

## Gestão de Riscos de Segurança Avaliação e Tratamento

Serviço: **Serviço Infosupec**Código: **11723**

Filtros/Tags: **Intranet; Navegador Web. URL (DNS); info.supec.serpro ; Linux; Brasília; PostgreSQL; JDBC; php; TomCat; Apache; Senha-Rede; 15 Horas por dia x 5 Dias por semana**

### 1 - Histórico de Versões:

<b>Versão:</b>	<b>Detalhes:</b>	<b>Data:</b>
1.0	Criação do Artefato	17/3/2020
1.0	Realização do GRS	17/3/2020
2.0	Correções no Risco de Id. 1	22/03/2020

### 2 - Participantes:

<b>Nome:</b>	<b>Lotação:</b>	<b>Ramal</b>	<b>E-mail:</b>
Helen Rose Costa Freitas	supec	(21)2159-3551	<a href="mailto:helen.freitas@serpro.gov.br">helen.freitas@serpro.gov.br</a>
Marcio Cunha	DIOPE/SUPEC/ECRTI/ECCVT	(41) 3137	<a href="mailto:marcio.cunha@serpro.gov.br">marcio.cunha@serpro.gov.br</a>
Leopoldo de Oliveira	DIOPE/SUPEC/ECRTI/ECCVT	(81) 4038	<a href="mailto:leopoldo.oliveira@serpro.gov.br">leopoldo.oliveira@serpro.gov.br</a>
Felipe Cezar	DIOPE/SUPEC/ECRTI/ECCVT	(21) 4705	<a href="mailto:felipe.cezar@serpro.gov.br">felipe.cezar@serpro.gov.br</a>
Emilio Araújo	DIOPE/SUPOP/OPGMR/OPGIP	(31) 6843	<a href="mailto:emilio.araujo@serpro.gov.br">emilio.araujo@serpro.gov.br</a>
Claudio Rocha	DIOPE/SUPCD/CDSAM/CDFAD	(31) 6268	<a href="mailto:claudio.rocha@serpro.gov.br">claudio.rocha@serpro.gov.br</a>
Fernando Rosa	DIOPE/SUPCD/CDSAB/CDSO	(61) 9077	<a href="mailto:fernando.rosa@serpro.gov.br">fernando.rosa@serpro.gov.br</a>
Mario Marcos Martins de Souza (enc. Viviane)	DIOPE/SUPCD/CDIGD/CDIGM	(61) 7611	<a href="mailto:mario.souza@serpro.gov.br">mario.souza@serpro.gov.br</a>

Selma Ester Trevisan	DIDES/SUPSE/SEDES/SEEIM	(41) 1517	selma.trevisan@serpro.gov.br
Mario Marcos Martins de Souza	DIOPE/SUPCD/CDIGD/CDIGM	(61) 7611	mario.souza@serpro.gov.br
Flerida Cristovão (enc. Bruno Assunes)	DIOPE/SUPCD/CDAED/CDBDL	(61) 7565	flerida.lobes@serpro.gov.br
Itallo da Silva Neves (enc. Thiago)	DIOPE/SUPSI/SISEG/SIAIS	(61) 7544	itallo.neves@serpro.gov.br
Julio Cesar Gonçalves Ribeiro	DIOPE/SUPSI/SISEG/SISIF	(61)9520	julio-cesar.ribeiro@serpro.gov.br
Mauro José Santos Brito	DIOPE/SUPCD/CDTE/CDAPA	(91)1774	mauro-jose.brito@serpro.gov.br
<b>Responsável pela Aprovação</b>	<b>Cargo</b>		
<b>Helen Rose Costa Freitas</b>	Coordenador de Negócios		

### 3 - Introdução:

A Avaliação de Riscos visa analisar os dados do projeto, a arquitetura entre outros, a fim de elicitar riscos de segurança inerentes, bem como a definição dos níveis de criticidade. Já o Plano de Tratamento dos Riscos possui o objetivo de selecionar controles, identificar prioridades e propor um plano de ações visando o tratamento dos riscos, caso identificados na etapa de avaliação dos riscos, além de manter um acompanhamento adequado da implementação dos controles.

