MUNICÍPIO DE PINHEIRO PRETO

DIRETORIA DE INFORMÁTICA E TRANSPARÊNCIA

ESTUDO TÉCNICO PRELIMINAR

"ESCOPO DA CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA ASSESSORIA, PLANEJAMENTO E IMPLEMENTAÇÃO DE PROJETO DE SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE ORGANIZACIONAL PARA A INFRAESTRUTURA DE TIC (TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES) DA PREFEITURA MUNICIPAL DE PINHEIRO PRETO."

Pinheiro Preto – 2024

1. NECESSIDADE DA CONTRATAÇÃO

A Diretoria de Informática e Transparência da Prefeitura de Pinheiro Preto desempenha um papel fundamental no gerenciamento dos pilares da Segurança da Informação (disponibilidade, integridade, autenticidade, confidencialidade, legalidade) da infraestrutura de TIC (Tecnologia da Informação e Comunicações) da administração municipal. Esta responsabilidade abrange a totalidade das necessidades estratégicas e técnicas para rodagem dos serviços online disponibilizados aos cidadãos, bem como os sistemas e dados internos.

Proteger a infraestrutura de TIC, portanto, configura-se como um componente estratégico vital à administração municipal, pois é sobre essa base tecnológica que se sustentam serviços essenciais à população, o cumprimento de obrigações legais, a comunicação transparente com a sociedade e a gestão eficiente dos recursos públicos.

Neste sentido, a negligência em relação à segurança da informação pode resultar em incidentes com consequências catastróficas, que ferem os princípios da administração pública. Quando as necessidades tecnológicas não são geridas de maneira profissional e em alinhamento com as melhores práticas, normas técnicas e legislação, a mera ocorrência de um evento chamado "Desastre de TI", possui potencial para não apenas interromper a prestação de serviços momentaneamente, mas tornar irrecuperável as atividades dependentes de TIC, repercutindo de maneira direta e severa na vida dos cidadãos.

Há diversos fatores que podem desencadear um Desastre de TI, desde falhas humanas e tecnológicas até eventos da natureza. A negligência na manipulação de dados ou configurações incorretas de sistemas, são uma causa significativa de incidentes. Falhas de hardware, como problemas em servidores ou equipamentos de armazenamento, representam um risco constante, assim como as falhas elétricas, que podem comprometer o funcionamento da infraestrutura de TI.

A crescente dependência digital também expõe o município a ataques cibernéticos cada vez mais sofisticados. Ataques de *ransomware*, invasões de *hackers* e ataques de negação de serviço (DDoS) podem comprometer dados, sistemas e a continuidade dos serviços. Falhas de software, como *bugs* e vulnerabilidades, também podem levar a interrupções significativas.

É crucial destacar que os desastres de TI não se limitam ao mundo digital. Desastres climáticos como incêndios e inundações, falhas na infraestrutura civil como desabamentos e até mesmo a falha na segurança do perímetro, permitindo acesso físico indevido aos equipamentos, podem ter impactos catastróficos. Da mesma forma, interrupções nos serviços terceirizados, como provedores de internet ou suporte a softwares, representam um risco adicional.

Em um cenário de ameaças cibernéticas cada vez mais frequentes e sofisticadas, a questão não é mais se, mas quando uma organização será alvo de um ataque. A gravidade da situação é evidenciada por ataques recentes a importantes entes e órgãos públicos brasileiros, incluindo o Tribunal Superior Eleitoral (TSE), o Ministério da Saúde, o Superior Tribunal de Justiça (STJ), o Tribunal de Justiça do Rio Grande do Sul (TJRS), o Governo do Distrito Federal, o Detran SP e a DataPrev, entre outros. Esses ataques, que vão desde invasões hackers e ransomware até vazamentos de dados, demonstram a vulnerabilidade do setor público e a necessidade urgente de ação.

Além disso, o incidente de segurança cibernética ocorrido em 07 de setembro de 2024, no qual a própria Prefeitura de Pinheiro Preto foi vitimada por um ataque de *ransomware* que criptografou completamente a infraestrutura crítica de TI incluindo o *backup* local, destaca a complexidade e a periculosidade das ameaças contemporâneas, além de expor a vulnerabilidade dos sistemas digitais municipais. Este evento sublinha a necessidade premente de implementar políticas de segurança da informação e procedimentos de recuperação de desastres eficazes e robustos.

Como se pode observar, a ocorrência de um desastre de TI representa uma ameaça crítica e iminente para o município, podendo ter inúmeras origens e consequências devastadoras em múltiplas esferas. A

paralisação da administração pública, a interrupção dos serviços essenciais aos cidadãos, os danos à reputação, os altos custos ou a impossibilidade de recuperação e as potenciais implicações legais são apenas alguns exemplos dos riscos envolvidos.

Nesse contexto, onde a iminência e a inevitabilidade da ocorrência de um desses eventos são certas, é essencial que o município adote estratégias robustas e confiáveis não apenas de prevenção, mas de recuperação de desastres de TI e continuidade operacional. Essas estratégias devem incluir a realização de backups regulares, abrangentes e testados, a implementação de sistemas redundantes e de alta disponibilidade, a elaboração de planos de contingência detalhados, o treinamento constante da equipe de TI para uma resposta eficaz em emergências e o monitoramento e gestão de mudanças na infraestrutura de TI com o objetivo de evitar novas vulnerabilidades. Ao implementar essas estratégias, será possível assegurar uma resposta eficiente e eficaz a incidentes, minimizando os impactos negativos e garantindo a continuidade das atividades do município.

2. CENÁRIO ATUAL

2.1. Análise da Infraestrutura de TI e Segurança da Informação

Atualmente, a Prefeitura de Pinheiro Preto concentra a maioria dos seus sistemas críticos e dados no CPD (Central de Processamento de Dados) localizado no paço municipal. Essa centralização gera a exposição da TI do município a um risco significativo de interrupção dos serviços em caso de desastres naturais, falhas de infraestrutura ou incidentes que afetem o local.

O maior impacto seria na conectividade de Internet, nos sistemas como o TMI, Pública, emissão de nota fiscal rural, dados das secretarias e até mesmo o acervo histórico municipal. Apenas os serviços de e-mail, GOVBox e 1DOC, não seriam afetadas caso o CPD seja comprometido, porém, seus acessos estariam igualmente impossibilitados pois não haveria conexão de rede e internet disponíveis.

Fica evidente que manter os dados exclusivamente na infraestrutura de TI da prefeitura representa um risco significativo para a continuidade operacional da administração pública, já que qualquer incidente local poderia comprometer a recuperação e a continuidade dos sistemas de informação. Diante desse cenário, torna-se imprescindível a criação e manutenção de cópias de segurança dentro e fora das dependências da prefeitura.

2.2. Recente Ataque de Ransonware

Entre os dias 07/09/2024 e 12/09/2024, a Prefeitura de Pinheiro Preto sofreu um ataque de ransomware, comprometendo todos os dados sob sua gestão, incluindo o servidor de backup local. O incidente resultou na criptografia total das informações, caracterizando um típico desastre de TI.

O Serviço de Recuperação de Desastres de TI prestado pela BR Soluções em TI garantiu a restauração dos sistemas e serviços críticos. A existência de backups periódicos, abrangentes e testados, armazenados

externamente tanto na nuvem quanto de forma offline em fitas LTO foi fundamental. Essa estratégia permitiu, apesar da criptografia do servidor de backup local, a rápida recuperação dos sistemas e a retomada das operações administrativas, sem perdas significativas de dados.

Destaca-se que, caso essas salvaguardas não estivessem em vigor, a administração pública teria ficado sem alternativas para recuperar os dados, o que poderia ter resultado na paralisação completa dos serviços essenciais, na necessidade de negociar o pagamento de resgate com criminosos sem garantia de sucesso e na perda irreparável de informações.

