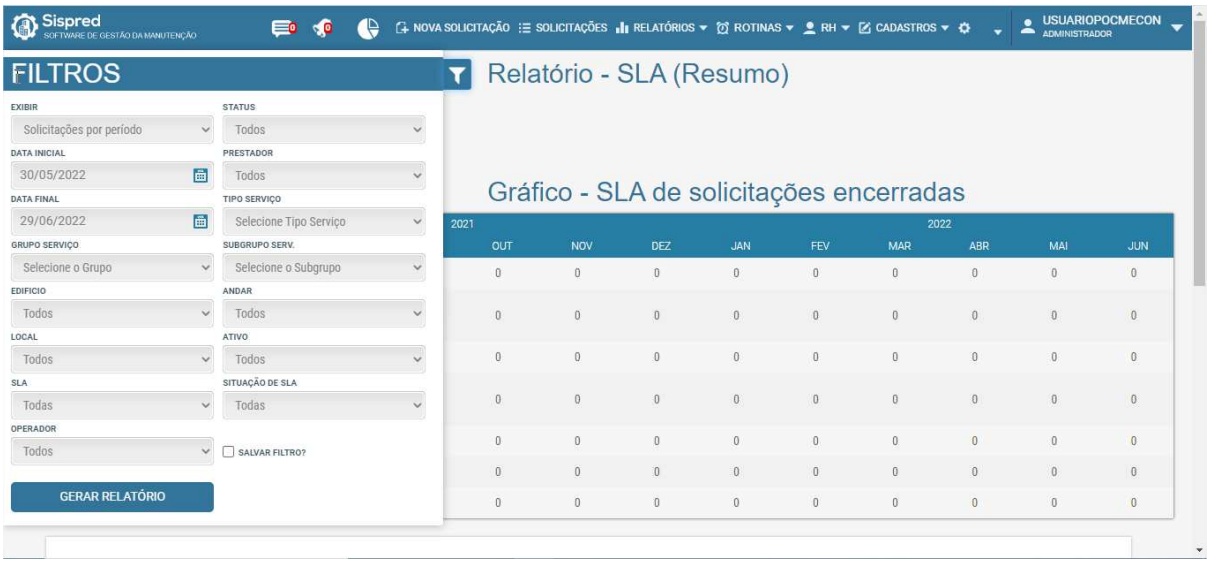
Item 3.2.1 – Consultas

Não foi disponibilizado informações de acesso ao banco de dados, porém entendemos que se trata de uma fase de implantação do sistema onde a Contratada deverá disponibilizar essas informações e acessos à Contratante.

Item 3.2.2 - Relatórios

Trilha de Navegação: Menu Principal -> Relatórios





Status: Aderente com ressalvas.
Sugestão de melhoria/ajuste: Na última versão do sistema apresentada, nem todas as funcionalidades dos relatórios, apresenta a opção de impressão dos relatórios em formato XLS.

Item 3.2.3 – Disponibilidade

Podemos observar que o sistema apresenta disponibilidade de acesso via WEB e Mobile através da URL de acesso e não por aplicativo exclusivo do sistema.

Status: Aderente.

Item 3.2.4 – Manutenção da solução tecnológica

Aspectos de ordem contratual, não sendo tratados em Prova de Conceito.

Item 3.2.5 – Atualização da solução tecnológica

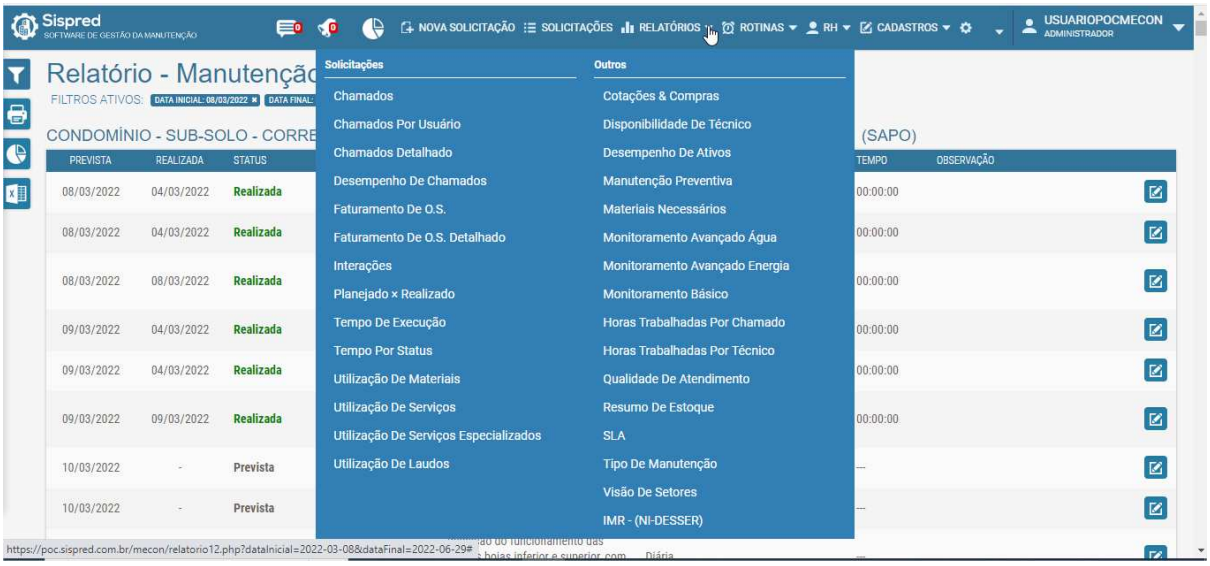
Aspectos de ordem contratual, não sendo tratados em Prova de Conceito.

Item 3.2.6 – Aspectos gerais

Para os itens de Parâmetro de I à XVIII – Com exceção ao item XVII abaixo e aos itens de segurança e rede, os demais são tratados nas validações das Funcionalidades Gerais Mínimas do item 3.1 do Anexo VI do Termo de Referência.

XVII - Cadastramento de relatórios e estudos

Trilha de Navegação: Menu Principal -> Relatórios



Status: **Não aderente. Observação: Não foi identificado na funcionalidade de geração de Relatórios as opções de cadastramentos constantes nesse item.**

6 EXECUÇÃO DOS TESTES E INSPEÇÃO DE SEGURANÇA

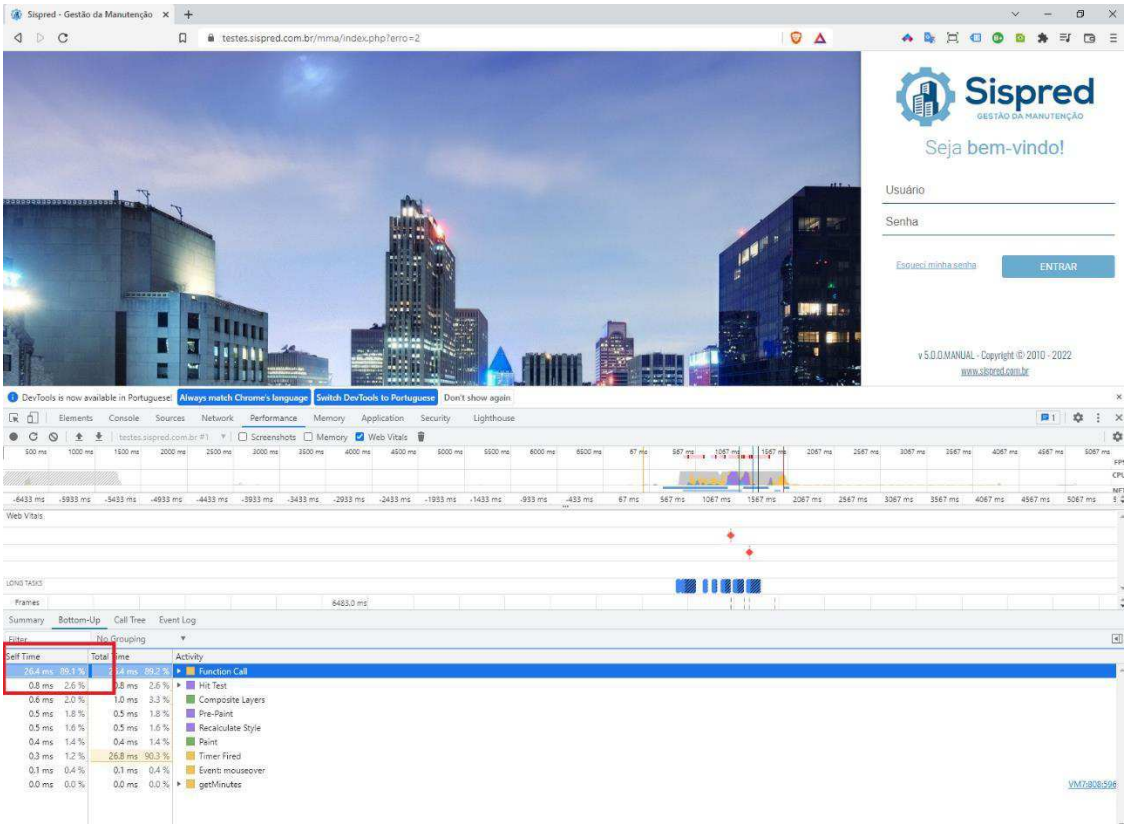
Devido ao baixo nível de aderência no quesito de segurança, a equipe de execução da Prova de Conceito foi orientada a expor no canal oficial de comunicação da POC os pontos não aderentes para a empresa contratada poder efetuar procedimentos corretivos até o término do período da POC.
Com isso relataremos os pontos encontrados no cenárias do sistema até o dia 23/06/2022 e o último no dia 24/06/2022

Os requisitos de segurança que foram verificados até o dia 23/06/2022:

6.1. Tempo de resposta do portal na Web

Observando o item 4.4.2. Desempenho do sistema.

