LOTE 1 – SOFTWARE DE BACKUP – QUANTIDADE 01
1. A solução deve incluir recursos de backup e replicação integrados em uma única solução; incluindo replicação e reversão da replicação de e para a infraestrutura virtualizada. 2. A solução não deve precisar da instalação de agentes para realizar suas tarefas de backup, recuperação e replicação de máquinas virtuais. 3. A solução não deve precisar de agentes para a recuperação granular de aplicações e arquivos dos sistemas suportados. 4. Deverá ser capaz de executar backups sem interromper o funcionamento das máquinas virtuais e sem gerar uma diminuição no desempenho, facilitando as tarefas de backup e as migrações como um todo. 5. Deve ser capaz de entender as máquinas virtuais como objetos no ambiente virtual e suportar as configurações desses, independentemente dos dados das máquinas. 6. Deverá ser capaz de suportar uma máquina virtual inteira ou discos virtuais específicos de uma máquina virtual sem distinção. 7. Deverá fornecer uma ferramenta de gerenciamento de arquivos para administradores de máquinas virtuais no console do operador. 8. Deverá ser uma solução altamente eficiente e preparada para o futuro, integrando-se extensivamente, com as APIs dos fabricantes de infraestrutura virtualizada, para proteção de dados. 9. Deverá ser capaz de fazer backups incrementais ultra-rápidos, aproveitando a tecnologia de rastreamento de blocos de disco modificados (changed block tracking - CBT) minimizando o tempo de backup e permitindo que uma cópia de segurança (backup) e replicação sejam realizados de maneira mais frequente. Desta forma, atingindo o que é estabelecido em relação à perda de desempenho. 10. A solução deverá oferecer várias estratégias e opções de transporte de dados para tarefas de backup, a saber: • Diretamente através da Rede de Área de Armazenamento (SAN). • Diretamente do armazenamento por meio do Hypervisor I/O (Virtual Appliance). • Através do uso da rede local (LAN). • Diretamente do repositório NFS (Datastore NFS) 11. Deverá fornecer um controle centralizado da implantação distribuída, para isso deverá incluir um console Web que forneça uma visão consolidada de sua implantação distribuída e federação de vários servidores de backup, relatórios centralizados, alertas consolidados e restauração de autoatendimento de máquina virtual e no nível de sistema de arquivos (granular). 12. Deverá ser capaz de manter um backup completo sintético (sythetic full), eliminando assim a necessidade de realizar backup completo periódico (active full), pois fornecerá um backup incremental permanente (incremental forever), permitindo economizar tempo e espaço de armazenamento. 13. Deverá ter tecnologia de desduplicação para obter uma economia de espaço de armazenamento para backups.

14. Deverá fornecer proteção de dados quase contínua (near CDP), permitido a redução ao mínimo dos pontos de objetivo de recuperação (RPO).
15. Deverá fornecer uma estratégia de recuperação rápida, que permita aos usuários prover/restabelecer o serviço quase imediatamente e de maneira simples. Esta estratégia deve consistir em iniciar e ligar a máquina virtual, que falhou, diretamente do arquivo de backup no armazenamento usual do backup.
16. A recuperação instantânea das máquinas virtuais deve permitir mais de uma máquina virtual e/ou ponto de restauração simultâneo para a disponibilidade do ponto de recuperação funcional, permitindo ter vários pontos no tempo de uma ou mais máquinas virtuais em execução.
17. Após uma recuperação rápida, deve ser possível realizar uma restauração total sem interrupções de serviço. A ferramenta deve garantir que o trabalho feito pelos usuários não seja afetado ao migrar suas máquinas virtuais do repositório de backup para o armazenamento de produção, sem impor uma restrição de tempo na execução da máquina durante o processo de recuperação instantânea.
18. A capacidade de executar backup completo (backup) de qualquer máquina virtual deve ser fornecida dentro de uma janela de manutenção mínima, permitindo processos de recuperação completos em interrupções de serviço mais curtas e menos frequentes. A estratégia deve ser replicar ou copiar a quente o backup (backup) da máquina virtual que está em um armazenamento desduplicado para o armazenamento em produção onde a máquina virtual é executada. Além disso, deve poder transferir deste estado de recuperação através de mais de um método tecnológico.
19. Deverá ter uma opção de recuperação instantânea de arquivos que estão dentro dos backups e réplicas das máquinas virtuais. O que deve permitir o acesso ao conteúdo dos discos virtuais dessas máquinas, sem a necessidade de recuperar o backup completo e reiniciar a máquina virtual a partir dele.
20. Deverá incluir um assistente de recuperação instantânea em nível de arquivo nos sistemas de arquivos mais utilizados do Windows – FAT, FAT32, NTFS, ReFS. Linux – ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs. Solaris – UFS e ZFS (exceto qualquer versão pool do Oracle Solaris). BSD – UFS e UFS2. MacOS – HFS e HFS+.
21. Deverá ser capaz de criar um índice (catálogo) de todos os arquivos gerenciados pelos sistemas operacionais Windows ou Linux, sem um agente, quando este for o sistema operacional executado dentro de uma máquina virtual cujo backup foi feito.
22. Deverá ser capaz de realizar pesquisas rápidas através de índices de arquivos que são manipulados por um sistema operacional Windows ou Linux, quando este for o sistema operacional executado dentro de uma máquina virtual cujo backup foi feito.
23. Deverá garantir a consistência das aplicações transacionais automaticamente por meio da integração com o Microsoft VSS, nos sistemas operacionais Windows.
24. Deverá ser capaz de realizar backup e truncamento de logs transacionais (logs de transação) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle sem utilização de agentes.
25. Deverá ser capaz de enviar notificações por correio eletrônico (e-mail), SNMP ou através dos atributos da máquina virtual do resultado da execução de suas tarefas.