Este incidente reforça necessidade urgente da Prefeitura de Pinheiro Preto adotar medidas proativas e avançadas de segurança da informação. A implementação e o aprimoramento contínuo de um Plano de Recuperação de Desastres, com backups externos e testes regulares, são fundamentais para garantir a proteção dos dados, a continuidade dos serviços públicos e a confiança dos cidadãos, sendo a prevenção o melhor remédio em um cenário digital cada vez mais complexo e suscetível a ameaças imprevisíveis, como a que recentemente atingiu o município.

3. DEFINIÇÃO DO ESCOPO ESTRATÉGICO DA CONTRATAÇÃO

3.1. Objetivo Estratégico

Este estudo tem como objetivo definir o escopo técnico-estratégico para que a prefeitura assegure a segurança da informação e a continuidade operacional de sua infraestrutura de TI, elencando as tecnologias, ações e componentes necessários para implementar as capacidades de proteção e recuperação adequadas.

3.2. Estudo de Frameworks de Boas Práticas, Normas Técnicas e Legislações de

Segurança da Informação e Continuidade Organizacional

Para alcançar os objetivos de Segurança da Informação do município, a Diretoria de Informática e Transparência está direcionando suas ações e estratégias com base nas recomendações de normas e padrões técnicos estabelecidos por organizações internacionalmente reconhecidas. Esse alinhamento assegura que os procedimentos adotados estejam em conformidade com os mais altos padrões de segurança e eficácia, promovendo uma gestão eficiente de riscos e uma recuperação ágil em situações de desastre.

As diretrizes adotadas abrangem desde a análise de riscos até a implementação de soluções de continuidade de negócios, assegurando uma abordagem sistemática e integrada para proteger os ativos de informação críticos do município.

As principais diretrizes que orientam essas estratégias incluem:

1. **COBIT (Governança de TI):** Fornece um modelo abrangente que ajuda as organizações a alcançarem seus objetivos de TI, focando em governança e gestão.

2. **ITIL (Gestão de Serviços de TI):** Oferece práticas detalhadas para a gestão de serviços de TI, focando na alinhar os serviços de TI às necessidades dos negócios.

3. **NIST Cybersecurity Framework (CSF) (Gestão de Cibersegurança):** Um framework para melhorar a segurança cibernética de infraestruturas críticas, oferecendo diretrizes para prevenir, detectar e responder a ataques cibernéticos.

4. **ISO/IEC 27001 (Gestão em Segurança da Informação):** Um conjunto de padrões para sistemas de gestão de segurança da informação (SGSI), que inclui políticas e procedimentos para proteger informações confidenciais.

5. **BCI Good Practice Guidelines:** Diretrizes de boas práticas do Business Continuity Institute para a gestão da continuidade dos negócios, ajudando as organizações a se prepararem para, responderem e se recuperarem de interrupções.

3.3. Recomendações extraídas das normas e frameworks consultados:

Na tabela a seguir, apresentamos um conjunto de recomendações essenciais derivadas dos frameworks de boas práticas de referência. Estas foram cuidadosamente selecionadas pela Diretoria de Informática com o objetivo de orientar a elaboração do Plano de Recuperação de Desastres do município e são fundamentais para estabelecer uma estrutura robusta que assegure a segurança da informação e a continuidade das operações municipais em cenários de crise:

3.3.1. DIRETRIZES ESTRATÉGICAS PARA O PRD			
STANDARD OU FRAMEWORK		**OBJETIVO E RECOMENDAÇÕES**	**AÇÕES VOLTADAS AO PRD**
1	**COBIT 2019** Governança de TI e Gestão de Riscos	**Integrar governança de TI na estratégia da organização** - Avaliação de maturidade dos processos de TI. - Estabelecimento de objetivos de controle.	**Alinhamento estratégico** Criação do comitê de crises cibernéticas para definir os Objetivos de Ponto e Tempo de recuperação em ata oficial envolvendo a alta administração.
		- Monitoramento de desempenho de TI.	**Otimização de recursos** Testar periodicamente a efetividade do PRD e apontar as melhorias necessárias.

			Medição de desempenho Instituir calendários de testes e homologações do plano de recuperação com participação da alta administração.
2	**ITIL V4** Definição de processos de gestão de serviços de TI	**Implementar práticas avançadas de gestão de serviços de TI para otimizar a eficiência operacional e garantir um alinhamento estratégico entre as funções de TI e os objetivos globais da organização** - Gerenciamento de incidentes. - Gerenciamento de mudanças. - Melhoria contínua dos serviços.	**Gerenciamento de incidentes** Criar um grupo em aplicativo de mensagens para a comunicação de incidentes de TI para todos os usuários.
			Gerenciamento de disponibilidade Possuir meios alternativos de reestabelecer os serviços críticos em um período que não gere prejuízos.
3	**NIST SP 800-34** Cybersecurity Framework (CSF)	**Desenvolver um plano de continuidade de operações visando minimizar interrupções e recuperar funções críticas rapidamente** - Desenvolvimento de estratégias de recuperação. - Realização de testes e exercícios regulares.	**Identificação de ativos críticos e objetivos de recuperação** Listagem dos itens protegidos e se respectivos RPO e RTO individuais.
			Proteção de ativos Implementar uma infraestrutura de backup e replicação adequada aos riscos e necessidades técnicas.
			Resposta a incidentes

		- Atualização contínua do plano.	Descrição do que é um evento de desastre e quem pode declará-lo.
			Recuperação de serviços Ações pós declaração de desastres, matriz de comunicação entre prestadores de serviço, TI e alta administração e requisitos para declaração de encerramento de crise.
4	**ISO/IEC 27001** Gestão de Segurança da Informação (SGSI)	**Proteger informações contra ameaças, garantindo segurança** - Implementação de um Sistema de Gestão de Segurança da Informação (SGSI)	**Política de segurança da informação** Criar um documento com as bases, diretrizes e objetivos de segurança da informação.
			Segurança em recursos humanos Realizar workshops e treinamentos periódicos sobre segurança da informação para os colaboradores com objetivo de mitigar riscos humanos.
			Segurança física e lógica do ambiente Controlar o acesso físicos e lógicos aos ambientes de TI.
5	**BCI Good Practice Guidelines** Análise de impacto no negócio (BIA) e estratégias de recuperação	**Análise de impacto nos negócios (BIA)** - Identificar processos de negócio dependentes de TI e impactos de interrupções/perdas.	**Segurança e prevenção** Gerenciar recursos necessários para a recuperação.

Após um exame minucioso, foi possível constatar que a aplicação de todas as recomendações e diretrizes sugeridas não se alinha às condições operacionais e financeiras da prefeitura, além de não serem estritamente necessárias.

Diante deste cenário, a estratégia mais eficaz e realista envolve a seleção e implementação das recomendações essenciais que sejam viáveis financeiramente e que, simultaneamente, ofereçam um nível de segurança e proteção adequados. Esta abordagem pragmática permite otimizar recursos, assegurando a implementação de medidas de segurança críticas sem comprometer a sustentabilidade financeira e operacional da prefeitura.

Portanto, de acordo com as recomendações acima listadas, o Plano de Recuperação de Desastres de TI deve ser orientado por dois critérios fundamentais, que servem como pilares para a sua efetividade e relevância estratégica:

3.4. Objetivo de Ponto de Recuperação (RPO): Este critério define o volume máximo de dados que a organização pode se permitir perder em função de um desastre, expresso em termos de tempo. O RPO é determinante para estabelecer a periodicidade dos backups. A precisão na definição do RPO permite à organização equilibrar de maneira eficaz a necessidade de proteção de dados com os custos operacionais e de infraestrutura associados às soluções de backup.