O tempo de teste pode não representar as variações de desempenho ao longo do dia. Evidência 26.4ms tempo de resposta do portal menor que 10s segundos exigidos.



6.2. Soberania dos dados

Identificado que o sistema reside em um site americano na Florida, ou seja, não está alocada preferencialmente em um Data Center no Brasil. Não foi possível comprovar a adequação a INS5 e LGPD conforme informado nos itens 3.2.1 e 3.2.2.

Site na Florida:

ISP	Vultr Holdings LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	207.246.78.135.vultrusercontent.com
Domain Name	vultr.com
Country	United States of America
City	Miami, Florida

a) Seção VI - Do gerenciamento da nuvem - INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021

Lei: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684

Art. 18. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II docaputart. 17, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

b) Identificação das informações pessoais: LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Lei: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Art. 5º Para os fins desta Lei de Proteção de Dados, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

6.3. Usuários:

Itens verificado:

4.1. As funcionalidades da solução tecnológica acima especificadas devem ser associadas a

cada um dos perfis de acesso, observadas as atividades por eles desenvolvidas.

a) Perfil usuário do prédio (servidores) e colaboradores: acesso à abertura de chamados por meio de QR Codes ou na plataforma tecnológica, por todos os usuários do prédio;
b) Perfil contratante (gestor do contrato, fiscal administrativo, fiscal técnico, fiscal setorial e apoio à fiscalização): acesso integral a todos os dados da solução tecnológica e função específica de aprovação de chamados e compra de materiais;
c) Perfil contratada – acesso integral, porém garantindo a inviolabilidade dos históricos, exceto aprovação de chamados e compra de materiais.

Evidenciado:

#	Usuário	Login	Password
01	Admin	adminengemafe	@Adminengemafe123
02	Fiscal	fiscalengemafe	@Fiscalengemafe123
03	Contratada	Contratadaengemafe	@Contratadaengemafe123
04	Solicitante	solicitanteengemafe	@Solicitaengemafe123

6.4. Teste e inspeção do item 4.4.1

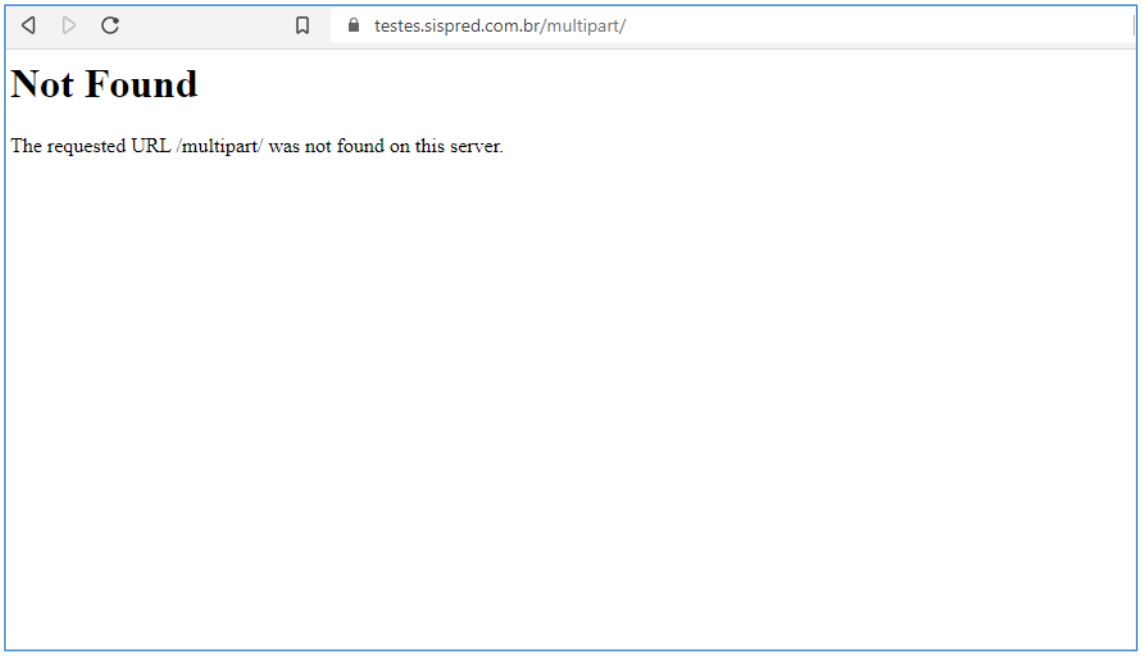
a) Site de hospedagem com certificado SECURE SOCKET LAYER - SSL

SSL Certificate:

```
Certificate:

    Data:

        Version: 3 (0x2)

        Serial Number: 16746 (0x416a)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizatio
nalUnit, CN=sispred/emailAddress=root@sispred

        Validity

            Not Before: Feb  2 17:59:51 2019 GMT

            Not After : Feb  2 17:59:51 2020 GMT
```

b) Resistente a CROSS-SITE REQUEST FORGERY”

Tratamento de erro para páginas não conhecidas, apenas listando a página como não encontrada. Não lista conteúdo.

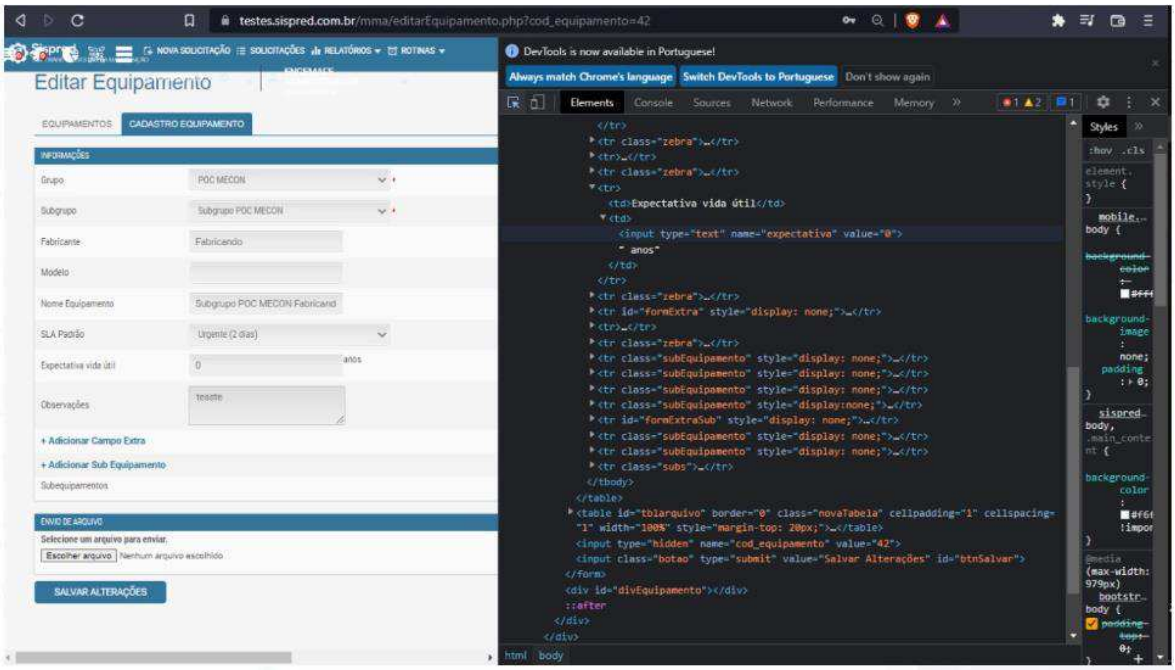


Não identificado o uso de CSRF nos formulários:

Código exemplo:

```
<form action="http://example.com/edit.php" method="POST">
<input type="hidden" name="SESSCSRF" value="1462920523-
5fd057a6ff9dc7a124fa5c814765a498e5aa024a" />
<input type="submit" />
</form>
```

Evidência no Código:



c) Resistente a CROSS-SITE SCRIPTING

Segue evidencia que não possui vulnerabilidades:

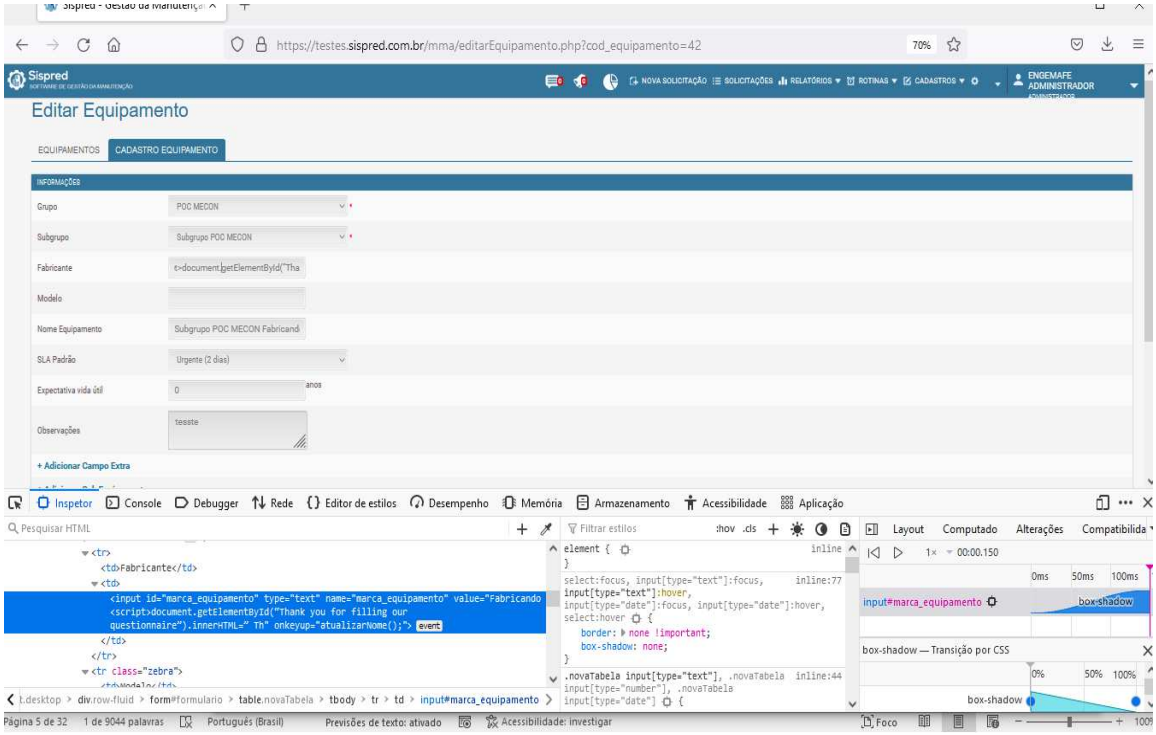
d) Resistente a INJECTION ;”