26. Deverá ser capaz de recuperar no nível de objetos de qualquer aplicação virtualizada , em qualquer sistema operacional, usando as ferramentas de gerenciamento de aplicações existentes .
27. Deverá incluir ferramentas de recuperação fácil e assistida, através das quais os administradores de servidores de correio como o Microsoft Exchange, nas versões 2010 (SP1, SP2, SP3), 2013, 2016 e 2019, possam comparar os backups realizados com a produção e recuperar objetos individuais, como e-mails e contatos, sem precisar recuperar os arquivos da máquina virtual como um todo e reiniciá-la. Sem exigir uma infraestrutura intermediária ("staging").
28. Deverá incluir ferramentas de recuperação fácil e assistida, através das quais os administradores de servidores de serviços de diretório, como o Microsoft Active Directory a partir de sua versão 2008-R2 e superiores, possam comparar os backups realizados com a produção e recuperar objetos individuais, como usuários, grupos, diretivas de grupo (GPOs), registros DNS, partições de configuração, além de outros objetos do AD . Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciá-la.
29. Deverá incluir ferramentas de recuperação fáceis, por meio das quais os administradores dos servidores de banco de dados do Microsoft SQL Server a partir de sua versão 2005 SP4 e superiores, possam recuperar objetos individuais, como tabelas e registros. Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciar a mesma. Também deverá ser possível a publicação das bases protegidas para servidores SQL de destino, respeitando a versão dos backups.
30. Deve incluir ferramentas de recuperação fáceis, através das quais os administradores dos servidores de banco de dados Oracle possam recuperar os banco de dados . Não havendo a necessidade de recuperar os arquivos da máquina virtual como um todo e reiniciar a mesma.
31. Deverá oferecer visibilidade instantânea, recursos avançados de pesquisa e recuperação rápida de itens individuais para o Sharepoint 2010 , 2013 , 2016 e 2019, sem o uso de agentes.
32. Deverá ser capaz de oferecer 100% de confiabilidade na inicialização correta de todas as suas máquinas virtuais protegidas e no funcionamento do serviço/função dessas máquinas virtuais (servidor DNS, controlador de domínio , servidor de correio, servidor SQL, Oracle , etc.) no momento da recuperação, sendo capaz de realizar testes de recuperabilidade automaticamente a partir das máquinas copiadas.
33. Deverá ser capaz de criar uma cópia de trabalho do ambiente de produção de qualquer estado anterior para solução de problemas, teste de procedimentos, treinamento etc; executando uma ou várias máquinas virtuais a partir do arquivo de backup em um ambiente isolado, sem a necessidade de mais espaço de armazenamento e sem modificar o backup.
34. A solução deve permitir a migração de máquinas virtuais entre clusters e datacenters do VMware vSphere.
35. A solução deve monitorar o espaço livre das LUNs e, se não houver espaço, não deverá executar o snapshot no ambiente virtual.
37. Deverá oferecer arquivamento em fita, suporte a VTL (Virtual Tape Libraries), biblioteca de fitas e unidades independentes.
38. Deverá oferecer trabalhos de cópia de segurança com a implementação de políticas de retenção; com o objetivo de manter uma cópia ou réplica dos arquivos de backup em caso de desastre .

39. Deve incluir suporte para VMware vCloud Diretor com visibilidade integrada da infraestrutura de vCD no console de backup, tornando o backup e os atributos de metadados associados a vApps e VMs, permitindo a recuperação diretamente para o vCD.
40. Deverá incluir um VMware Plug-in para o vSphere Web Client e monitorar a infraestrutura de backup diretamente do vSphere Web Client, com exibições detalhadas e gerais do status das tarefas e dos recursos de backup.
41. A solução deve ter um mecanismo de recuperação de emergência dos backups criptografados em caso de perda da senha, podendo ser recuperada com uma senha mestra gerada através do portal web.
42. A solução deve ter um mecanismo de pesquisa de arquivos global entre os backups.
43. Deverá oferecer suporte às últimas versões disponíveis dos hipervisores mais populares no mercado: VMWare vSphere e Microsoft Hyper-V em todas as versões compatíveis com o respectivo fabricante.
44. Não deve exigir hardware específico para obter a desduplicação e a compactação de informações fora dos requisitos padrão de qualquer software (appliance desduplicadora).
45. Não deve exigir licenças independentes para atividades de backup, recuperação e replicação.
46. Não deverá exigir licenças separadas de software para backup e recuperação granular assistida e consistente das seguintes aplicações:
a. Microsoft Active Directory 2008 R2 em diante
b. Microsoft Exchange Server 2010 SP1 em diante
c. Microsoft SQL Server 2005 SP4 em diane
d. Oracle Database 11.x e superior para Windows / Linux
e. Microsoft Sharepoint 2010 em diante
47. Deve permitir a recuperação granular sem a necessidade de configurar ambientes temporários para:
a. Microsoft Active Directory 2008 R2 e superiores
b. Microsoft Exchange Server 2010 SP1 em diante
c. Microsoft SQL Server 2005 SP4 em diante
d. Oracle Database 11.x e superior para Windows / Linux
e. Microsoft Sharepoint 2010 e superiores.
48. Deve ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups previamente realizados.
49. Deve apresentar um método de recuperação fácil para ambientes de contingência, com ações pré-configuradas para evitar ações manuais em caso de desastre, semelhante a um botão de emergência.
50. Deverá oferecer a possibilidade de armazenar backups de forma criptografada , bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.
51. Deverá ter recursos internos que permitam selecionar um destino de armazenamento de backup que possa ser hospedado por um provedor de serviços em nuvem (BaaS).
52. Deverá ter funcionalidades integradas que permitam a seleção de um destino de replicação

que possa ser hospedado em um provedor de serviços em nuvem (DRaaS).

53. Deverá ter a funcionalidade para gerar armazenamento de backup global, que pode incluir vários e diferentes tipos de armazenamento, e direcionar tarefas de backup para ele como se fosse um, permitindo também crescimento em escala dos mesmos, sem impacto sobre o meio ambiente de backup já configurado.