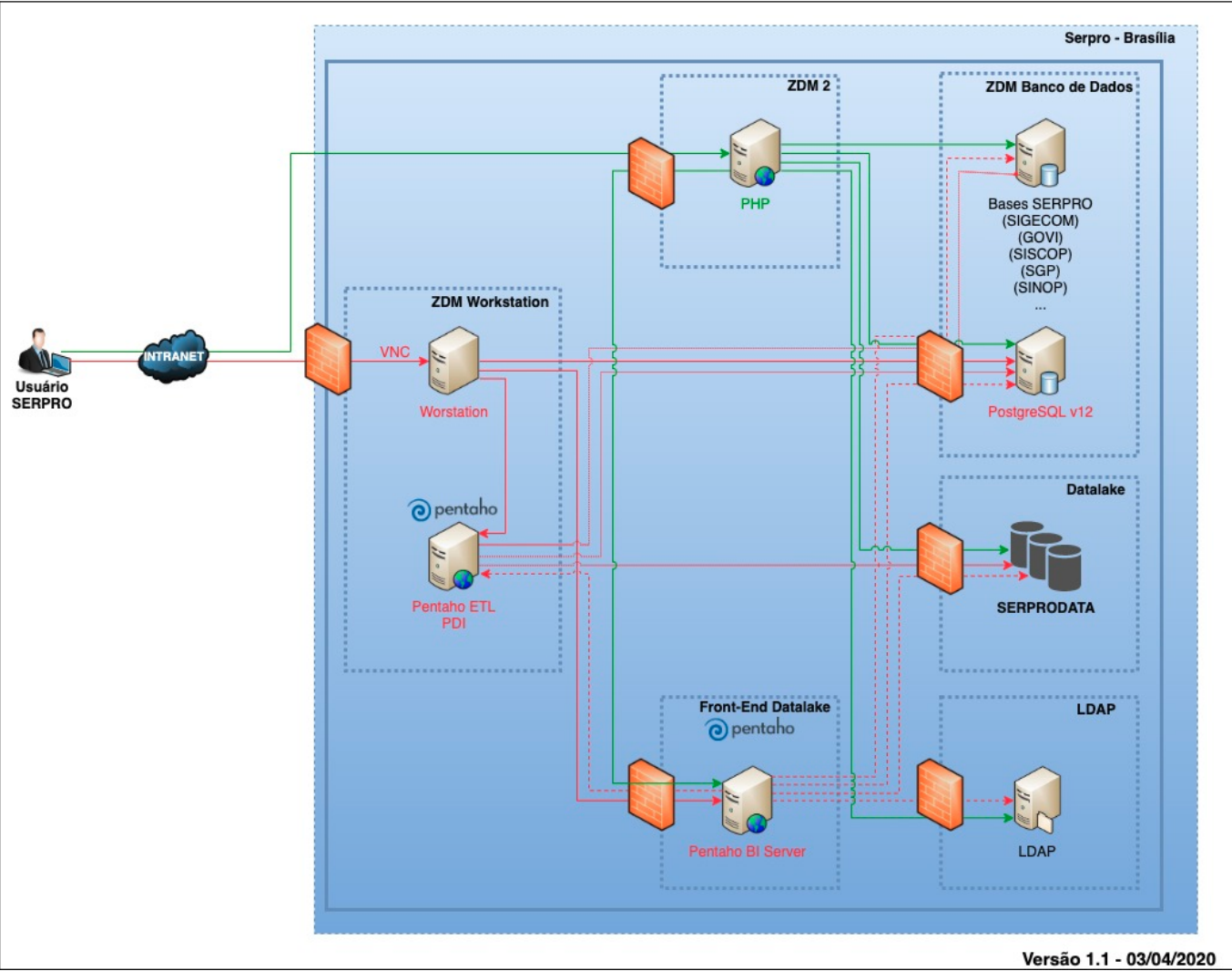
As atualizações devem ser realizadas sempre que ocorrerem alterações significativas nos ambientes (eventualmente) ou periodicamente (anual).

### 4 - Escopo:

O objetivo da arquitetura do Infospec visa promover a geração de processo ETL, relatórios ad-hoc, relatórios de layout estático, análises OLAP, painéis analíticos, mineração de dados e camada de integração por webservice.

4.1 - Arquitetura:

InfoSUPEC



## 4.2 - Documentação Utilizada no Evento:

Arquitetura\_Infospec\_11723  
Formulário de Agendamento - GRS InfoSUPEC 11723  
DAN-InfoSUPEC v1.0  
GR\_DocumentodeVisao\_Infospec-DVS  
Relação Inicial de Participantes- GRS INFOSUPEC -11723

## 4.3 - Descrição:

Localização	Brasília
Responsável	Helen Rose Costa Freitas
Gestor do Projeto	Helen Rose Costa Freitas
Facilitador	Selma Ester Trevisan

## 4.4 - Processos:

Os processos mais relevantes existentes no ambiente do serviço estão descritos na documentação utilizada no subitem 4.2.