3.5. Objetivo de Tempo de Recuperação (RTO): Este critério estabelece o tempo máximo aceitável para a recuperação das operações e sistemas de TI após um incidente, assegurando a retomada das atividades empresariais dentro de um intervalo de tempo considerado crítico para a sustentabilidade do negócio. O RTO é crucial para planejar a capacidade de resposta da infraestrutura de TI e dos processos de negócio em situações adversas.

A definição dos valores de RPO e RTO deve ser realizada em colaboração estreita com a administração da organização, assegurando que as metas estabelecidas estejam em consonância com as prioridades

estratégicas e a capacidade de investimento da organização. Com esses objetivos definidos, incumbe à área de tecnologia da informação a responsabilidade de:

3.6. Estruturar o Plano de Recuperação de Desastres: Isso inclui a identificação detalhada dos sistemas e processos de negócio críticos, bem como dos recursos necessários para a recuperação efetiva.

3.7. Listar Componentes e Características Técnicas: Deve-se detalhar as soluções de backup adotadas, a infraestrutura de TI envolvida, os softwares utilizados e os procedimentos operacionais para a recuperação de dados e sistemas.

3.8. Apresentar o Cenário Técnico-Econômico: Avaliar e propor a solução mais adequada para a implementação do plano, considerando uma análise de custo-benefício que identifique a opção mais eficiente e economicamente viável.

4. ESTRUTURA DO PLANO DE RECUPERAÇÃO DE DESASTRES DE TI

A concretização dos objetivos do Plano de Recuperação de Desastres do município só pode ser assegurada por meio da adoção de uma estratégia de backups de imagem (point-in-time) abrangente, íntegra e confiável. Essencialmente, esta estratégia precisa envolver a totalidade da infraestrutura de Tecnologia da Informação (TI) da qual depende a administração municipal.

Além disso, é imperativo que essas cópias de segurança sejam armazenadas em uma variedade de mídias físicas e digitais, bem como distribuídas em múltiplas geolocalizações, para garantir a máxima proteção e acessibilidade em caso de qualquer eventualidade que possa comprometer os dados originais.

Conforme levantamento realizado pela Diretoria de Informática e Transparência, a estratégia de backup do PRD deve incluir a proteção dos seguintes componentes e dados críticos para a operação da Prefeitura de Pinheiro Preto, localizados em duas localidades: o Paço Municipal e a Secretaria de Saúde:

4.1. INVENTÁRIO DE ITENS PROTEGID OS		
LOCAL	**ITEM**	**QUANTIDADE**

Paço municipal	Host de Virtualização (Hyper-V)	01 unidade
	VMs (Servidores Virtuais)	08 unidades
Secretaria de Saúde	Hosts de Virtualização (Hyper-V)	01 unidade
	VMs (Servidores Virtuais)	08 unidades

Para assegurar a resiliência e a continuidade das operações do Município de Pinheiro Preto frente a incidentes de TI, é essencial estabelecer metas claras e rigorosas para a recuperação de dados e sistemas. Nesse contexto, os seguintes objetivos mínimos de tempo de recuperação devem ser implementados:

4.2. OBJETIVOS DE RPO E RTO DE CADA ITEM PROTEGIDO			
LOCAL	**ITEM**	**RPO**	**RTO**
Paço municipal	Hosts de Virtualização (Hyper-V)	48 horas	48 horas
	VMs (Servidores Virtuais)	48 horas	48 horas
Secretaria de Saúde	Hosts de Virtualização (Hyper-V)	48 horas	48 horas
	VMs (Servidores Virtuais)	48 horas	48 horas

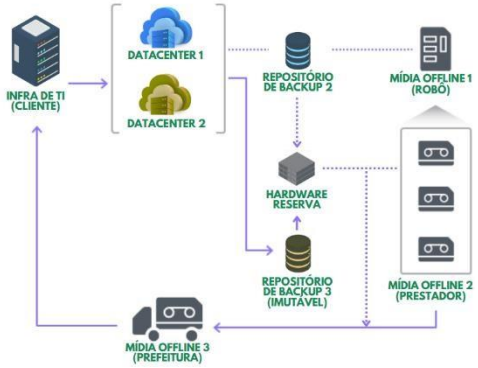
A Estratégia de Backup **3-2-1** (3 cópias, 2 tipos de mídias e 1 offsite/remoto), apesar de ser uma recomendação mínima, não é suficiente contra ameaças cibernéticas avançadas e desastres de TI de maior impacto.

As ameaças atuais exigem soluções mais robustas, incluindo criptografia avançada, backups em diversas geolocalizações, diferentes tipos de armazenamento incluindo cópias offline e sobretudo acompanhamento diário e um rígido calendário de testes de restauração.

Portanto, para o cumprimento dos objetivos de ponto e tempo de restauração o PRD da prefeitura de Pinheiro Preto, a estratégia **6-5-3-3-1-1-1-1-0** deve ser adotada.

- 6 cópias
- 5 tipos de mídias
- 3 geolocalizações

- 3 mídias offline automatizadas alternadas
- 1 cloud pública imutável
- 1 cloud privada
- 1 hardware reserva
- 1 teste periódico
- 0 falhas



5. LISTA DE COMPONENTES E CARACTERÍSTICAS TÉCNICAS

Para a efetiva implementação do Plano de Recuperação de Desastres (PRD), a Diretoria de Informática e Transparência identificou a necessidade de aquisição/subscrição de determinadas ferramentas e soluções tecnológicas essenciais. Estas são fundamentais para estabelecer uma infraestrutura resiliente e preparada para responder a incidentes de segurança de forma eficaz. As soluções selecionadas abrangem desde software até hardware, incluindo suporte técnico especializado e procedimentos de teste rigorosos, garantindo a integridade e disponibilidade dos dados em qualquer cenário adverso:

5.1 FERRAMENTAS E SOLUÇÕES NECESSÁRIAS PARA IMPLEMENTAÇÃO DO PRD		
5.1.1.	**SOFTWARE PROFISSIONAL DE BACKUP**	Ferramenta avançada para a criação de cópias de segurança dos dados críticos, permitindo a restauração rápida das informações em caso de perda ou danos.
5.1.2.	**CONFIGURAÇÃO DE REDE IP E SUA SEGURANÇA**	Configuração e otimização de isolamento de rede para suportar operações de backup e replicação de dados sem comprometer o desempenho da rede existente.