54. Integração com hardware de desduplicação EMC Data Domain , HP StoreOnce , Quantum DXi e ExaGrid, além de otimizações para o uso de qualquer sistema de armazenamento desduplicado.

55. Integração com plataformas de desduplicação na origem – EMC DataDomain Boost e HP StoreOnce Catalyst e Quantum Accent.

56. Deverá possuir um número de produto exclusivo, de acordo com a versão ou edição, fornecido pelo fabricante para a aquisição do pacote de software que inclui todas as funcionalidades mencionadas acima.

57. Capacidade de definir grupos de fitas magnéticas para serem utilizadas em uma única sessão de armazenamento em fita (Media Pool) para maximizar o desempenho e a velocidade de transferência.

58. A solução deve suportar e armazenar os arquivos de fita desduplicados, obtendo maior eficiência do espaço da fita.

59. Deverá ter a capacidade de processar o envio de dados em várias unidades de fita, em paralelo para maximizar a largura de banda e minimizar o tempo de transferência.

60. Deverá ter a capacidade de desvincular a função do servidor da infraestrutura da solução que permite acesso a unidades de fita, evitando a necessidade de essa função se sobrepor a outras funções na solução.

61. Ter a capacidade de leitura direta do sistema de armazenamento central, quando em um ambiente de infraestrutura VMWare, apresentado através do protocolo NFS, evitando assim o tráfego de informações através das interfaces de controle do hipervisor.

62. Ser capaz de diferenciar, nas máquinas virtuais com sistema operacional MS Windows, os blocos de disco que contêm dados irrelevantes (blocos sujos) e evitar sua transferência para os backups, bem como a exclusão arbitrária de arquivos nas máquinas virtuais com sistema operacional MS Windows instalado no sistema de arquivos NTFS.

63. A solução deve fornecer mecanismos de proteção para evitar sobrecarga nos sistemas de armazenamento da plataforma virtual, através de monitoramento pró-ativo da latência dos datastores, permitindo a auto-regulação do sistema de backups e da função de replicação, em função dos limites definidos.

64. Capacidade de migrar máquinas virtuais entre hipervisores que não estão conectados entre si pelo mesmo cluster ou controlador de gerenciamento de ambiente virtual (vCenter ou SCVMM).

65. Capacidade de aproveitar o subsistema de rastreio de blocos alterados (CBT) do ambiente virtual, também para operações de retorno (failback), acelerando a transferência de dados para o datacenter produtivo.

66. Suporte para backups nativos (integrados) no VMWare Cloud na AWS.

67. Integração com armazenamento de objetos como o Amazon S3, Azure Blob Storage, IBM Cloud Object Storage, bem como com provedores de serviços compatíveis com o protocolo S3 e

armazenamento local compatível com o protocolo S3.

68. Executar o arquivamento de backups mais antigos no armazenamento de objetos, conforme descritos no item 79.

69. Eficiência no uso da largura de banda quando integrada ao armazenamento em nuvem pública (item 79), permitindo a recuperação granular de dados, a partir dos blocos do arquivo de backup, economizando significativamente o custo da operação em largura de banda.

70. Quando integrado ao armazenamento em nuvem pública (item 79), ele deve ser autossuficiente e não depender de qualquer catálogo externo, permitindo, em caso de desastre, a recuperação completa dos arquivos armazenados na nuvem pública.

71. A solução deve permitir recuperações futuras a qualquer momento sem exigir uma licença paga. Ou seja, você pode usar a versão gratuita do produto para esses fins.

72. A solução deve permitir a conformidade com padrões como o GDPR para dados ou registrar exclusões de maneira automatizada usando scripts (feitos pelo cliente) nos arquivos de backup antes de restaurar uma máquina virtual no ambiente produtivo. Além disso, deverá permitir que os administradores façam alterações no sistema operacional, instalação ou remoção de aplicações para estar em conformidade com diretriz corporativa ao restaurar uma máquina virtual.

73. A solução deve ser integrada com diferentes antivírus para realizar análises de infecção nos backups existentes na plataforma, por exemplo, backups anteriores da mesma solução, análise antes de fazer uma recuperação instantânea ou completa da máquina virtual. Além de estar integrado no mecanismo de teste automatizado das máquinas virtuais e/ou conteúdo da máquina virtual, para realizar proativamente a análise prévia.

74. A solução deve identificar e excluir automaticamente as máquinas virtuais que possuem o recurso "Multi-Writer" habilitado.

75. Deverá prover suporte para plataformas de servidor Microsoft Windows Server 2019.

76. A solução deve permitir a publicação de bancos de dados de servidores SQL suportados pela plataforma em um formato granular diretamente para uma instância e/ou servidor disponível, respeitando as versões backup/servidor.

77. Capacidade de recuperação de VMs e Backups de máquinas físicas com agentes da plataforma (realizando a conversão automática de UEFI para BIOS na AWS) de forma direta para Amazon ou Azure .

78. A solução deve permitir alterar os tipos de discos (Thin para Thick, por exemplo) quando for necessário replicar máquinas virtuais.

79. A solução também deve permitir a recuperação apenas dos blocos de disco da máquina virtual que foram alterados usando o CBT.

80. A solução deverá integrar uma solução unificada de monitoramento e geração de relatórios de ambientes virtuais e backups para poder correlacionar infraestruturas, alarmes e relatórios.

81. Deverá oferecer um conjunto de relatórios capazes de apresentar informações do tipo:

a. Relatórios que permitam planejamento de capacidade.

b. Relatórios que permitam a determinação da ineficácia no uso de recursos.

c. Relatórios que facilitem a visibilidade de tendências negativas e anomalias.

d. Painéis de controle claros, apresentáveis e integráveis em sites.

e. Envio automático e programado de relatórios de auditoria para operações de recuperação

e modificações em políticas de backup ou replicação.