Objetivo: Teste de CODE INJECTION

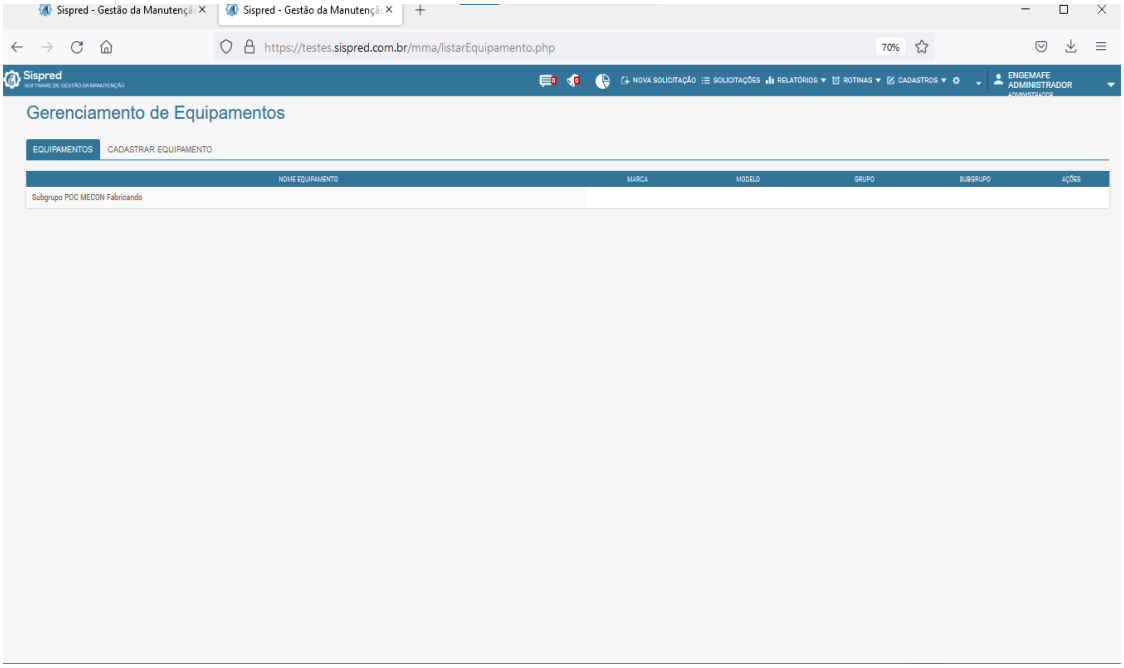
Código Inserido no campo “Fabricante”:

<script>document.getElementById(“Thank you for filling our questionnaire”).innerHTML=”Th”

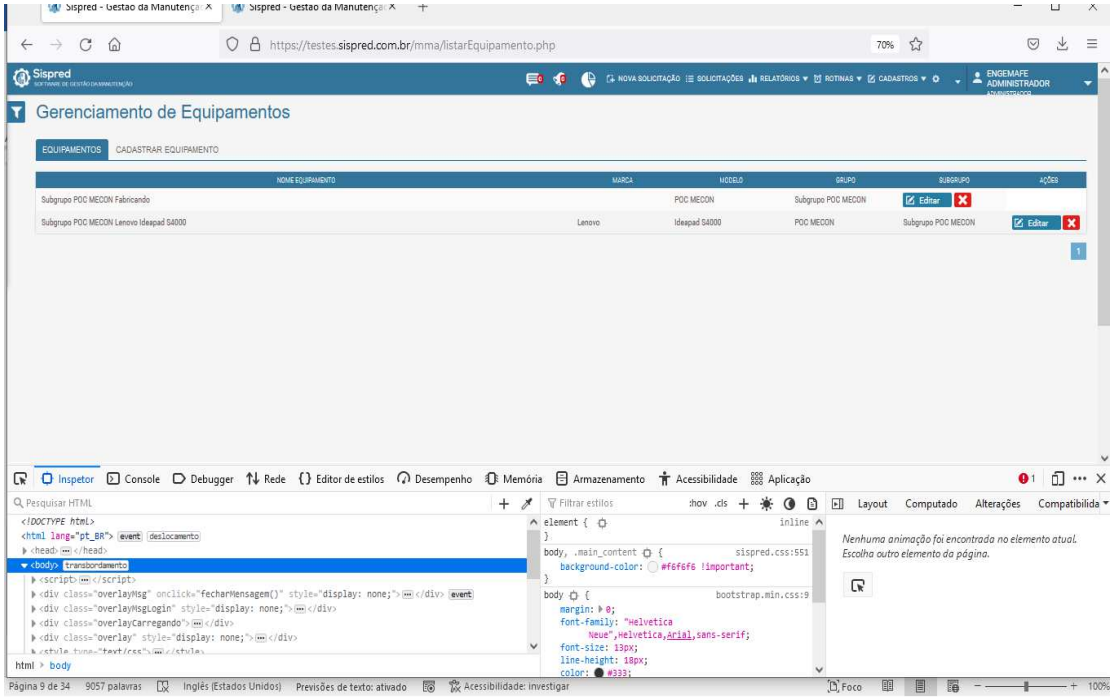
Evidencia do código:



Tela do Sistema com Script inserido:



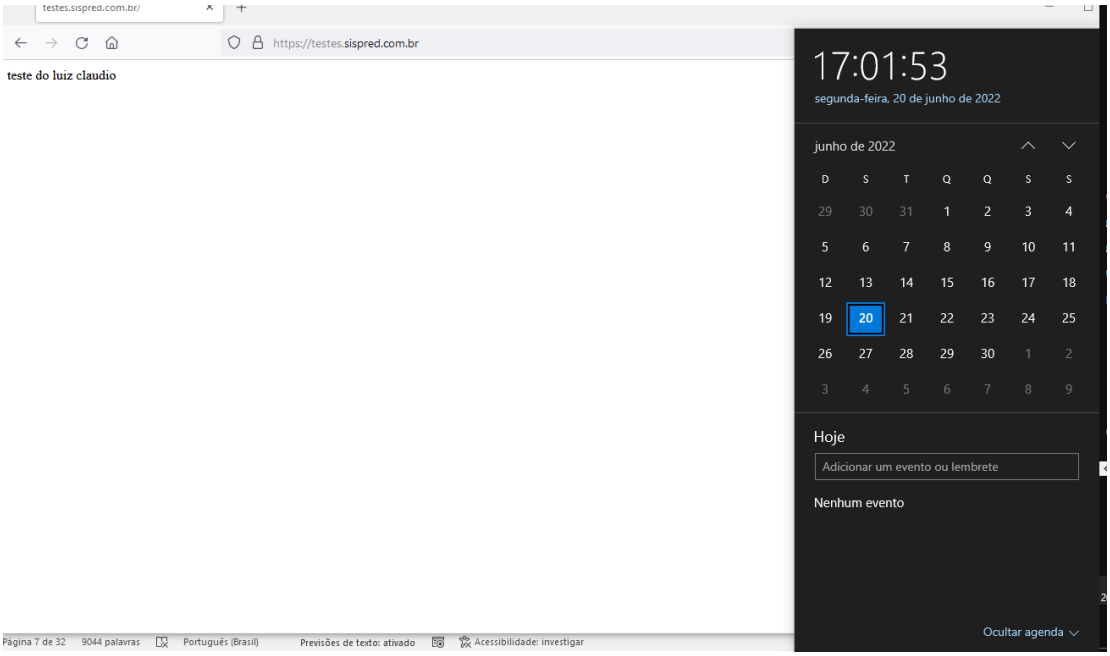
Tela 01 - Executando



Tela 02 – Conteúdo HTML

6.5. Falha na Tela inicial

Foi identificado uma falha na abertura da Tela Inicial.