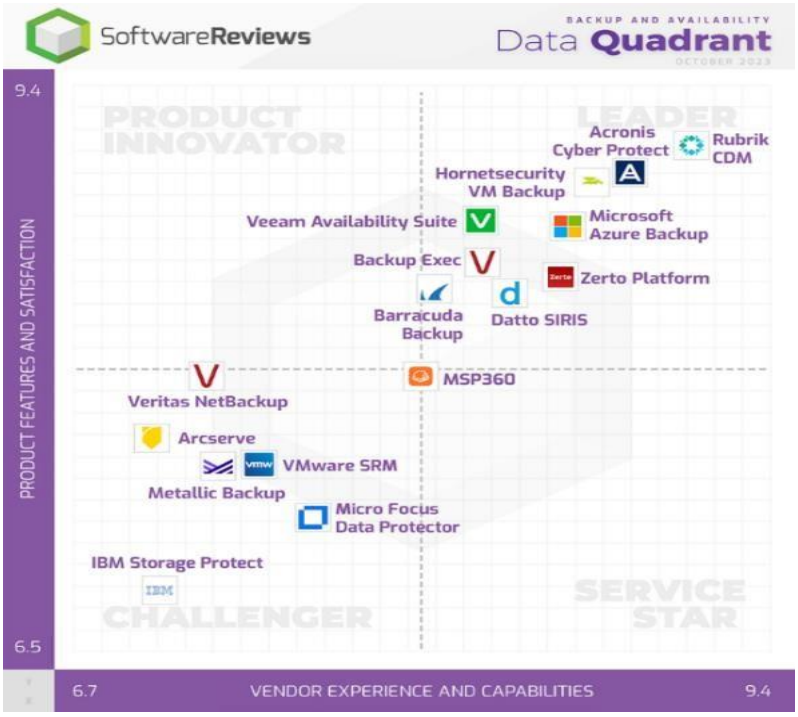
5.1.3.	**HOSTS DE VIRTUALIZAÇÃO, SWITCHS, NOBREAKS, ACCESS POINTS**	Equipamentos para hospedar o software profissional de backup, receber as replicações, armazenar as cópias de segurança, fornecer energia e conectividade IP para o plano.
5.1.4.	**CONFIGURAÇÃO DAS ROTINAS DE BACKUP E REPLICAÇÃO**	Estabelecimento de procedimentos operacionais para a execução regular e automatizada de backups e replicações, assegurando a continuidade dos serviços.
5.1.5	**OPERACIONALIZAÇÃO DO PLANO DE RECUPERAÇÃO E SUPORTE TÉCNICO**	Serviços de suporte técnico para manutenção e solução de problemas, armazenamento de dados conforme cada rotina, complementados por testes regulares de restauração para validar a
		eficácia e a prontidão do sistema de recuperação de desastres.

5.1.1. REQUISITOS DO SOFTWARE PROFISSIONAL DE BACKUP

Após uma avaliação detalhada e testes iniciais, a equipe de TI constatou que o uso de scripts personalizados ou ferramentas de backup gratuitas não atende aos requisitos necessários para a segurança e gestão eficaz dos dados. Em um ambiente onde a proteção e a recuperação de informações são vitais, depender de soluções que não oferecem suporte confiável, garantias ou funcionalidades avançadas representa um risco inaceitável.

Além disso, os testes revelaram que as opções gratuitas carecem de funcionalidades críticas, tais como operação intuitiva, suporte a diversos tipos de armazenamento, deduplicação, compressão, e a realização de backups incrementais, diferenciais e sintéticos. Essas características são indispensáveis para o desenvolvimento de um sistema de backup e recuperação eficiente e seguro.

Diante dessas constatações, verifica-se que a alternativa mais segura e eficiente é a implementação de um software de backup e restauração de nível corporativo. Este posicionamento é corroborado por análises de renome, como a realizada pela Gartner no documento “Magic Quadrant for Enterprise Backup and Recovery Software Solutions”, que avalia as soluções disponíveis no mercado com base em sua capacidade e eficácia.



As soluções destacadas no Quadrante Mágico da Gartner são projetadas para realizar backups point-in-time (imagem de backup) de cargas de trabalho empresariais, abrangendo ambientes onpremises, híbridos, multinuvem, SaaS e BaaS (Backup as a Service). Essas soluções são essenciais para a recuperação de dados em situações de perda, oferecendo flexibilidade na contratação, que pode ser realizada através da compra direta do software, soluções integradas em appliances físicos e virtuais, ou por meio de modelos SaaS e BaaS.

Para atender às necessidades do PRD, é fundamental que as empresas fornecedoras sejam revendedoras autorizadas dos softwares de backup corporativo mencionados no Quadrante Mágico da Gartner nos últimos dois anos. Este critério assegura que o fornecedor não apenas disponibilize uma solução de backup de ponta, mas também possua uma equipe técnica altamente especializada, capaz de realizar a instalação, configuração, manutenção, suporte e atendimento de chamados de forma eficiente para a solução de backup escolhida.

A solução de backup profissional também deve possuir obrigatoriamente as especificações técnicas elencadas na tabela baixo, destinadas a oferecer uma abordagem de backup integral e de alto desempenho. Este conjunto de especificações técnicas é necessário para garantir que a ferramenta de backup atenda aos desafios específicos relacionados à gestão de dados em ambientes governamentais, assegurando a resiliência e a integridade dos dados essenciais para as operações no município:

5.1.1.1. ESPECIFICAÇÕES TÉCNICAS DO SOFTWARE PROFISSIONAL DE BACKUP	
Proteção Contínua para Máquinas Virtuais	Capacidade de salvaguardar máquinas virtuais sem afetar seu funcionamento ou performance.
Otimização de Dados	Implementação de deduplicação e compressão para reduzir o volume de dados das máquinas virtuais.
Replicação Flexível	Suporte à replicação de máquinas virtuais em diversos ambientes.
Verificação de Integridade dos Backups	Funcionalidade para assegurar a consistência e a integridade dos dados armazenados.
Gestão Automatizada de Armazenamento	Administração e alocação inteligente do espaço de armazenamento de backup, com suporte a storages de objetos em nuvens como Google Cloud, AWS, Azure e Wasabi.
Segurança de Dados	Criptografia de dados em repouso e em trânsito, garantindo a confidencialidade das informações.

Políticas de Retenção Flexíveis	Possibilidade de definir políticas de retenção específicas para diferentes jobs ou máquinas virtuais.
Backups sem Agentes	Capacidade de realizar backups completos sem a necessidade de instalar agentes nas máquinas virtuais.
Backups Incrementais Eficientes	Realização de backups incrementais, transmitindo apenas os dados que foram alterados.
Notificações Proativas	Envio de alertas e notificações por e-mail sobre o status dos backups.
Interface de Gerenciamento Intuitiva	Uma interface simplificada que fornece visibilidade completa sobre o estado dos backups, incluindo detalhes dos backups realizados e das cópias disponíveis.

5.1.2. CONFIGURAÇÕES DE SEGURANÇA DE REDE

A Diretoria de Informática e Transparência identificou a necessidade de implementar configurações de rede específicas para suportar eficazmente o Plano de Recuperação de Desastres (PRD), detalhadas a seguir:

5.1.2.1. CONFIGURAÇÕES DE REDE PARA O PRD	
Implementação de Segregação e Isolamento do Ambiente de Rede Corporativa, Rede Wi-fi de Visitantes e Rede do PRD	
LOCALIZAÇÃO	**CONFIGURAÇÃO DE REDE**

PAÇO MUNICIPAL	**IMPLANTAÇÃO DE FIREWALL NEXT GENERATION**: o FW-NG pode ser implementado em uma appliance física ou virtual, com as seguintes características: • Inspeção profunda de pacotes (DPI) • Sistema de Prevenção de Intrusões (IPS) • Antivírus e anti-malware integrados • Filtragem de URL • Controle de aplicações granular com pelo menos 5.000 assinaturas • Inspeção SSL/TLS • Sandboxing para análise de ameaças desconhecidas • Proteção contra ataques de negação de serviço (DoS/DDoS) • Suporte a IPv4 e IPv6 • VLANs e agregação de links (LACP) • NAT (Network Address Translation) avançado • QoS (Quality of Service) e traffic shaping • VPN IPSec e SSL com suporte para milhares de túneis simultâneos • Interface de gerenciamento web intuitiva • CLI (Command Line Interface) para configuração avançada • SNMP v2c e v3 para monitoramento • Suporte a syslog para centralização de logs • Relatórios detalhados e personalizáveis
	PDR VPN SERVER SITE-TO-SITE: Configuração de um servidor VPN para conectar o paço municipal à Secretaria de Saúde.
	PDR2 VPN CLIENT SITE-TO-SITE: Configuração de um servidor VPN para conectar o paço municipal à infraestrutura de Cloud.