82. Deve ter a capacidade de gerar segregação de acesso de acordo com o perfil do usuário, para monitorar a infraestrutura conectada à plataforma.

83. Deverá correlacionar a execução de tarefas de backup e replicação com os objetos no ambiente virtual.

84. Deverá oferecer a capacidade de relatar a conformidade com as políticas de proteção e disponibilidade de dados de acordo com os parâmetros definidos.

85. Deverá ter uma base de conhecimento integrada nos alarmes, embora também deva apoiar a personalização dos alarmes e descrições da base de conhecimento.

86. A plataforma deverá fornecer um mecanismo de diagnóstico inteligente que analise os logs da solução para identificar proativamente e alertar sobre problemas de infraestrutura.

87. A plataforma deve conter relatórios inteligentes para verificar se a infraestrutura virtual está pronta para executar backups e de acordo com boas práticas. Deve conter recomendações para a correção de um problema encontrado.

88. A plataforma deve conter relatórios inteligentes para a revisão após a implementação da solução de backup, para validar se ela está em conformidade com as boas práticas de implementação e configuração.

89. A solução também deve permitir ações de correção para automatizar processos manuais rotineiros associados à solução de problemas comuns de infraestrutura virtual e de backup, como a eliminação de um snapshot de máquinas virtuais.

90. A plataforma deve fornecer monitoramento das aplicações, isto é, conhecer o status de integridade dos serviços e aplicações encontradas nas máquinas virtuais da plataforma.

91. Deverá possibilitar o envio de notificações de alarme quando um processo de recuperação for iniciado.

92. Deverá enviar uma notificação de alarme quando forem detectados erros de configuração ou potenciais problemas na infraestrutura de apoio.

93. Deverá possuir suporte para relatórios de backup de agentes físicos da solução.

94. A plataforma deverá conter relatórios genéricos, tais como:

a. Histórico das tarefas de backup
b. Relatórios de máquinas protegidas, físicas e virtuais
c. Relatório de atividade de recuperação de dados
d. Relatório de verificação de recuperabilidade
e. Último status das tarefas de backup
f. Resumo dos alarmes de backup
g. Relatório de configuração da infraestrutura virtual
h. Relatório de backup em fitas
i. Relatório de máquinas em conformidade
j. Inventário de backup

95. Além disso, deve conter relatórios avançados, como:

a. Auditoria de alterações de objeto da infraestrutura virtual
b. Auditoria de alterações da infraestrutura de backup

c. Modelagem em caso de falhas
d. Capacidade planejamento da infraestrutura virtual
e. Relatórios para otimização de infraestrutura virtual
f. Crescimento de Máquinas
g. Capacidade planejamento de infraestrutura de backup
h. Avaliação de desempenho do armazenamento de dados
i. Avaliação de configuração de máquinas virtuais
j. Estimativa da taxa de alteração de máquinas virtuais

96. A plataforma deverá permitir visualizar dashboards da plataforma virtual e de backup, além de prover um mapa de calor (heatmap) dos recursos utilizados pela infraestrutura de backup , a fim de permitir a análise de consumo dos recursos envolvidos.

Agentes

94. Deverá permitir a integração de agentes para ambientes de nuvem ou ambientes físicos de plataformas Windows ou Linux, para consolidar a visualização da execução de tarefas de backup a partir do console centralizado.
95. Instalação, configuração e gerenciamento de agentes de backup para computadores físicos Linux ou Windows de forma centralizada.
96. Instalação remota de agentes, sem a necessidade de entrada interativa no equipamento a ser instalado.

Agente Linux

97. Deverá permitir a proteção de dados em ambientes físicos ou de nuvem com base no sistema operacional Linux. Deverá ter a capacidade de executar backup, no mínimo, para as seguintes plataformas de 32 e 64 bits:
a. Debian 6 - 9.4
b. Ubuntu 10.04 - 18.04
c. CentOS / RHEL 6,0 - 7,6
d. Oracle Linux 6 (do UEK R1) - Oracle Linux (da UEK R 4 U7)
e. Oracle 6 - 7.6 (RHCK)
f. Fedora 23 - 29, 42.0 - 42.1, Tumbleweed
g. openSUSE 11.3 - 13.2
h. openSUSE Leap 42.2 - 42.3, Leap 15
i. SLES 11 SP4 - 15 (SP0)
j. SLES para SAP 11 SP4 - 15 (SP0)

98. Deverá permitir os seguintes tipos de backup:
a. Computador / Servidor completo
b. No nível de volume específico (volumes únicos ou LVM)

c. No nível de arquivos ou pastas.

99. Deve permitir a execução de scripts antes do início do trabalho de backup e após a conclusão do trabalho.

100. Deverá permitir a execução de scripts antes da geração do snapshot correspondente ao trabalho de backup e subsequente à geração do snapshot.

101. Deve permitir backup sem snapshot do sistema operacional, a fim de fazer backup de arquivos de qualquer sistema de arquivos montado no servidor

102. Deve permitir a criação de um índice de arquivos e pastas durante o backup, permitindo a busca de arquivos na imagem de backup.

103. Deverá oferecer os seguintes tipos de repositórios de backup:

i. Discos locais

ii. DAS (" Direct Attached Storage")

iii. NAS ("Network Attached Storage")

iv. Repositórios manipulados pelo Servidor de Backup Centralizado.

v. Repositórios de provedores de serviços em nuvem.

104. Deverá oferecer suporte para backup e recuperação dos seguintes tipos de sistema de arquivos : Btrfs (para sistemas operacionais que usam o kernel 3.16 ou superior), Ext 2/3/4, F2FS, FAT16, FAT32, HFS, HFS +, HFSP, JFS, NILFS2, NTFS, ReiserFS , XFS.

105. Deverá permitir a programação de tarefas de backup por meio de um único console, incluindo:

i. Permitir a execução de processos de backup de acordo com as políticas a serem definidas (frequência, retenção, tipo de backup completo ou incremental)

ii. Permitir definir a periodicidade dos trabalhos

iii. Permitir programar os trabalhos para execução de forma automatizada.