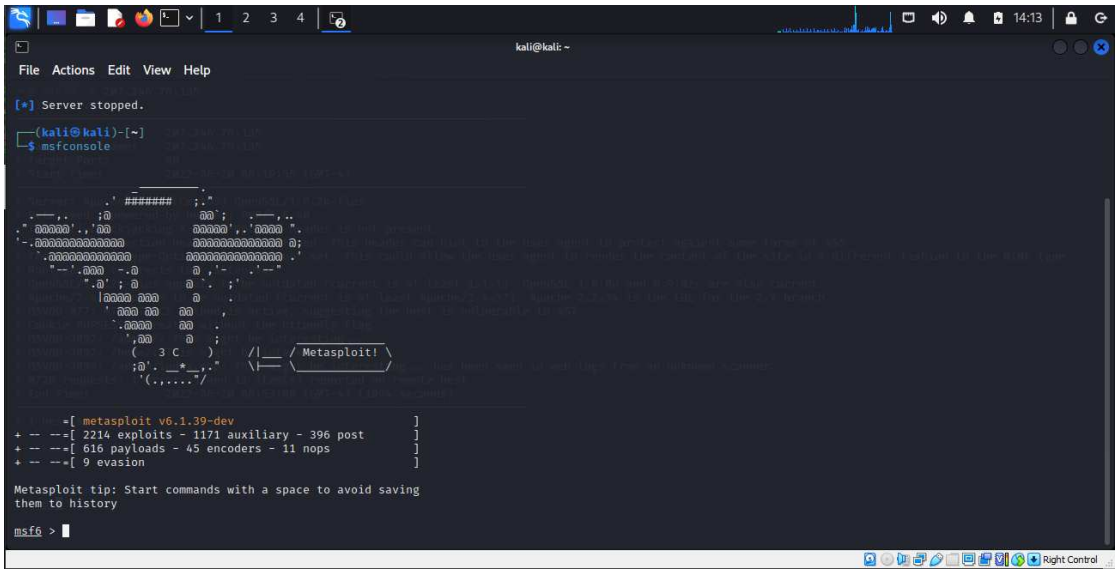


6.6. Análise executadas para análise de exploit de código:

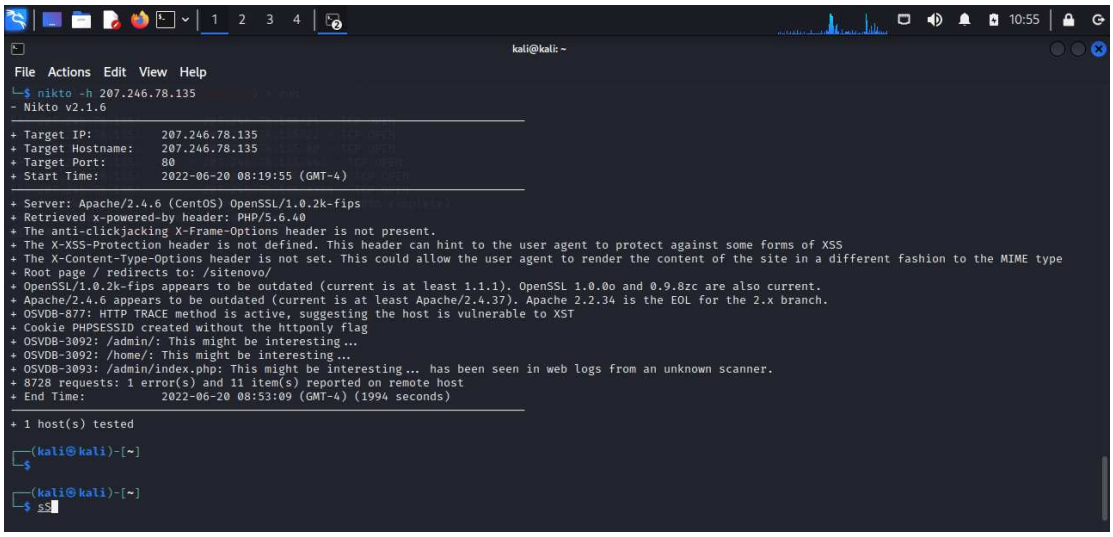
- Versão da Kali Linux utilizado: **kali-linux-2022.2-virtualbox-amd64.ova** no **VirutalBox**
- Sugestão seria o uso de API de comunicação de dados e bloqueio de todas as portas que não sejam apenas as portas HTTPS 443 e HTTP 80.
- Seria importante que as informações estejam em um Data Center no Brasil.

6.7. Utilizando o Nikto para evidenciar softwares desatualizados

Utilizando o Metasploit

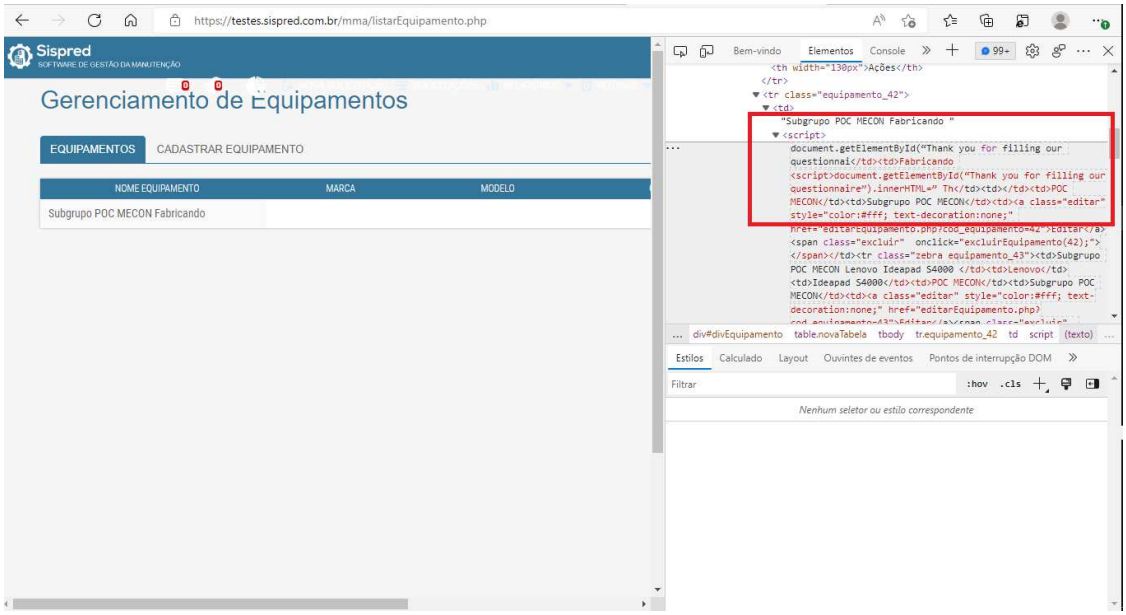


Execução:



Utilizando o Kali Linux e msfconsole descobrindo as portas

Evidências do Code Injection no Código:



6.8. Informações do Shodan o link: https://www.shodan.io/host/207.246.78.135

OpenPorts – Portas Abertas: **21 / 22 / 80 / 4433 / 3063 / 389**

- **21 / TCP**

  220 Bem-vindo ao servico FTP da Diatech.
  530 Login incorrect.
  530 Please login with USER and PASS.
  211-Features:
  EPRT

EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
UTF8
211 End

- **22 / TCP**

```
OpenSSH7.4
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDCWbFQs1QOjVj227hMZeXCVyg3JsRi039r9hXrH/mYUY
kC
qPTU3P8rB2soqTELZmtuHmlHAuwQzgVDSEudfNklqy3qyNbDAEd3NFW9zleEgZEZ+eiaBbu8vz9j
/lCM23Xbjo//AH7wD3eFXLiL+47GPfmplyZOEM+tZzLk0Md12f9BVF4ivLS0QV1oYOa0jr5jjA1s
AAsPBCRxgfOd4eFStwFvNtIJuEVQl4zEPuCAuIF72YuWOHQo1jyrB5uVcK7cL+FaQ5ri4JJWREKk
eoz11nX67sw8D0h+FZpNEo66Tp1R85s1usFZSw9hasROvW4WsqSFaBGIKxAhpOsgZZ9H
Fingerprint: d4:13:ce:90:42:a9:7d:ff:42:25:2b:5e:74:5c:3e:e0

Kex Algorithms:
    curve25519-sha256
    curve25519-sha256@libssh.org
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    diffie-hellman-group-exchange-sha1
    diffie-hellman-group14-sha256
    diffie-hellman-group14-sha1
    diffie-hellman-group1-sha1

Server Host Key Algorithms:
    ssh-rsa
    rsa-sha2-512
    rsa-sha2-256
    ecdsa-sha2-nistp256
    ssh-ed25519

Encryption Algorithms:
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-gcm@openssh.com
    aes256-gcm@openssh.com
    aes128-cbc
    aes192-cbc
    aes256-cbc
    blowfish-cbc
    cast128-cbc
    3des-cbc

MAC Algorithms:
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
```

```
            hmac-sha2-512
            hmac-sha1

        Compression Algorithms:
            none
            zlib@openssh.com
```

- **80 / TCP**

```
Apache httpd2.4.6
HTTP/1.1 301 Moved Permanently
Date: Sun, 19 Jun 2022 02:05:53 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/7.4.19
X-Redirect-By: WordPress
Location: https://www.sispred.com.br/sitenovo/
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

443 / TCP

Apache httpd2.4.6