SECRETARIA DE SAÚDE	**IMPLEMENTAÇÃO DE FIREWALL NEXT GENERATION**: o FW-NG pode ser implementado em uma appliance física ou virtual, com as seguintes características: • Inspeção profunda de pacotes (DPI) • Sistema de Prevenção de Intrusões (IPS) • Antivírus e anti-malware integrados • Filtragem de URL • Controle de aplicações granular com pelo menos 5.000 assinaturas • Inspeção SSL/TLS • Sandboxing para análise de ameaças desconhecidas • Proteção contra ataques de negação de serviço (DoS/DDoS) • Suporte a IPv4 e IPv6 • VLANs e agregação de links (LACP) • NAT (Network Address Translation) avançado • QoS (Quality of Service) e traffic shaping • VPN IPSec e SSL com suporte para milhares de túneis simultâneos • Interface de gerenciamento web intuitiva • CLI (Command Line Interface) para configuração avançada • SNMP v2c e v3 para monitoramento • Suporte a syslog para centralização de logs • Relatórios detalhados e personalizáveis
	PDR1 VPN CLIENT SITE-TO-SITE: Configuração de um cliente VPN para conectar a Secretaria de Saúde ao paço municipal.
	PDR2 VPN CLIENT SITE-TO-SITE: Configuração de um cliente VPN para conectar a Secretaria de Saúde à infraestrutura de Cloud.
INFRAESTRUTURA EM NUVEM	**PDR1 VPN SERVER SITE-TO-SITE:** Configuração de um servidor VPN replicado para uso em cenários de failover.

5.1.3. DIAGRAMA DE REDE PARA O PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

O diagrama de rede a seguir foi meticulosamente desenvolvido para ilustrar as conexões estratégicas entre o paço municipal, a Secretaria de Saúde e a infraestrutura em nuvem. Este esquema reflete as configurações de VPN detalhadas anteriormente, proporcionando uma visualização clara da infraestrutura de rede projetada para suportar o Plano de Recuperação de Desastres (PRD). As conexões VPN site-to-site

são fundamentais para garantir a segurança, a segregação e o isolamento adequados dos ambientes de rede, essenciais para a eficácia do PRD.

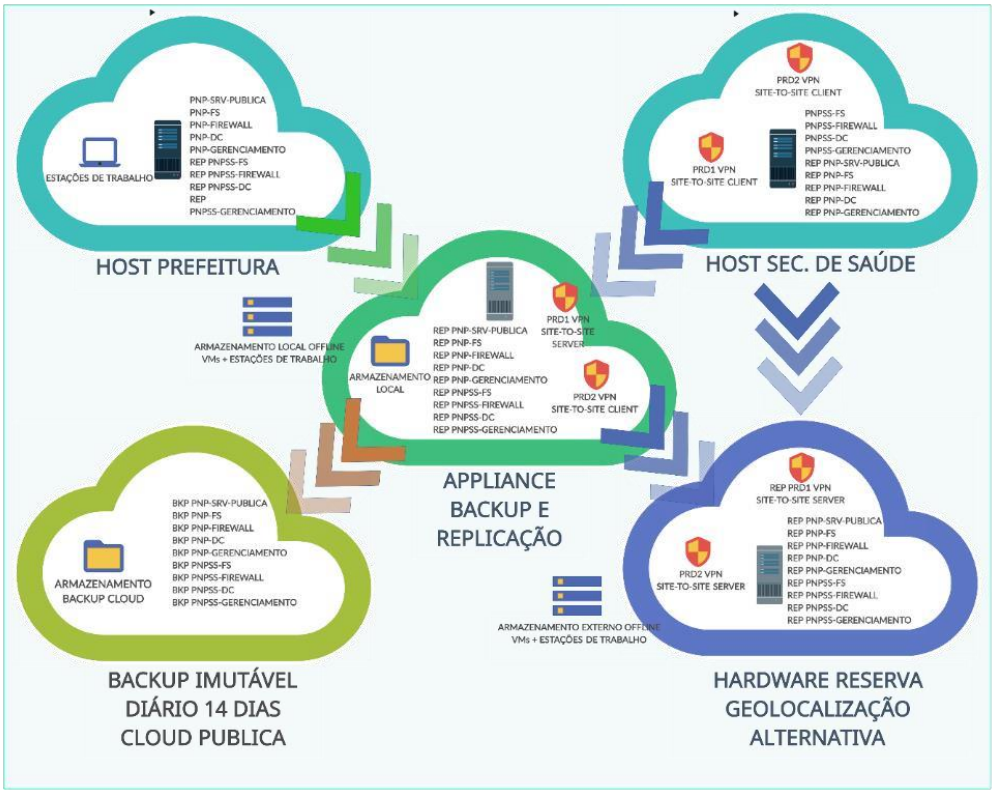


DIAGRAMA DE REDE DO PRD

5.2. HOSTS DE VIRTUALIZAÇÃO, SWITCHS, NOBREAKS E ACCESS POINTS

Para garantir a recuperação eficaz dos sistemas, a Diretoria de Informática definiu especificações técnicas rigorosas para hardware e software. As especificações, detalhadas na tabela abaixo, abrangem requisitos cruciais como: capacidade de armazenamento, poder de processamento e versões de software compatíveis.

5.2.1. ESPECIFICACÕES TÉCNICAS DE HARDWARE (HOSTS DE VIRTUALIZAÇÃO)

QUANTIDADE	DESCRIÇÃO	CONFIGURAÇÕES MÍNIMAS NECESSÁRIAS
02	Appliance (hospedagem de servidores virtuais da Prefeitura e host reserva) com as configurações mínimas, podendo ser superior em quantidade e/ou qualidade:	1,8Tb de armazenamento disponíveis em partição NTFS em Raid1 SSD ou NVME da linha Enterprise
		40 TB Armazenamento disponível em partição ReFS, em Raid5 ou superior com discos novos da linha Enterprise
		08 núcleos de CPU 2,0Ghz
		128 Gb de Memória RAM DDR4 2100Mhz
		04 adaptadores de rede gigabit
		01 adaptador PCI-E SFP+
		Fonte 500W reais, linha Silver
		Gabinete Rack 19”
02	Appliance (hospedagem de servidores virtuais da Secretaria de Saúde e host reserva) com as configurações mínimas, podendo ser superior em quantidade e/ou qualidade:	900Gb de armazenamento disponíveis em partição NTFS em Raid1 SSD ou NVME da linha Enterprise
		30 TB Armazenamento disponível em partição ReFS, em Raid5 ou superior com discos novos da linha Enterprise
		08 núcleos de CPU 2,0Ghz
		64 Gb de Memória RAM DDR4 2100Mhz
		01 adaptador PCI-E SFP+
		04 adaptadores de rede gigabit

		Fonte 500W reais, linha Silver
		Gabinete Rack 19”

5.2.2. ESPECIFICACÕES TÉCNICAS DE HARDWARE (SWITCHS)		
QUANTIDADE	**DESCRIÇÃO**	**CONFIGURAÇÕES MÍNIMAS NECESSÁRIAS**
		24 portas Gigabit
04	Switch de Rede	02 portas SFP+ 10Gbit
		Gerenciável Layer 2
04	Opção 1: Kit Transceptor Óptico 100 metros + Cordões de 2,5m + Conectores Ópticos + Adaptadores (se necessário) + Cabo de Fibra Óptica 50 metros Ou Opção 2: DAC Cable de 50 metros	Tecnologia SFP+ 10gigabit (O kit deve ter capacidade de iluminar 100 metros de fibra. Pode ser Monomodo ou Multimodo, desde que os 4 kits sejam idênticos).