106. Deverá fornecer console de monitoramento via interface gráfica com visibilidade da execução do trabalho em tempo real.

107. Deverá fornecer arquivos de log para a verificação / análise dos trabalhos.

108. Deverá ter o gerenciamento centralizado de tarefas de backup e recuperação por meio de interface gráfica (GUI) e linha de comando (CLI).

109. Deverá permitir recuperações em nível de volume para seu local original ou para um novo local

110. Deve permitir recuperações no nível de arquivos ou pastas.

111. Deverá permitir uma recuperação completa de desastres do backup para o mesmo hardware ou similar, também chamado de "Restauração bare-metal".

112. Deve permitir a criação de uma Imagem de Recuperação, tanto para a recuperação de dados do backup, quanto para a execução de ferramentas do Linux para diagnóstico de problemas e correção de erros.

113. Deverá permitir a replicação dos backups do Repositório Primário para o Repositório Secundário.

114. Deverá permitir o arquivamento de backup em dispositivos de fita autônomos, bibliotecas

virtuais ou bibliotecas Física , LTO3 ou superior através do console centralizado

115. Deve oferecer a possibilidade de converter discos dos formatos suportados em discos virtuais VMDK, VHD ou VHDX.

116. Deverá ter a capacidade de criptografar backups, utilizando os algoritmos mais comuns no mercado, suportando o uso de chaves de pelo menos 256 bits.

117. Deve permitir a possibilidade de executar o criptografia no processamento de dados, no tráfego via rede ou no repositório de backup.

118. Deve oferecer recuperação do computador físico / backup do servidor , iniciar o computador / servidor no repositório e publicá-lo diretamente no hipervisor Hyper-V, permitindo então a migração para o Hyper-V online e sem paradas em seu serviço.

119. Deverá oferecer a opção de recuperar arquivos, pastas, etc. diretamente do backup, sem a necessidade de recuperar totalmente o backup.

120. O agente deve suportar o processamento do Oracle para fazer backups consistentes do banco de dados e arquivar logs de soluções não clusterizadas , como RAC, ASM, e suportar as versões oficiais mais recentes do Oracle.

121. Suporte para backups completos no dia desejado da máquina física do Linux.

122. Deverá permitir a recuperação para a nuvem do Microsoft Azure e para a Amazon por meio do console centralizado.

Agente para Windows

123. A plataforma deve permitir a proteção de dados em computadores / servidores baseados no sistema operacional Microsoft Windows. Deve possuir a capacidade de executar backup, pelo menos, para as seguintes plataformas x86-64 bits (quando aplicável):

I. Microsoft Windows 7 SP1
II. Microsoft Windows 8.x
III. Microsoft Windows 10 – inclusive versão 1809
IV. Microsoft Windows Server 2008 R2 SP1
V. Microsoft Windows Server 2012
VI. Microsoft Windows Server 2012 R2
VII. Microsoft Windows Server 2016
VIII. Microsoft Windows Server 2019

124. Deve oferecer suporte para o Microsoft Bitlocker, para backup e recuperação.

125. Deve oferecer a possibilidade de suportar o computador / servidor completo, volumes individuais ou arquivos / pastas específicos.

126. A solução deve ter um controlador CBT (Rastreamento de Blocos Alterados) para ambientes físicos com o objetivo de executar backups incrementais com eficiência e rapidez.

127. Deve permitir o gerenciamento centralizado de backups e recuperações via interface gráfica (GUI) e linha de comando (CLI)

128. Permitir backup de arquivos abertos, garantindo a integridade do backup.
129. Ele deve oferecer seu próprio mecanismo de rastreamento de blocos modificados para detecção rápida de blocos para backup.
130. Deverá permitir como destino de backup:
i. Disco local
ii. Pasta compartilhada de rede
iii. Repositório de disco centralizado da plataforma de backup
iv. Repositório de disco de provedor de serviço certificado
v. Microsoft OneDrive
131. Deve permitir o uso de discos rotativos como destino dos backups.
132. Ele deve ter um mecanismo para permitir que o backup continue, mesmo se o computador / servidor remoto estiver temporariamente sem conectividade com o servidor de backup central.
133. Ele deve ter integração com o Microsoft VSS para suportar e garantir a consistência transacional dos aplicativos no backup.
134. Deve permitir a execução de scripts antes da geração do snapshot VSS e a execução de scripts após a geração do snapshot VSS.
135. Deve permitir a criação de uma Imagem de Recuperação, possibilitando:
i. A restauração do computador / servidor completamente antes do evento de desastre em outro hardware ou no hardware original, também chamado de "bare-metal"
ii. Executar tarefas de diagnóstico de memória
iii. Executar reparos de inicialização
iv. Resetar a senha do Administrador Local para computadores / servidores fora do domínio.
136. Ele deve ter a capacidade de criptografar os backups, usando os algoritmos mais comuns no mercado, suportando o uso de uma chave de pelo menos 256 bits.
137. Deve permitir escolher se a criptografia será realizada no processo dos dados, no tráfego de dados via rede ou no repositório de backup.
138. Deverá ser capaz de inicializar o computador / servidor completo do repositório de backup (sem transferência de dados) publicando diretamente no Hypervisor Hyper-V como uma máquina virtual, permitindo que o serviço seja reestabelecido rapidamente.
139. Deve permitir a recuperação granular de arquivos, pastas, etc ; diretamente do repositório de backup sem precisar recuperar o backup completo.
140. Deverá permitir a recuperação para a nuvem do Microsoft Azure e para a Amazon por meio do console centralizado.
141. Deve permitir a recuperação no nível de volume.
142. Deverá permitir o redimensionamento de volumes durante a recuperação no nível de volume.
143. Deve permitir a conversão de backups de nível de volume como discos virtuais dos seguintes formatos: VMDK , VHD e VHDX.
144. Deve permitir o gerenciamento centralizado de backups e recuperações via interface gráfica (GUI) e linha de comando (CLI)
145. Ele deve permitir a execução agendada de backups de computador / servidor por meio de

uma única interface:

i. Execução de processos de backup de acordo com políticas a serem definidas (frequência, retenção, tipo de backup).

ii. A definição de prioridade de execução dos backups.

iii. A programação de trabalhos de backup automatizados.