```
HTTP/1.1 403 Forbidden
Date: Sun, 19 Jun 2022 02:09:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
ETag: "1321-5058a1e728280"
Accept-Ranges: bytes
Content-Length: 4897
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16746 (0x416a)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizat
ionalUnit, CN=sispred/emailAddress=root@sispred
        Validity
            Not Before: Feb  2 17:59:51 2019 GMT
            Not After : Feb  2 17:59:51 2020 GMT
        Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganiza
tionalUnit, CN=sispred/emailAddress=root@sispred
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a4:b1:32:d0:be:e3:7a:a5:f9:90:19:b1:fe:99:
                    1a:78:55:8e:e9:07:45:ed:49:6c:37:25:94:3c:16:
                    e1:17:ad:34:df:dc:42:9f:c7:0e:2f:53:5d:1d:ce:
                    4d:da:fe:e0:e6:b5:83:f9:5e:68:d2:03:43:32:5e:
                    d7:e1:a8:4e:ff:b7:c9:ea:6b:b2:10:9f:e1:26:c6:
                    66:43:5f:91:53:76:21:6b:d0:f7:62:d0:c8:cc:2e:
                    d4:75:54:68:c9:4b:95:5a:35:f2:d2:c4:3f:70:bd:
                    26:87:9b:ab:b0:c0:a3:6d:f0:58:d3:a2:a2:8b:42:
                    20:6f:d5:8c:eb:d2:e3:12:bc:95:9d:3d:7c:41:8e:
                    7f:72:30:2f:f8:83:1d:ae:38:f1:64:49:0d:6f:54:
                    20:31:57:fd:ca:59:6d:c9:1a:99:0e:fc:7d:7d:fb:
                    80:5d:5f:ee:ce:dc:dc:b9:53:1d:7b:3f:ec:e3:73:
                    32:00:b8:af:7b:4e:f7:81:52:41:e6:81:c6:c9:28:
                    96:80:04:59:25:ab:c7:01:f6:68:e8:71:43:cb:23:
                    dc:f6:c9:4d:7b:9b:2b:04:da:d8:59:13:33:99:90:
                    af:ec:4b:d2:45:00:56:ae:f2:e5:74:ad:01:f4:ae:
                    01:21:b9:89:c3:f8:cf:34:fe:17:2f:d2:8a:ab:e2:
                    24:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
```

```
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            23:3c:28:b8:5e:f4:84:42:e8:f3:27:e3:a6:db:07:e0:7d:7e:
            a1:5e:1e:08:3f:35:20:03:b6:2e:fd:67:d3:7d:8a:5b:98:a0:
            16:66:f6:ab:f1:2c:28:8b:6f:dc:f5:57:98:43:ad:67:1c:9b:
            80:1f:2a:0c:77:48:84:4d:81:f5:6f:6b:db:91:60:7e:d6:91:
            a2:1d:f0:7d:34:f8:35:a3:8d:38:91:a1:a5:6b:4b:98:2e:bd:
            6f:de:5d:41:b4:ef:d8:7c:c8:c5:52:48:96:66:0c:48:87:5c:
            87:8e:56:23:7b:d9:ed:3f:86:b2:8e:b9:bd:55:88:6b:55:66:
            40:71:c0:22:00:a8:9f:63:1d:d6:04:6a:5a:52:99:e8:2c:3f:
            48:14:0f:54:fa:5e:8b:f1:bb:cf:fc:67:63:41:41:58:22:72:
            83:12:e1:41:01:cb:63:19:4b:ef:4e:c8:ac:4c:34:40:ce:1b:
            b7:06:12:00:be:82:c6:ac:ef:03:90:49:16:d5:c2:03:e9:e7:
            94:0e:04:28:85:cf:7f:96:6e:ff:eb:be:56:cd:fb:ba:7a:6c:
            1e:86:f0:41:cb:1d:dd:9d:31:59:94:b6:47:7c:5c:60:d0:ba:
            16:76:2b:1c:fd:50:31:60:64:6b:35:3d:cb:32:00:b9:ca:c2:
            bf:8b:bc:b4
```

- **3306 / TCP**

  MySQL5.7.34 - 5.7.34

- **3389 / TCP**

```
OpenSSH7.4
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDCWbFQs1QOjVj227hMZeXCVyg3JsRi039r9hXrH/mYUYkC
qPTU3P8rB2soqTELZmtuHmlHAuwQzgVDSEudfNklqy3qyNbDAEd3NFW9zleEgZEZ+eiaBbu8vz9j
/lCM23Xbjo//AH7wD3eFXLiL+47GPfmplyZOEM+tZzLk0Md12f9BVF4ivLS0QVloYOa0jr5jjA1s
AAsPBCRxgfOd4eFStwFvNtIJuEVQl4zEPuCAuIF72YuWOHQo1jyrB5uVcK7cL+FaQ5ri4JJWREKk
eoz11nX67sw8D0h+FZpNEo66Tp1R85s1usFZSw9hasROvW4WsqSFaBGIKxAhpOsgZZ9H
Fingerprint: d4:13:ce:90:42:a9:7d:ff:42:25:2b:5e:74:5c:3e:e0

Kex Algorithms:
  curve25519-sha256
  curve25519-sha256@libssh.org
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group1-sha1

Server Host Key Algorithms:
  ssh-rsa
  rsa-sha2-512
  rsa-sha2-256
  ecdsa-sha2-nistp256
  ssh-ed25519

Encryption Algorithms:
  chacha20-poly1305@openssh.com
  aes128-ctr
  aes192-ctr
  aes256-ctr
  aes128-gcm@openssh.com
  aes256-gcm@openssh.com
  aes128-cbc
  aes192-cbc
```

```
    aes256-cbc
    blowfish-cbc
    cast128-cbc
    3des-cbc

  MAC Algorithms:
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
    hmac-sha2-512
    hmac-sha1