6.3.4. ESPECIFICACÕES TÉCNICAS DE HARDWARE (NOBREAKs)		
QUANTIDADE	**DESCRIÇÃO**	**CONFIGURAÇÕES MÍNIMAS NECESSÁRIAS**
02	Nobreak (hospedagem de servidores virtuais da secretaria de saúde e host reserva) com as configurações mínimas:	Nobreak interativo senoidal
		Potência mínima da 1500Va
		Conexão para banco de bateria externo

		Tensão de entrada e saída: 220V~
02	Nobreak (servidor de backup e replicação do paço municipal) com as configurações mínimas:	Nobreak interativo senoidal
		Potência mínima da 6000Va
		Estabilizador interno integrado
		Tensão de entrada e saída: 220V~

6.3.5. ESPECIFICACÕES TÉCNICAS DE HARDWARE (ACCESS POINTs)		
QUANTIDADE	**DESCRIÇÃO**	**CONFIGURAÇÕES MÍNIMAS NECESSÁRIAS**
04	Access Point	Frequências de Operação: 2.4 GHz
		5 GHz
		Taxa mínima de transferência de Dados: 400 Mbps em 2,4Ghz 800 Mbps em 5Ghz
		Alimentação tipo: POE (Power over Ethernet)
		Interface de rede: Gibabit
		Ganho da antena: 3 dBi em 2.4 GHz 3 dBi em 5 GHz

6.4. CONFIGURAÇÃO DAS ROTINAS DE BACKUP E REPLICAÇÃO

A Diretoria de Informática e Transparência, após um estudo abrangente, definiu as rotinas de backup e recuperação como parte fundamental do Plano de Recuperação de Desastres (PRD). Estas rotinas abrangem diversos procedimentos essenciais para garantir a segurança e a disponibilidade da infraestrutura de TI. Entre os procedimentos definidos estão:

- **RPO (Recovery Point Objective)**: O ponto no tempo ao qual os dados devem ser recuperados após uma falha.
- **RTO (Recovery Time Objective)**: O tempo máximo aceitável para a recuperação dos dados e a retomada das operações.
- **Frequência**: A periodicidade com que os backups são realizados (diária, semanal, etc.).
- **Retenção**: O período pelo qual os backups são mantidos antes de serem descartados.
- **Tipo de Backup**: A metodologia utilizada, podendo ser completo, incremental ou diferencial.
- **Armazenamento**: O local onde os backups são armazenados, que pode ser local, em nuvem ou em um local remoto.
- **Localização dos Backups**: A distribuição geográfica dos backups para garantir redundância e segurança.
- **Periodicidade dos Testes de Restauração**: A frequência com que os testes de restauração são realizados para assegurar que os backups podem ser recuperados com sucesso.

Esses detalhes estão especificados de forma detalhada na tabela abaixo:

6.4.1. ROTINAS DE BACKUP (SERVIDORES VIRTUAIS)
FINALIDADE: **DETALHAMENTO TÉCNICO DAS ROTINAS E DO ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA (BACKUPS)**
OBJETIVO DO BACKUP: **CÓPIAS DE SEGURANÇA DE CURTA RETENÇÃO PARA FINS DE RECUPERAÇÃO DE DESASTRES**

ELEMENTOS PROTEGIDOS | *NOME DO JOB DE BACKUP*:

SERVIDORES VIRTUAIS (VMs) PAÇO MUNICIPAL:

- PNP - SRV-PUBLICA | *PNP - SRV-PUBLICA*
- PNP - FS | *PNP - FS*
- PNP - FIREWALL | *PNP - FIREWALl*
- PNP - DC | *PNP - DC*
- PNP - GERENCIAMENTO | *PNP - GERENCIAMENTO*

SERVIDORES VIRTUAIS (VMs) SECRETARIA DE SAÚDE:

- PNPSS - FS | *PNPSS - FS*
- PNPSS - FIREWALL | *PNPSS - FIREWALL*
- PNPSS - DC | *PNPSS - DC*
- PNPSS – GERENCIAMENTO | *PNPSS – GERENCIAMENTO*

GEOLOCALIZAÇÃO DOS ELEMENTOS PROTEGIDOS: **PAÇO MUNICIPAL E SECRETARIA DA SAÚDE**

TIPO DE BACKUP: **POINT-IN-TIME (CÓPIAS DE SEGURANÇA DE IMAGEM)** CAPTURAM O ESTADO DO ELEMENTO PROTEGIDO, INCLUINDO TODAS AS CONFIGURAÇÕES E DADOS