146. Permitir monitoramento via interface gráfica e em tempo real dos trabalhos, gerando arquivo de log.

147. Deverá usar o banco de dados para salvar o catálogo de tarefas, arquivos e dispositivos de backup.

148. Deve incluir ferramentas de recuperação granulares para o Microsoft Exchange 2010 SP1 e superior, para que seja possível recuperar objetos individuais, como contatos, mensagens, itens da agenda, anexos, etc. diretamente para a produção, sem a necessidade de recuperar o banco de dados do MS Exchange.

149. Deverá incluir ferramenta de recuperação granular para Microsoft Active Directory 2008 R2 SP1 e superiores, de modo que seja possível recuperar objetos individuais, tais como: usuários, grupos, containers, contas, objetos de politícas de grupo (GPO), registros DNS, etc – Sendo estes enviados direto para a produção sem a necessidade de recuperar a base do AD.

150. Deve incluir ferramentas de recuperação granular para o MS SQL Server 2005 SP4 e superiores, para que seja possível recuperar objetos individuais, como Bancos de Dados, Tabelas, Procedimentos de Armazenamento , Visualizações, Funções, etc. diretamente para produção. Sem a necessidade de recuperar a base do SQL.

151. Deverá oferecer suporte ao Microsoft Failover Cluster , incluindo o cluster de failover do SQL Server e os Grupos de Disponibilidade AlwaysOn do SQL Server .

152. Deve incluir ferramentas de recuperação granular para o MS SharePoint 2010 e superiores, de modo que seja possível recuperar sites , documentos, anexos, etc. direto para a produção. Não havendo a necessidade de recuperar o banco de dados do SharePoint.

153. Deverá incluir a ferramenta de recuperação de banco de dados do Oracle 11.xe 12.x diretamente na produção.

154. Deverá permitir o truncamento de logs transacionais para o MS Exchange, MS SQL e truncamento de log de archive para o caso do Oracle 11.xe 12.x.

155. Deve permitir o backup de logs transacionais para MS SQL e log de arquivamento para o caso do Oracle 11.xe 12.x

156. Deverá permitir a replicação dos backups do repositório principal para o repositório secundário gerenciado a partir da interface gráfica central.

157. Deverá permitir o backup em dispositivos de fita gerenciados a partir da interface gráfica central.

158. Deve permitir a importação de backups feitos pela solução.

159. Deverá ter uma ferramenta que forneça interface por linha de comando para executar tarefas de proteção de dados e operações administrativas, criar scripts ou integrar-se a soluções de terceiros.

160. Suportar múltiplas tarefas de backup

161. Backup de discos (HDD ou SSD) USB

162. A solução deve ter a capacidade de configurar a largura de banda a ser usada para a realização de backups.
163. A solução também deve restringir os caminhos de comunicação do agente de backup, isto é, restringir por conexão VPN, Restringir por conexão Wi-Fi e / ou por redes com medições.
164. O agente para Windows deve oferecer suporte ao Microsoft Exchange DAG, incluindo o IPless DAG, bem como as versões mais recentes do Exchange Server e do SharePoint .
165. Os agentes devem oferecer suporte ao gerenciamento centralizado do console da plataforma de backup, bem como sem administração.
166. A plataforma deve apoiar a recuperação granular de arquivos através de um portal de autosserviço via web.

Cronograma de Atividades (BACKUP E REPLICACAO):
• Planejamento
• Análise e dimensionamento da infraestrutura de backup
• Criação de servidor para instalação do software de backup
• Configuração de repositório no NAS para Backup e Replication
• Criação da rotina de backup para o NAS
• Criação da rotina de replicação para o NAS
• Testes de backup e restore
• Monitoramento e controle
• Encerramento

Deverá ser realizado *in loco* um treinamento de no mínimo 8 horas para equipe definida pelo município (máximo de 5 participantes)

LOTE 2 – ESTRUTURA E SERVIDORES

ITEM 1 - RACK 42U – QUANTIDADE 01

ESTRUTURA RACK 42U com as seguintes características mínimas:
- Peso Líquido não superior 126kg
- Dimensões máximas de altura: 2150mm
- Dimensões máximas de largura: 770.00 mm
- Dimensões máximas de profundidade: 1200.00 mm
- Capacidade de Carga (carga estática) 1363.64 KG
- Capacidade de Carga (carga dinâmica) 1022.73 KG
- Profundidade Mínima de Montagem 191.00 mm
- Profundidade Máxima de Montagem 915.00 mm
- Altura do rack: 42U
- Largura do plano interno de montagem: 19"
- Cor: Preto
- Posições Verticais aço #16
- Porta Frontal aço #16

- Porta Traseira aço #18
- Teto aço #18
- Painéis Laterais aço #18
- Aprovações UL 60950
- Garantia padrão: cinco anos para reparo ou substituição;
- Atendimento a normas ambientais RoHS, Norma REACH:
- Não contém substâncias altamente preocupantes (SVHC).
- Deverá possuir duas PDU´s com no minimo 20 tomadas cada.