  Compression Algorithms:
    none
    zlib@openssh.com
```

6.9. Vulnerabilidades identificadas no shodan

O host informado aparentemente possui as seguintes vulnerabilidades:

Porta abertas e serviços:

CVE	Vulnerabilidades
CVE-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2021-36368	** DISPUTED ** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."
CVE-2018-15473	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2020-14145	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where

	no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
CVE-2020-15778	** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."
CVE-2021-41617	sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
CVE-2018-20685	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2016-20012	** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.
CVE-2019-6110	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
CVE-2019-6111	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
CVE-2019-6109	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2014-0117	The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.
CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3184	mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2015-3183	The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.
CVE-2019-1563	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2021-44790	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
CVE-2016-4975	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
CVE-2020-13938	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2022-22719	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2018-5407	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.
CVE-2014-3523	Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.
CVE-2013-5704	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."
CVE-2019-17567	Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
CVE-2013-6438	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
CVE-2022-30522	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.
CVE-2014-0231	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
CVE-2021-26690	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2021-3712	ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit.

	This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).
CVE-2022-30556	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2021-39275	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2021-21707	In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended.
CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2019-10092	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVE-2021-21706	In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.
CVE-2021-21705	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with FILTER_VALIDATE_URL parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.
CVE-2021-21704	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.
CVE-2021-21703	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2015-0228	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.
CVE-2016-5387	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
CVE-2021-21708	In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits.
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
CVE-2021-23840	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users

	should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).
CVE-2021-23841	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-1301	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
CVE-2018-1302	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
CVE-2020-1968	The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).
CVE-2020-11985	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.
CVE-2021-4160	There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of

	December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).
CVE-2013-4352	The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.
CVE-2022-26377	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2014-0098	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.
CVE-2016-8743	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
CVE-2022-0778	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

CVE-2020-1971	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2017-3736	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.
CVE-2017-3737	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.
CVE-2019-1547	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2017-3735	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

CVE-2022-1292	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).
CVE-2017-3738	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.
CVE-2018-17199	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2018-0737	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-0734	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2014-8109	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

CVE-2016-2161	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.
CVE-2016-8612	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
CVE-2019-1552	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2019-1551	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).
CVE-2019-1559	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2018-1303	A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

Os requisitos de segurança que foram verificados no dia 24/06/2022:

6.10. Tempo de resposta do portal na Web

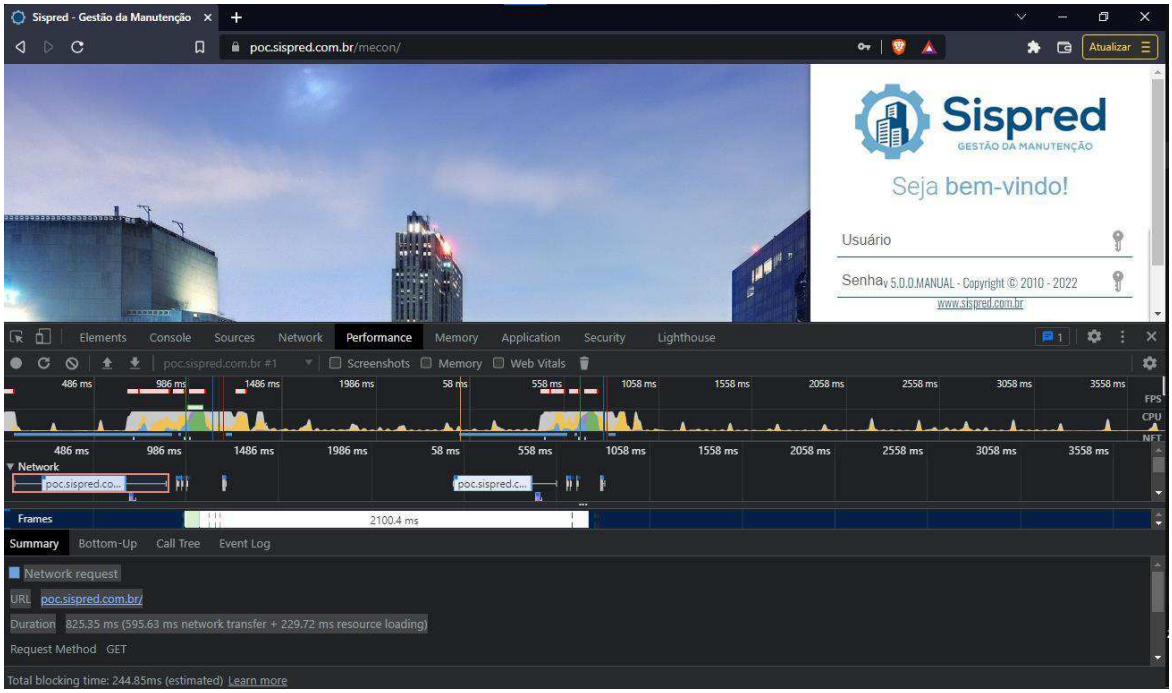
Observando o item 4.4.2. Desempenho do sistema.

O tempo de teste pode não representar as variações de desempenho ao longo do dia.

Evidência:

- Network request URLpoc.sispred.com.br/ Duration825.35 ms (595.63 ms network transfer + 229.72 ms resource loading)

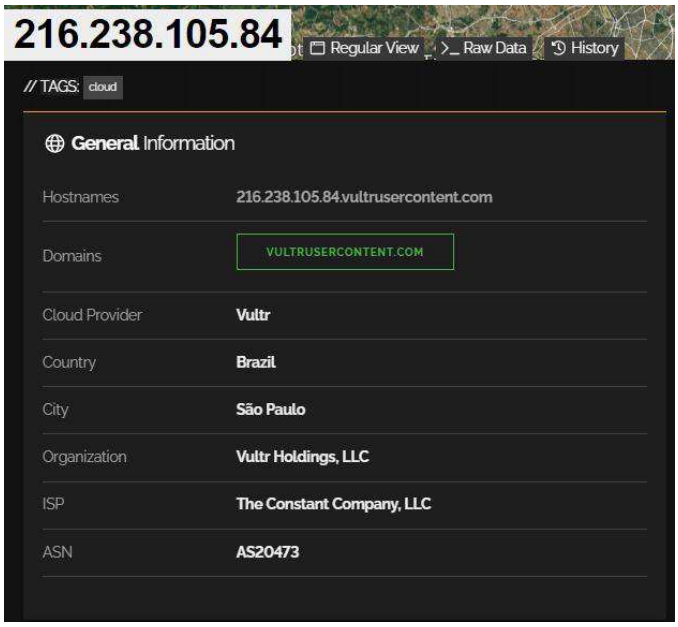
tempo de resposta do portal menor que 10s segundos exigido.



6.11. Soberania dos dados

O portal “poc.sispred.com.br/mecon” foi migrado para um portal com Data Center no Brasil. O software não estava totalmente operacional pois muitos problemas de execução foram identificados no acesso ao portal.

Site no Brasil:



6.12. Usuários:

Itens verificado:

- 4.1. As funcionalidades da solução tecnológica acima especificadas devem ser associadas a cada um dos perfis de acesso, observadas as atividades por eles desenvolvidas.
- Perfil usuário do prédio (servidores) e colaboradores: acesso à abertura de chamados por meio de
- QR Codes ou na plataforma tecnológica, por todos os usuários do prédio;
- Perfil contratante (gestor do contrato, fiscal administrativo, fiscal técnico, fiscal setorial e apoio à fiscalização): acesso integral a todos os dados da solução tecnológica e função específica de aprovação de chamados e compra de materiais;
- Perfil contratada – acesso integral, porém garantindo a inviolabilidade dos históricos, exceto aprovação de chamados e compra de materiais.

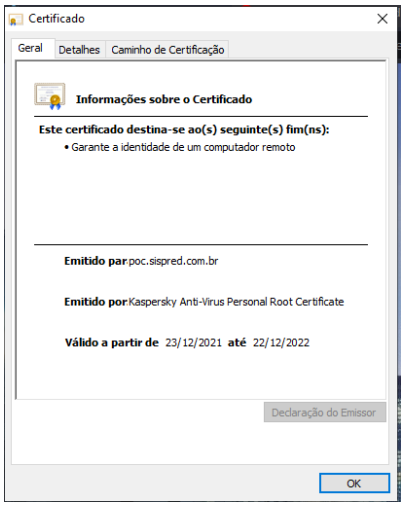
Evidenciado:

#	Usuário	Login	Password
01	Admin	adminengemafe	@Adminengemafe123
02	Fiscal	fiscalengemafe	@Fiscalengemafe123
03	Contratada	Contratadaengemafe	@Contratadaengemafe123
04	Solicitante	solicitanteengemafe	@Solicitaengemafe123

6.13. Teste e inspeção do item 4.4.1

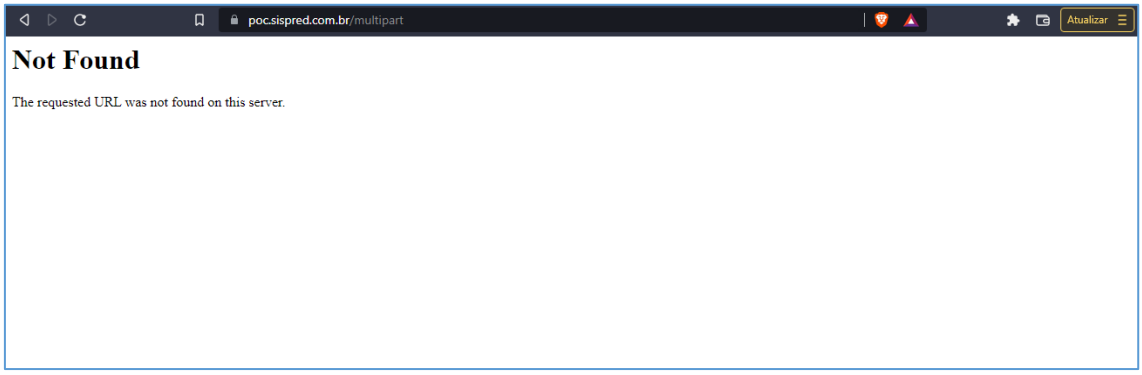
a) "Site de hospedagem com certificado SECURE SOCKET LAYER - SSL"

SSL Certificate:

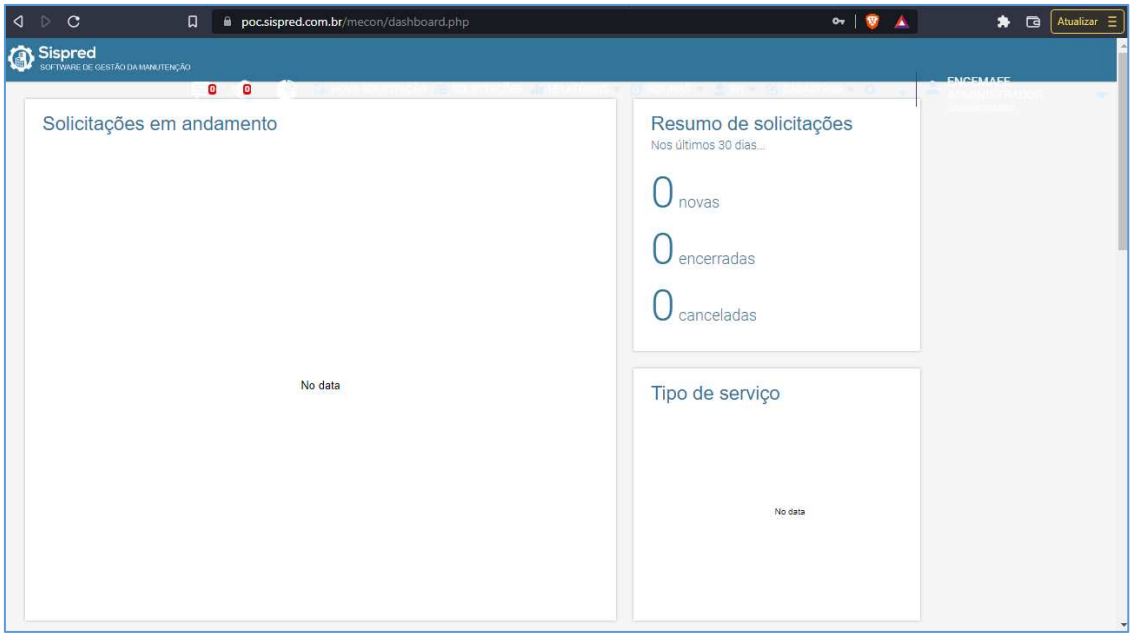


b) Avaliando o item "b) Resistente a CROSS-SITE REQUEST FORGERY"

Tratamento de erro para páginas não conhecidas, apenas listando a página como não encontrada. Não lista conteúdo.



Sem tratamento e falhas nas páginas do sistema:



c) Resistente a CROSS-SITE SCRIPTING;

Segue evidencia que não possui vulnerabilidades CROSS-SITE SCRIPTING

d) Resistente a INJECTION ;”

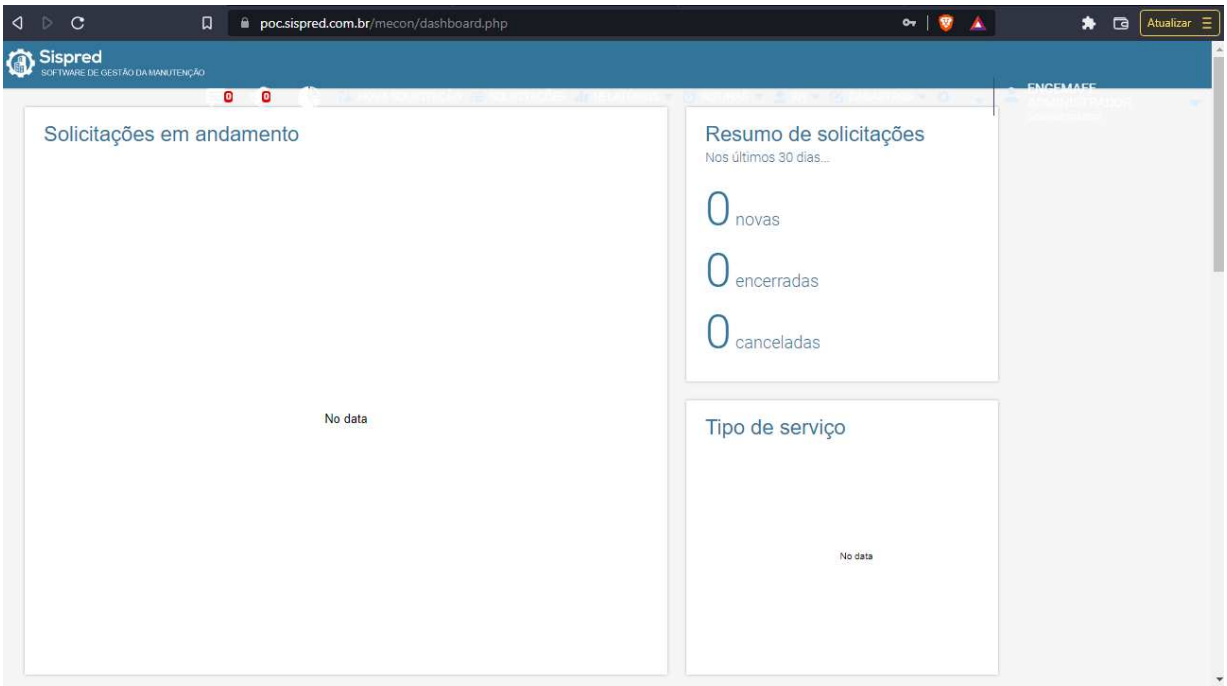
Objetivo: Teste de CODE INJECTION

Código Inserido no campo “Fabricante”:

<script>document.getElementById(“Thank you for filling our questionnaire”).innerHTML=”Th”

Evidência do código:

Página apresentando falhas



6.14. Acesso ao Shoda https://www.shodan.io/host/216.238.105.84

Informações de vulnerabilidades do Shodan

22 / TCP - OpenSSH8.7