## 5 - Resultados Obtidos:

## 5.1 - Ativos:

Durante a Avaliação foram relacionados os ativos que possuem valor para os sistemas de informação incluídos no escopo. A tabela a seguir descreve os ativos incluem as seguintes categorias:

**Ativos Identificados**

<b>Ativos de Software</b>
Vide documentação descrita no item 4

<b>Ativos Físicos</b>
Vide documentação descrita no item 4

<b>Ativos de Serviços</b>
Vide documentação descrita no item 4

<b>Ativos de Informação</b>
Vide documentação descrita no item 4

<b>Ativos de Pessoas</b>
Vide documentação descrita no item 4

5.2 - Riscos Identificados no Escopo do Serviço/Sistema:

<i><b>Id</b></i>	<i><b>Ameaças</b></i>	<i><b>Vulnerabilidades Existentes</b></i>	<i><b>Controles Existentes</b></i>	<i><b>I</b></i>	<i><b>P</b></i>	<i><b>R</b></i>	<i><b>Controles Recomendados</b></i>	<i><b>Categoria de Ativos</b></i>	<i><b>Observações</b></i>
1	Acessos e mau uso de dados. Ex.: extrações ao banco de dados.	Acesso por meio de VNC ao ambiente de produção.	Norma SG022.	A	A	1	Acesso ao ambiente de desenvolvimento deve ser por entreposto. Além disso, acessos devem ser feitos na ZDm de Frontend ao DataLake.	Infraestrutura de Hardware e Software	NORMA: O acesso a ambientes de Produção só é realizado pela SUPCD para acessos administrativos. Só em casos especiais, p. ex. , apurações especiais se abre a regra para outros.
2	Integridade, confidencialidade, entre outras ameaças a dados pessoais.	Dados pessoais sensíveis a acessos indevidos.	Lei Geral de Proteção a Dados Pessoais.	A	A	1	Consultar e alinhar ações necessárias inerentes à LGPD junto aos responsáveis.	Infraestrutura de Hardware e Software	

5.3 - Plano de Tratamento dos Riscos:

Id	R	Controle Definido	Ação	Responsável	Prazo	Observações	Situação
1	1	Acessos a ambientes de desenvolvimento e produção devem ser por entreposto. Além disso, acessos devem ser feito na ZDm de Frontend ao DataLake.	1. Discutir se é possível utilizar entreposto; 2. Discutir a possibilidade , e se sim, implementar um DataLake de desenvolvim ento.	Helen / Márcio, em conjunto com equipe multidisciplinar.	20/04/2020		Não Iniciada.
2	2	Consultar e alinhar ações necessárias inerentes à LGPD junto aos responsáveis.	1. Consultar lei e responsáveis pela utilização da LGPD no SERPRO; 2. Acionar equipe multidisciplin ar caso necessário.	Helen / Márcio, em conjunto com equipe multidisciplinar (Leandro Gomes).	20/04/2020		Não Iniciada.

Onde:

- Id:** Identificação do item;
- R:** Nível do Risco (1,2,3,4 );
- Controle Definido:** Descrição dos controles a serem adotados para tratar o risco;
- Ação:** Ações a serem desenvolvidas para a implementação do controle;
- Responsável:** Responsável pelo desenvolvimento de cada ação;
- Prazo:** Data prevista de conclusão da implementação da ação;
- Observações:** Qualquer informação importante para o escopo ou código do controle da ABNT NBR ISO/IEC 27001:2006 (coluna opcional);
- Situação:** - Situação do desenvolvimento da ação (não iniciada, em andamento, suspensa, cancelada ou concluída. Se concluída, informar data de conclusão). Nos casos onde não há ação a ser executada, informar a situação de risco aceito;
- Os controles que não serão implementados em função de questões de custos, devem ter essa condição registrada.

6 - Histórico das Decisões Adotadas:

A seguir são descritas as decisões adotadas na fase de Avaliação dos Riscos.

Id	Descrição das Decisões
1.	Será enviado o relatório de avaliação e tratamento de riscos aos participantes, pelo Agendador GRS.
2.	Helen / Marcio: Enviar matriz de conectividades.
3.	Helen: Pedir abertura de RDM's para produção e homologação.
4.	
5.	
6.	
7.	



## 7 - Outras Considerações:

- Código de Serviço SIGECOM:	11723
- Unidade Gestora (UG):	SUPEC
- Data Prevista para a Homologação:	25/04/2020
- Data Prevista para a Entrada em Produção:	01/05/2020

### IMPORTANTE

- Os números/ID's da RDM's criadas (se houver) deverão ser informadas em nota para "agendamento-grs@serpro.gov.br"
- Qualquer ação tratativa (se houver) deve ser informada em nota para "agendamento-grs@serpro.gov.br"

**- Não existe uma topologia homologada de desenvolvimento e produção explicitadas para análise.**