ITEM 2 – SWITCH – QUANTIDADE 01

Switch de Acesso 48 portas Gigabit UTP 48G e 4 portas SFP/SFP+ com no mínimo os seguintes recursos e capacidades:

Deve ser novo, de primeiro uso, fazer parte do catálogo de produtos comercializados pelo fabricante na data de publicação do edital e não ter sido descontinuado.
Deve possuir 48 (quarenta e oito) portas 10/100/1000BASE-T com conector RJ-45;
Deve possuir 4 (quatro) portas 1/10Gbps SFP/SFP+;
Deve utilizar o método de switching "Store-and-forwarding";
Deve ter como tipos de tráfego unicast, multicast e broadcast;
Deve ter capacidade de supotar 6384 endereços mac em sua base;
Deve ter capacidade de suportar 64 instâncias de PVST;
Deve ter capacidade de suportar 31 instâncias de MSTP;
Deve ter capacidade de suportar 64 grupos de Link Aggregation;
Deve ter capacidade de suportar 8 portas em 1 grupos de Link Aggregation;
Deve ter capacidade de suportar 192 interfaces IP
Deve ter capacidade de suportar 512 entradas de cache ARP;
Deve ter capacidade de suportar 512 rotas em sua tabela de rotas;
Deve ter capacidade de suportar 256 entradas de ACLs.
Funcionalidades de camada 2
Deve implementar 802.1D Spanning Tree Protocol (STP);
Deve implementar 802.1s Multiple STP (MSTP);
Deve implementar 802.1w Rapid STP (RSTP);
Deve implementar Per-VLAN STP (PVST) e Rapid PVST (RPVST);
Deve implementar UDLD;
Deve implementar até4093 Vlans ativas;
Deve implementar 802.1Q VLANs eVLAN tagging em todas as portas;
Deve implementar tunelamento 802.1Q-in-Q VLAN;
Deve implementar Private VLAN;
Deve implementar Voice VLAN;
Deve implementar Multicast VLAN Registration (MVR).

Funcionalidades de Stacking
Deve implementar Stacking, suportando até 8 switches;
Deve implementar Stacking em topologia linear ou anel;
Deve implementar Link Aggregation entre os membors do Stacking com preferência local.
Funcionalidades de segtrança
Deve implementar ACLs de controle em IPV4, IPV6 e MAC address;
Deve implementar Gerenciamento de controle de acesso e administração;
Deve implementar Controle de acesso a rede (porta) baseado em 802.1x
Deve implementar Port Security;
Deve implementar Multiplos usuários e senhas para gerenciamento;
Deve implementar Autenticação e autorização através de base local, RADIUS ou TACACS+;
Deve implementar Proteção de DoS;
Deve implementar DHCP Snooping (IPV4 e IPV6).
Funcionalidades de QoS
Deve implementar IEEE 802.1p, IP ToS/DSCP, DiffServ, e ACL baseadas em classificação de tráfego e processamento;
Deve implementar Traffic shaping e remarcação baseados em políticas definidas;
Deve implementar IPV4/IPV6 ACL metering.
Funcionalidades Layer 3 (IPV4)
Deve implementar Portas roteadas;
Deve implementar ARP e Proxy ARP;
Deve implementar Encaminhamento IP;
Deve implementar Filtragem IP com ACLs;
Deve implementar Rotas estáticas;
Deve implementar RIP v1/v2
Deve implementar OSPF v1/v2
Deve implementar DVMRP;
Deve implementar VRRP;
Deve implementar PBR;
Deve implementar DHCP server, client e operações de relay;
Deve implementar IGMP v1/v2/v3;
Deve implementar PIM-SM e PIM-DM.
Funcionalidades Layer 3 (IPV6)
Deve implementar Portas roteadas;
Deve implementar NDP;
Deve implementar Encaminhamento IPV6;
Deve implementar Filtragem IPV6 com ACLs;
Deve implementar Rotas estáticas;
Deve implementar OSPFv3;
Deve implementar VRRP;
Deve implementar PBR;
Deve implementar DHCP server, client e operações de relay;

Deve implementar MLD;
Deve implementar PIM-SM e PIM-DM
Funcionalidades de monitoramento
Deve implementar SPAN e RPAN para análise de tráfego;
Deve implementar RMON;
Deve implementar Logs de buffer, console e syslog;
Deve implementar Alertas via email;
Deve implementar sFLOW agent para monitoramento de tráfego.
Deve implementar LEDs indicativos de status das portas.
Funcionalidades de gerência
Gerencimento através de interface WEB (GUI);
Gerencimento através de interface serial (CLI);
Gerencimento através de telnet (CLI);
Gerencimento através de SSH v2 (CLI);
Gerencimento através de SNMP v1,v2 e v3;
Gerencimento através de LLDP para discoberta de dispositivos na rede;
Gerencimento através de ISDP para discoberta de dispositivos CISCO na rede;
Gerencimento através de SNTP para sincronização de relógio;
Gerencimento através de GARP VLAN Registration Protocol para registro dinâmico de VLANs;
Características de padrão Ethernet
IEEE 802.1Q VLANs and VLAN tagging
IEEE 802.3ac VLAN tagging
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.1D Spanning Tree Protocol (STP)
IEEE 802.1s Multiple STP (MSTP)
IEEE 802.1w Rapid STP (RSTP)
IEEE 802.1p Class of Service (CoS) prioritization
IEEE 802.3x Full-duplex Flow Control
IEEE 802.1x Port-based authentication
IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)
IEEE 802.3az Energy Efficient Ethernet (EEE)
IEEE 802.3 10BASE-T copper twisted pair Ethernet (10 Mb)
IEEE 802.3u 100BASE-TX copper twisted pair Fast Ethernet (100 Mb Ethernet)
IEEE 802.3ab 1000BASE-T copper twisted pair Gigabit Ethernet
IEEE 802.3z 1000BASE-SX short range fiber optics Gigabit Ethernet
IEEE 802.3z 1000BASE-LX long range fiber optics Gigabit Ethernet
IEEE 802.3ae 10GBASE-SR short range fiber optics 10 Gb Ethernet
IEEE 802.3ae 10GBASE-LR long range fiber optics 10 Gb Ethernet
IEEE 802.3ae 10GBASE-ER extended range fiber optics 10 Gb Ethernet
IEEE 802.3an 10GBASE-T copper twisted pair 10 Gb Ethernet
SFF-8431 10GSFP+Cu SFP+ Direct Attach Cable
Características físicas