BACKUPS **LOCAIS**					BACKUPS **EXTERNOS**					
BACKUPS **LOCAIS ONLINE**			BKPs **LOCAIS OFFLINE**		BACKUPS **EXTERNOS ONLINE**				BKPs **EXTERNOS OFFLINE**	
IMPLEMENTAR: SIM	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** SIM	**IMPLEMENTAR:** SIM	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** NÃO	**IMPLEMENTAR:** SIM	**IMPLEMENTAR:** SIM
BACKUP LOCAL AUTOMÁTICO	CÓPIA DE BACKUP AUTOMÁTICO IMUTÁVEL	**REPLICAÇÃO AUTOMÁTICA DE VMS EM HOST/CLUSTER SECUNDÁRIO**	**BACKUP OFFLINE (FITAS LTO)**	HARDWARE RESERVA PREPARADO E A 10 MINUTOS	CÓPIA DE BACKUP EM CLOUD PÚBLICA IMUTÁVEL	CÓPIA DE BACKUP DE OBJETOS EM CLOUD PÚBLICA	CÓPIA DE BACKUP EM ARMAZENAMENTO IMUTÁVEL	REPLICAÇÃO INFRA VPS/CLOUD PREPARADA + VPN	**BACKUP OFFLINE (FITAS LTO)**	**HARDWARE RESERVA PREPARADO DO BACKUP TAPE OFFLINE / SEDE DO PRESTADOR**
FONTE DE DADOS: 16 VMs em 02 HOSTS	-	**FONTE DE DADOS:** 16 VMs em 02 HOSTS	**FONTE DE DADOS:** 16 VMs em 02 HOSTS	-	**FONTE DE DADOS:** 16 VMs em 02 HOSTS	-	-	-	**FONTE DE DADOS:** 16 VMs em 02 HOSTS	**FONTE DE DADOS:** 16 VMs em 02 HOSTS
VOLUME BRUTO DA FONTE DE DADOS: 08TB	-	**VOLUME BRUTO DA FONTE DE DADOS:** 08TB	**VOLUME BRUTO DA FONTE DE DADOS:** 08TB	-	**VOLUME BRUTO DA FONTE DE DADOS:** 08TB	-	-	-	**VOLUME BRUTO DA FONTE DE DADOS:** 08TB	**VOLUME BRUTO DA FONTE DE DADOS:** 08TB
CARACTERÍSTICAS DE ARMAZENAMENTO: 03 OU MAIS HDs NASWARE em RAID 5, Formatação ReFS	-	**CARACTERÍSTICAS DE ARMAZENAMENTO:** 03 OU MAIS HDs NASWARE em RAID 5, Formatação NTFS	**CARACTERÍSTICAS DE ARMAZENAMENTO:** 02 OU MAIS MÍDIAS REMOVIVEIS (HDs EXTERNOS), Formatação NTFS, ALTERNADOS DIARIAMENTE	-	**CARACTERÍSTICAS DE ARMAZENAMENTO:** IMUTABILIDADE ATIVADA	-	-	-	**CARACTERÍSTICAS DE ARMAZENAMENTO: MÍDIAS** ALTERNADAS DIARIAMENTE SEM INTERVENÇÃO HUMANA (BIBLIOTECA LTO)	**CARACTERÍSTICAS DE ARMAZENAMENTO:** : 03 OU MAIS HDs NASWARE em RAID 5, Formatação NTFS
GEOLOCALIZAÇÃO ARMAZENAMENTO: APPLIANCE NO CPD DA PREFEITURA	-	**GEOLOCALIZAÇÃO ARMAZENAMENTO:** APPLIANCE NO CPD DA PREFEITURA	**GEOLOCALIZAÇÃO ARMAZENAMENTO:** LOCALSEGURO NO PAÇO MUNICIPAL	-	**GEOLOCALIZAÇÃO ARMAZENAMENTO:** DATACENTER EM TERRITÓRIO NACIONAL	-	-	-	**GEOLOCALIZAÇÃO ARMAZENAMENTO:** SEDE OU DATACENTER DO PRESTADOR	**GEOLOCALIZAÇÃO ARMAZENAMENTO:** SEDE OU DATACENTER DO PRESTADOR
FERRAMENTA DE BACKUP: SOFTWARE PROFISSIONAL DE BACKUP	-	**FERRAMENTA DE BACKUP:** SOFTWARE PROFISSIONAL DE BACKUP	**FERRAMENTA DE BACKUP:** SOFTWARE PROFISSIONAL DE BACKUP	-	**FERRAMENTA DE BACKUP:** SOFTWARE PROFISSIONAL DE BACKUP	-	-	-	**FERRAMENTA DE BACKUP:** SOFTWARE PROFISSIONAL DE BACKUP	**FERRAMENTA DE BACKUP:** SOFTWARE PROFISSIONAL DE BACKUP
JOBS E MÉTODO: GRANULAR (UMA VM POR JOB), INCREMENTAL DIÁRIO + SYNTHETIC FULL SEMANAL AOS SÁBADOS	-	**JOBS E MÉTODO:** GRANULAR (UMA VM POR JOB), INCREMENTAL DIÁRIO + SYNTHETIC FULL SEMANAL AOS SÁBADOS	**JOBS E MÉTODO:** BACKUP DE IMAGEM DO SISTEMA OPERACIONAL DOS HOSTS DE VIRTUALIZAÇÃO COM A TOTALIDADE DOS VOLUMES ONDE AS VMs ESTÃO HOSPEDADAS	-	**JOBS E MÉTODO:** BACKUP DE IMAGEM DO SISTEMA OPERACIONAL DOS HOSTS DE VIRTUALIZAÇÃO COM A TOTALIDADE DOS VOLUMES ONDE AS VMs ESTÃO HOSPEDADAS	-	´-	-.	**JOBS E MÉTODO:** BACKUP DE IMAGEM DO SISTEMA OPERACIONAL DOS HOSTS DE VIRTUALIZAÇÃO COM A TOTALIDADE DOS VOLUMES ONDE AS VMs ESTÃO HOSPEDADAS	**JOBS E MÉTODO:** BACKUP DE IMAGEM DO SISTEMA OPERACIONAL DOS HOSTS DE VIRTUALIZAÇÃO COM A TOTALIDADE DOS VOLUMES ONDE AS VMs ESTÃO HOSPEDADAS
JANELA DE EXECUÇÃO DA ROTINA: DE 04 EM 04 HORAS, DE SEG-SEX À	-	**JANELA DE EXECUÇÃO DA ROTINA:** DE 04 EM 04 HORAS, DE SEG-SEX À	**JANELA DE EXECUÇÃO DA ROTINA:** DE 24 EM 24 HORAS, TROCAR AS MÍDIAS DIARIAMENTE	-	**JANELA DE EXECUÇÃO DA ROTINA:** DE 24 EM 24 HORAS, DE SEG-	-	-	-	**JANELA DE EXECUÇÃO DA ROTINA:** 24 HORAS,	**JANELA DE EXECUÇÃO DA ROTINA:** DE 60 EM 60 DIAS, NA PRIMEIRA
PARTIR DAS 12:00 ÀS 20:00		PARTIR DAS 12:00 ÀS 20:00	NO ÍNÍCIO DO EXPEDIENTE		DOMINGO, À PARTIR DAS 20:00				DE SEG-DOMINGO, À PARTIR DAS 22:00	SEMANA DE CADA MÊS
RPO DA ROTINA: 24 HORAS	-	**RPO DA ROTINA:** 24HORAS	**RPO DA ROTINA:** 24 HORAS	-	**RPO DA ROTINA:** 24 HORAS	-	-	-	**RPO DA ROTINA:** 24 HORAS	**RPO DA ROTINA: 60 DIAS**
RETENÇÃO DA ROTINA: ÚLTIMOS 30 DIAS (60 PONTOS)	-	**RETENÇÃO DA ROTINA:** 30PONTOS (01 POR DIA)	**RETENÇÃO DA ROTINA:** 14 PONTOS (01 POR DIA)		**RETENÇÃO DA ROTINA: 14** PONTOS (01 POR DIA)				**RETENÇÃO DA ROTINA:** 14 PONTOS (01 POR DIA)	**RETENÇÃO DA ROTINA:** 01 PONTOS DOS ÚLTIMOS 60 DIAS

RTO DA ROTINA: 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE	-	**RTO DA ROTINA:** 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE	**RTO DA ROTINA:** 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE	-	**RTO DA ROTINA:** 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE	-	-	-	**RTO DA ROTINA:** 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE	**RTO DA ROTINA:** 24 HORAS DA DECLARAÇÃO E COMUNICAÇÃO DO EVENTO DE DESASTRE
DECLARAÇÃO DE DESASTRE: COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS	-	**DECLARAÇÃO DE DESASTRE:** COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS E A TENTATIVA DE RESTAURAÇÃO PELAS ROTINAS DE BACKUP À ESQUERA FALHARAM	**DECLARAÇÃO DE DESASTRE:** COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS E A TENTATIVA DE RESTAURAÇÃO PELAS ROTINAS DE BACKUP À ESQUERA FALHARAM	-	**DECLARAÇÃO DE DESASTRE:** COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS E A TENTATIVA DE RESTAURAÇÃO PELAS ROTINAS DE BACKUP À ESQUERA FALHARAM	-	-	-	**DECLARAÇÃO DE DESASTRE:** COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS E A TENTATIVA DE RESTAURAÇÃO PELAS ROTINAS DE BACKUP À ESQUERA FALHARAM	**DECLARAÇÃO DE DESASTRE:** COMPROMETIMENTO PARCIAL OU TOTAL DOS PILARES DA SEG. DA INFRMAÇÃO NOS ELEMENTOS PROTEGIDOS E A TENTATIVA DE RESTAURAÇÃO PELAS ROTINAS DE BACKUP À ESQUERA FALHARAM
AÇÃO DE RECUPERAÇÃO: CONETAR NA CONSOLE DO SOTWARE DE BACKUP E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS.	-	**AÇÃO DE RECUPERAÇÃO:** CONETAR NA CONSOLE DO SOTWARE DE BACKUP E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS (FAILOVER PLAN).	**AÇÃO DE RECUPERAÇÃO:** CONETAR NA CONSOLE DO SOTWARE DE BACKUP E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS (FAILOVER PLAN).	-	**AÇÃO DE RECUPERAÇÃO:** CONETAR NA CONSOLE CLOUD E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS (FAILOVER PLAN).	-	-	-	**AÇÃO DE RECUPERAÇÃO:** CONETAR NA CONSOLE DO SOTWARE DE BACKUP E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS (FAILOVER PLAN	**AÇÃO DE RECUPERAÇÃO:** CONETAR NA CONSOLE DO SOTWARE DE BACKUP E EXECUTAR A RESTAURAÇÃO DOS ELEMENTOS AFETADOS (FAILOVER PLAN). APÓS, LEVAR O HARDWARE ATÉ A SEDE DA PREFEITURA,
TESTE E HOMOLOGAÇÃO PERIÓDICO: TRIMESTRAL FAZER A RESTAURAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.	-	**TESTE E HOMOLOGAÇÃO PERIÓDICO:** TRIMESTRAL FAZER A RESTAURAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.	**TESTE E HOMOLOGAÇÃO PERIÓDICO:** TRIMESTRAL FAZER A RESTAURAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.	-	**TESTE E HOMOLOGAÇÃO PERIÓDICO:** TRIMESTRAL FAZER A RESTAURAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.	-	-	-	**TESTE E HOMOLOGAÇÃO PERIÓDICO:** TRIMESTRAL). FAZER A RESTAURAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.	**TESTE E HOMOLOGAÇÃO PERIÓDICO:** SEMESTRAL FAZER A LIGAÇÃO EM AMBIENTE DE TESTE (ISOLADO) E SOLICITAR QUE CADA LÍDER DE SETOR NAVEGUE PELOS DADOS E SISTEMAS A FIM DE HOMOLOGAR OS ÚLTIMOS LANÇAMENTOS. MEDIR POR E RTO PARA AVALIAR POSSÍVEIS MELHORIAS OU ADEQUAÇÕES.