```
SSH-2.0-OpenSSH_8.7
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH1WuV
S/FKUKyPDfAHOM3Owg
Bbq70LV2Ko8Pig/b4rU47nzlhhicqXjMArZGIw3+i3Z2//h0cKdKit4mSm8ivw0
=
Fingerprint: 42:61:f8:43:3a:90:74:6a:8b:de:1d:3c:eb:e9:ec:bc

Kex Algorithms:
  curve25519-sha256
  curve25519-sha256@libssh.org
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512

Server Host Key Algorithms:
  rsa-sha2-512
  rsa-sha2-256
  ecdsa-sha2-nistp256
  ssh-ed25519

Encryption Algorithms:
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com
  aes256-ctr
  aes128-gcm@openssh.com
  aes128-ctr

MAC Algorithms:
  hmac-sha2-256-etm@openssh.com
  hmac-sha1-etm@openssh.com
  umac-128-etm@openssh.com
  hmac-sha2-512-etm@openssh.com
  hmac-sha2-256
  hmac-sha1
  umac-128@openssh.com
  hmac-sha2-512

Compression Algorithms:
  none
  zlib@openssh.com
```

```
2117416117 | 2022-06-28 T14:41:57.342652

1.1.1.1.1.1  80 / TCP  Apache httpd 2.4.53
HTTP/1.1 200 OK
Date: Tue, 28 Jun 2022 14:41:56 GMT
Server: Apache/2.4.53 (CentOS Stream) OpenSSL/3.0.1
X-Powered-By: PHP/8.1.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=c3nedjo3sg25bi78vaqugctdmk; path=/
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

a) WebTechnologies

BOOTSTRAP
GOOGLE FONT
API JQUERY
JQUERY UI

b) Vulnerabilidades

Observação: As vulnerabilidades estão implícitas com base no software e na versão

CVE Econtrado	Falha encontrada
CVE-2022-1473	The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process periodically decodes certificates or keys its memory usage will expand without bounds and the process might be terminated by the operating system causing a denial of service. Also traversing the empty hash table entries will take increasingly more time. Typically such long lived processes might be TLS clients or TLS servers configured to accept client certificate authentication. The function was added in the OpenSSL 3.0 version thus older releases are not affected by the issue. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).

CVE-2022-0778	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).
CVE-2022-1292	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).
CVE-2022-1343	The function `OCSP_basic_verify` verifies the signer certificate on an OCSP response. In the case where the (non-default) flag OCSP_NOCHECKS is used then the response will be positive (meaning a successful verification) even in the case where the response signing certificate fails to verify. It is anticipated that most users of `OCSP_basic_verify` will not use the OCSP_NOCHECKS flag. In this case the `OCSP_basic_verify` function will return a negative value (indicating a fatal error) in the case of a certificate verification failure. The normal expected return value in this case would be 0. This issue also impacts the command line OpenSSL "ocsp" application. When verifying an ocsp response with the "-no_cert_checks" option the command line application will report that the verification is successful even though it has in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).

CVE-2022-26377	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2022-30522	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.
CVE-2022-1434	The OpenSSL 3.0 implementation of the RC4-MD5 ciphersuite incorrectly uses the AAD data as the MAC key. This makes the MAC key trivially predictable. An attacker could exploit this issue by performing a man-in-the-middle attack to modify data being sent from one endpoint to an OpenSSL 3.0 recipient such that the modified data would still pass the MAC integrity check. Note that data sent from an OpenSSL 3.0 endpoint to a non-OpenSSL 3.0 endpoint will always be rejected by the recipient and the connection will fail at that point. Many application protocols require data to be sent from the client to the server first. Therefore, in such a case, only an OpenSSL 3.0 server would be impacted when talking to a non-OpenSSL 3.0 client. If both endpoints are OpenSSL 3.0 then the attacker could modify data being sent in both directions. In this case both clients and servers could be affected, regardless of the application protocol. Note that in the absence of an attacker this bug means that an OpenSSL 3.0 endpoint communicating with a non-OpenSSL 3.0 endpoint will fail to complete the handshake when using this ciphersuite. The confidentiality of data is not impacted by this issue, i.e. an attacker cannot decrypt data that has been encrypted using this ciphersuite - they can only modify it. In order for this attack to work both endpoints must legitimately negotiate the RC4-MD5 ciphersuite. This ciphersuite is not compiled by default in OpenSSL 3.0, and is not available within the default provider or the default ciphersuite list. This ciphersuite will never be used if TLSv1.3 has been negotiated. In order for an OpenSSL 3.0 endpoint to use this ciphersuite the following must have occurred: 1) OpenSSL must have been compiled with the (non-default) compile time option enable-weak-ssl-ciphers 2) OpenSSL must have had the legacy provider explicitly loaded (either through application code or via configuration) 3) The ciphersuite must have been explicitly added to the ciphersuite list 4) The libssl security level must have been set to 0 (default is 1) 5) A version of SSL/TLS below TLSv1.3 must have been negotiated 6) Both endpoints must negotiate the RC4-MD5 ciphersuite in preference to any others that both endpoints have in common Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).
CVE-2022-30556	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

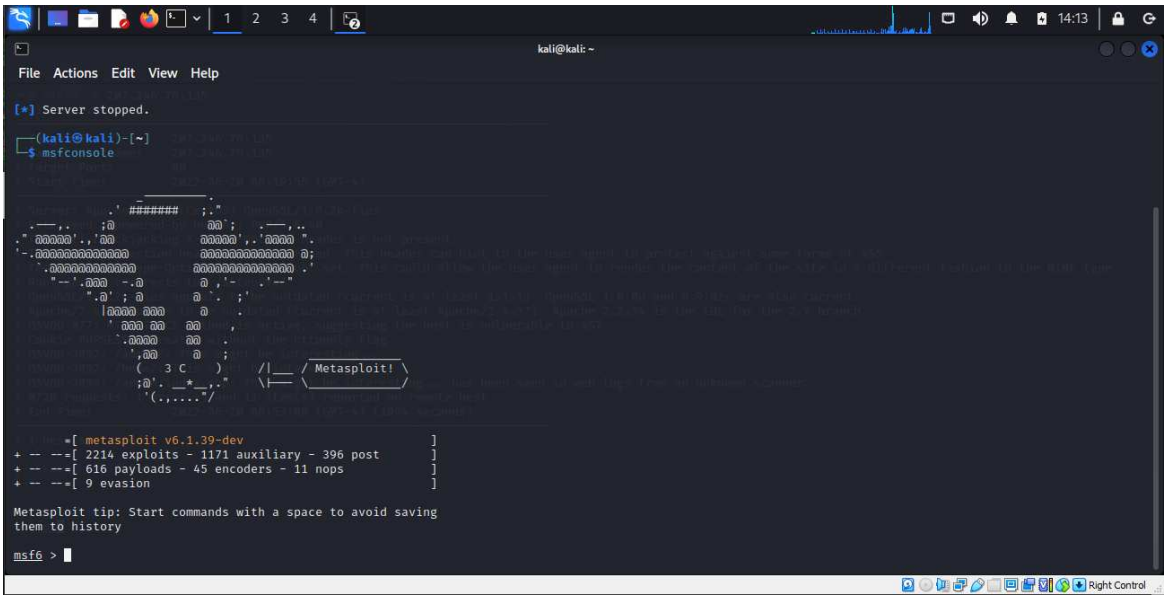
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