6.4.2. OBJETIVOS DE RPO E RTO DE CADA ITEM PROTEGIDO			
LOCAL	**ITEM**	**RPO**	**RTO**
Paço municipal	Host Hyper-V	48 horas	48 horas
	VMs (Servidores Virtuais)	48 horas	48 horas
Secretaria de Saúde	Host Hyper-V	48 horas	48 horas
	VMs (Servidores Virtuais)	48 horas	48 horas

6.5. OPERACIONALIZAÇÃO DO PLANO DE RECUPERAÇÃO E SUPORTE TÉCNICO

A operacionalização eficaz do plano de recuperação e suporte técnico é crucial para garantir a continuidade dos negócios e minimizar o impacto de possíveis interrupções. Este processo envolve a implementação meticulosa de procedimentos predefinidos, treinamento contínuo da equipe e a realização de testes regulares para validar a eficácia do plano. O calendário de atividades deve ser estruturado de forma a

alinhar-se com a tabela de rotinas previamente estabelecida, garantindo que todas as tarefas críticas sejam executadas nos intervalos apropriados. Para isso, é necessário utilizar a matriz e os prazos estipulados na tabela de rotinas acima.

O acompanhamento dos relatórios de sucesso das rotinas deve ser diário e o suporte técnico nunca deve demorar mais do que o os limites do RPO e RTO estabelecidos para reestabelecer os servidores de geração e guarda das cópias de segurança, bem como a própria restauração quando necessário.

O serviço ainda deve incluir suporte técnico integral à infraestrutura de TI legada, cuidando do funcionamento através de manutenções preventivas e corretivas, bem como o atendimento de chamados técnicos remotos e presenciais pelos usuários de TI da prefeitura e secretaria de saúde.

Os equipamentos e componentes relativos a TI que não estão descritos neste plano serão de responsabilidade de fornecimento da prefeitura. O prestador será responsável pelo serviço de instalação, configuração e ajustes para pleno funcionamento.

Todos os custos do prestador de serviços devem estar inclusos no valor das propostas, não sendo possível cobranças avulsas.

7. CRITÉRIOS DE SELEÇÃO DE FORNECEDORES PARA SOLUÇÕES DE BACKUP CORPORATIVO

Conforme constatado pela Diretoria de Informática e Transparência, para atender às necessidades do Plano de Recuperação de Desastres (PRD), é essencial que as empresas fornecedoras sejam revendedoras autorizadas dos softwares de backup corporativo mencionados no Quadrante Mágico da Gartner nos últimos dois anos. Este critério assegura que o fornecedor não apenas disponibilize uma solução de backup de ponta, mas também possua uma equipe técnica altamente especializada, capaz de realizar a instalação, configuração, manutenção, suporte e atendimento de chamados de forma eficiente para a solução de backup escolhida.

Além disso, ao definir os critérios de seleção para fornecedores de soluções de backup corporativo, a Diretoria de Informática e Transparência considerou uma série de fatores estratégicos e operacionais. Abaixo, detalhamos as principais justificativas que fundamentam a escolha desses critérios:

7.1. Revendedores Autorizados no Quadrante Mágico da Gartner:

- Qualidade e Inovação: Os fornecedores mencionados no Quadrante Mágico da Gartner são reconhecidos por sua excelência em inovação e execução. Isso garante que a solução de backup adotada seja de alta qualidade e esteja alinhada com as melhores práticas do mercado.
- Suporte Técnico Especializado: Empresas autorizadas possuem acesso direto ao suporte técnico do fabricante, garantindo que qualquer problema possa ser resolvido de maneira rápida e eficiente.

7.2. Documentação Comprobatória de Vínculo com o Fabricante:

- Autenticidade e Confiança: A exigência de contratos, atestados ou declarações emitidas pelo fabricante assegura que a empresa fornecedora tem um relacionamento legítimo e reconhecido com o fabricante do software de backup. Isso aumenta a confiança na capacidade da empresa de fornecer suporte adequado e atualizado.

7.3. Profissionais Certificados pelo Fabricante:

- Competência Técnica: Ter no quadro de funcionários, terceiros ou prepostos, pelo menos um profissional certificado pelo fabricante do software de backup, garante que a equipe possui o conhecimento técnico necessário para implementar e gerenciar a solução de backup de maneira eficaz.
- Atualização Constante: Profissionais certificados são obrigados a manter suas certificações atualizadas, o que assegura que estão sempre a par das últimas atualizações e melhores práticas.

7.4. Data Center Localizado em Território Nacional:

- Conformidade Legal e Regulatória: A localização do data center em território nacional garante a conformidade com as leis e regulamentações locais de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD).
- Desempenho e Latência: Data centers locais oferecem melhor desempenho e menor latência no acesso aos dados, o que é crucial para operações críticas.

7.5. Experiência Anterior Comprovada:

- Capacidade Técnica e Operacional: A exigência de atestados de capacidade técnica, notas fiscais ou contratos anteriores demonstra que a empresa possui experiência prática na prestação de serviços semelhantes. Isso reduz o risco de falhas e garante que a empresa está apta a lidar com as complexidades do projeto.
- Histórico de Sucesso: A comprovação de experiência anterior com escopo semelhante é um indicativo de que a empresa tem um histórico de sucesso e pode ser confiável para entregar os resultados esperados.

A adoção desses critérios rigorosos para a seleção de fornecedores não é apenas uma medida de precaução, mas uma estratégia para garantir que a solução de backup escolhida seja robusta, confiável e capaz de atender às necessidades específicas do PRD. Ao assegurar que os fornecedores sejam revendedores autorizados, possuam profissionais certificados, tenham data centers localizados no país e experiência comprovada, a prefeitura está investindo em uma solução de backup que oferece segurança, eficiência e conformidade regulatória.

8. CONCLUSÃO

8.1. Conclusão Técnica

A adoção de uma estratégia de backup e recuperação de desastres diversificada e abrangente, conforme proposto neste ETP, é essencial para garantir a continuidade dos sistemas de TI da prefeitura. A combinação de replicações e backups locais para reestabelecimento rápido, backups externos online e offline, e hardware de reserva em uma localização segura, proporciona uma base sólida para assegurar a continuidade dos serviços públicos essenciais, mesmo em situações de desastres. Além disso, a solução proposta atende integralmente aos requisitos de conformidade e se destaca pelo excelente custo-benefício, permitindo uma gestão eficiente dos recursos públicos.

Pinheiro Preto/SC, 04 de Dezembro de 2024.

MATHEUS HENRIQUE FRIEBEL

DIRETOR DE INFORMÁTICA E TRANSPARÊNCIA