6.15. Análise executadas para análise de exploit de código:

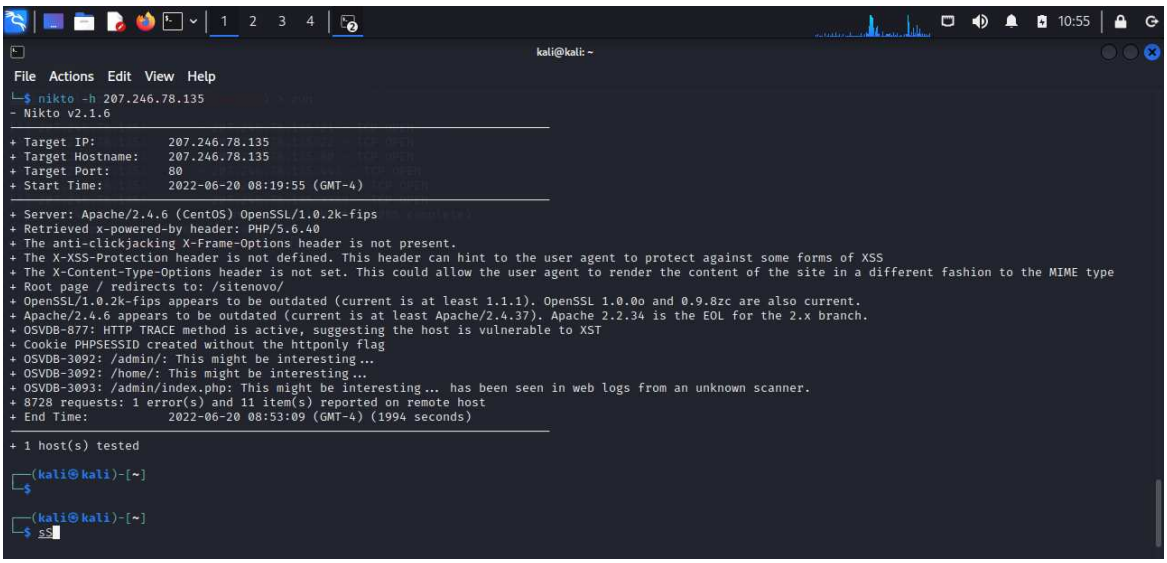
- Versão da Kali Linux utilizado: **kali-linux-2022.2-virtualbox-amd64.ova** no **VirutalBox**
- Sugestão seria o uso de API de comunicação de dados e bloqueio de todas as portas que não sejam apenas as portas HTTPS 443 e HTTP 80.
- Seria importante que as informações estejam em um Data Center no Brasil.

6.16. Utilizando o Nikto para evidenciar softwares desatualizados

Utilizando o Metasploit



Execução:



Utilizando o Kali Linux e msfconsole descobrindo as portas

Versão apresentada até o dia 23/06/2022

A portas TCP 21 / 22 / 80 / 443 / 3386 / 3389 foram identificadas pelo msfconsole do Kali Linux e apresenta alta exposição de portas desnecessárias na internet. Essa exposição pode acarretar ataques constantes ao sistema.

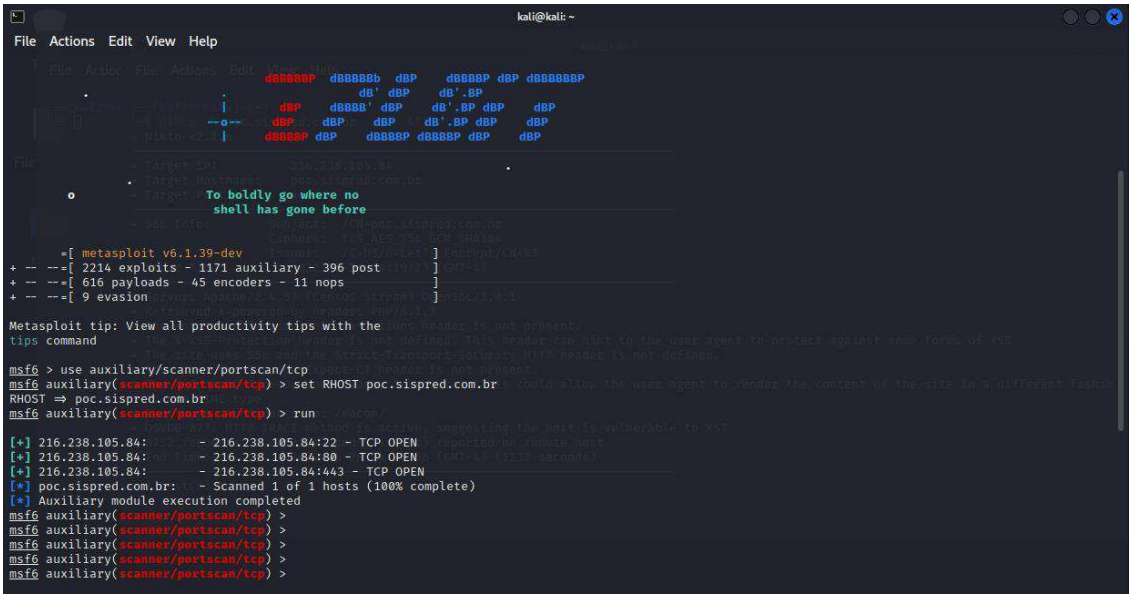
Consideramos apenas as portas 80 e 443 como necessárias para operacionalização do sistema.

Risco Alto

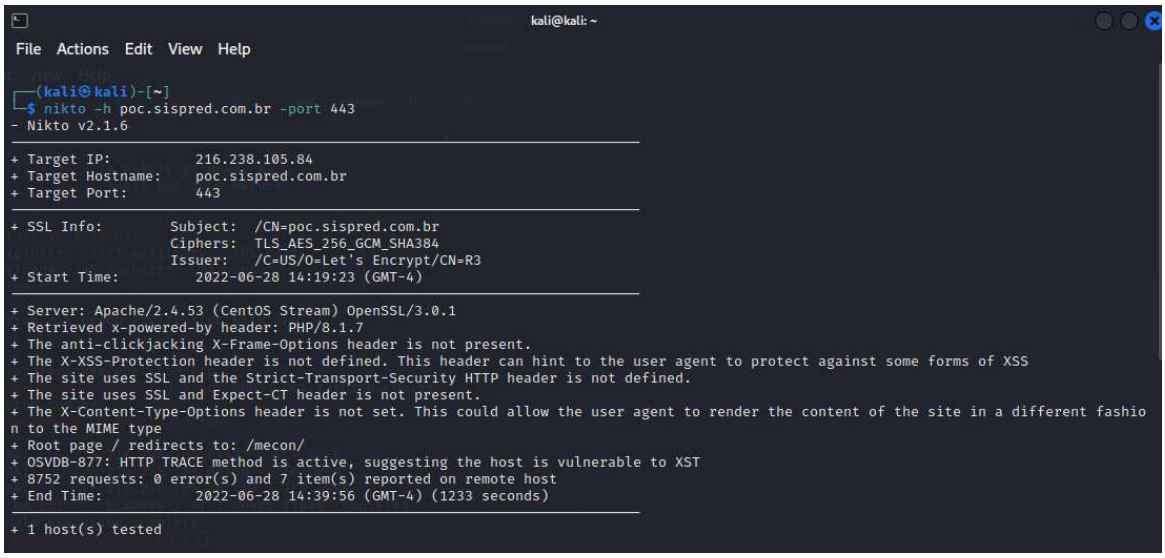
Versão apresentada após o dia 23/06/2022 até 24/06/2022

A portas TCP 22 / 80 / 443 foram identificadas pelo msfconsole do Kali Linux.

Consideramos apenas as portas 80 e 443 como necessárias para operacionalização do sistema.



Encontrado 7 falhas que podem ser utilizadas por pessoas não intencionadas para explorar as vulnerabilidades.



2. CONFORMIDADE LEGAL

Nº	Documento de Referência	Descrição

01	Contrato Nº 39/2018.	Estabelece os termos contratuais firmados entre o MECON e a G4F para prestação de serviços de apoio à gestão de contratos.
02	Instrução Normativa Nº 1, de 4 de abril de 2019.	Dispõe sobre o processo de contratação de soluções de tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.
03	Ordem de Serviço Nº 134/2021	Estabelece o seguinte serviço a ser executado pela contratada: apoiar no gerenciamento de projetos de aquisições, desenvolvimento/evolução de sistemas de informação, infraestrutura e implantação de processos, utilizando a metodologia padrão do Ministério da Economia.
04	Lei Nº 8.666, de 21 DE junho de 1993.	Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
05	Instrução Normativa nº 01/2019 MP/SLTI.	Dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações.

Tabela 2 - Conformidade Legal

7 CONCLUSÃO

Após análise de qualidade da solução tecnológica apresentada pela CONTRATADA referente a Prova de Conceito do processo licitatório para contratação do Facilities, percebe-se que a solução apresentada não está de acordo com critérios definidos no Item “3 - Escopo” deste documento e Anexo VI do Termo de Referência.

7.2 Parecer técnico testes de qualidade

Funcionalidades

A solução apresentou erros em algumas funcionalidades, principalmente na plataforma Web (Microsoft Edge, Safari, Chrome e Mozilla Firefox), Ausência de várias funcionalidades da parte de RH, além da não apresentação de todos os campos da maioria das funcionalidades, entre outros.

Durante a realização da Prova de Conceito compreendida entre o período de 20/06/2022 à 24/06/2022 o sistema passou por constantes evoluções e em paralelo a tentativa de desenvolvimento do módulo de RH o que impossibilitou a realização e validação dessas funcionalidades.

Diante do exposto, sugere-se que a solução seja devolvida para correção das desconformidades e ajustes apontados nos testes realizados.

7.2 Parecer técnico testes de segurança

Pelas análises realizadas no sistema disponível nos links “poc.sispred.com.br/mecon” e o “testes.sispred.com.br/mma” apresentaram falhas de segurança críticas não aderentes a qualidade mínima esperada no Termo de Referência além de demostrar aplicações desatualizadas que configuram um sistema sucetível a ser explorados por usuários maliciosos.

Tipo de avaliação: Conformidade
Estratégia de teste: Verificação manual e inspeção técnica especialista
Status: **Reprovado**

gov.br
Documento assinado digitalmente
IVAN CARLOS DE OLIVEIRA
Data: 29/06/2022 16:11:29-0300
Verifique em https://verificador.iti.br