Altura: 44 mm;
Largura: 441 mm;
Depth: 254 mm;
Peso máximo: 3.8 Kg.
Variaveis de ambiente
Temperatura: 0 - 50 °C ;
Humidade relativa: 5 - 95% (sem condensação)
Altitude: até 3000 m;
Fluxo de ar: lado a lado (esquerda para a direita)
Entrada elétrica:
100 - 127 V CA (nominal); 50 Hz / 60 Hz; 0,5 A
200 - 240 V CA (nominal); 50 Hz / 60 Hz; 0,25 A
Consumo de energia: 50 W
Dissipação de calor: 171 BTU / hora
Emissão de ruído acústico: menos de 64 Db

ITEM 3 – SERVIDOR COM STORAGE – QUANTIDADE 01
SERVIDOR RACK com as seguintes características mínimas:
CHASSI: Rack padrão 19 polegadas, ocupando, no máximo, 1 (UM) unidades de rack (1U).
FONTE DE ALIMENTAÇÃO: Duas fontes de alimentação redundantes, potência mínima de 750 Watts, 110/220 VAC à 60Hz.
PLACA MÃE "MOTHERBOARD": da mesma marca do fabricante do servidor. No mínimo, 24 (Vinte e Quatro) conectores na própria placa mãe, sem uso de placa de expansão para módulo de memória. 1 (uma) placa gráfica on-board para monitor com conectores DB15 (análogo).
PROCESSADOR: Suportar no mínimo de 2 (Dois) processadores de arquitetura com suporte a 64bits com no mínimo 08 (Oito) núcleos e 16 threads cada em sua configuração máxima;
Acompanhar no mínimo 02 (dois) processadores com frequencia base mínima de 2.1 GHz; Deve possuir pelo menos 11 MB de cache; No mínimo Memória com frequência de DDR4-2666MHz.
MEMÓRIA: Possuir no mínimo 512 GB de memória RAM; Deverá suportar expansão mínima de 3 TB (Terabytes), em 24 pentes (12 pentes por processador);
Modulos de memória não poderão ser de tamanho inferior à 32GB de memória do tipo DDR4 na frequência de 2666MHz.
UNIDADE DE DISCO RÍGIDO: Possuir no mínimo 02 discos MECÂNICOS do tipo Enterprise SAS 12GBPS com no mínimo 600GB;
Suportar no mínimo 10 (Dez) discos do tipo Serial SATA-III, com taxa de transferência mínima de 6 (seis) Gbit/S, com conector hot-swap de 2.5";
Deve suportar discos com velocidade rotacional de 7.200 rpm, 10.000 rpm, 15.000rpm, do tipo SSD e NVMe;
Tecnologia de pré-falha SMART (Self Monitor AnalysisReport Test) ou equivalente incorporado, atrelado à controladora de disco e ao Software de gerenciamento.
CONTROLADORA DE RAID: A controladora deve ser capaz de implementar os seguintes arranjos: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50;

INTERFACE DE REDE LOCAL: No mínimo 4 (quatro) portas interface RJ45, rede Gigabit Ethernet 10/100/1000 MBPs, Suporte à VLAN, Link Aggregation e Jumbo Frames; Suporte à VMwareNetQueue.
INTERFACE DE REDE LOCAL/SAN: No mínimo 4 (quatro) portas interface SFP+, 10GbE.
PORTAS DE COMUNICAÇÃO: 4 (quatro) portas USB.
BIOS: Desenvolvida pelo mesmo fabricante do equipamento ou este fabricante deve ter direitos copyright sobre a mesma
VÍDEO: Deverá possuir conector externo VGA (DB15).
GERENCIAMENTO: Deverá fornecer junto ao equipamento um software de gerência, do mesmo fabricante do servidor,
compatível com o padrão IPMI 2.0 que possibilite o gerenciamento remoto através de controladora de gerenciamento integrada com porta RJ-45 dedicada não sendo essa nenhuma das interfaces de controladora de rede.
COMPATIBILIDADE COM SISTEMAS OPERACIONAIS: Windows Server 2016 ou posterior; RedHat Enterprise Linux 6.7 ou posterior; apresentar compatibilidade comprovada para o sistema de virtualização VMWare ESX 6.5 ou posterior.

ARMAZENAMENTO DE DADOS (STORAGE) com as seguintes características mínimas:
Storage Enclosure para até 24 discos SFF, Cache de 8GB por controladora, Fonte de alimentação redundante, controller supports 8/16Gb FC, 1GbE iSCSI ou 10GbE iSCSI SFPs:
- 4 portas 10 Gb iSCSI SFP+
- Suporte a RAID 1, 5, 6, 10
- Suporte para expansão de até 96 discos SFF via módulos
- Suporte a virtual pools
- Suporte até 1024 LUN's de 128TB
- Software padrão para até 128 Snapshot's
- Form fator 2U
- Entregue com 20 discos de 1.2TB 12G SAS 10K RPM 2.5in SFF e 4 discos de 800GB 3DWD 12G SAS SSD 2.5in
- A solução de armazenamento deve possuir capacidade para auto monitoramento e geração de registro (log) de falhas, detecção e isolamento de erros de memória e de erros de disco.
- A solução de armazenamento deve suportar no mínimo a implementação de redundância de discos por RAID 1, 5, 6, 10.
- Suporte para hardware Foundation Care por 3 anos on-site com atendimento 24x7 e tempo de RESOLUÇÃO em até 6 horas.
- A solução de armazenamento deve possuir arquitetura de array virtualizado (Storage Array), abstraindo a gestão de drives e facilitando o gerenciamento da solução,
e deve ser composta por fontes de alimentação e ventilação redundantes e hot-swappable, drives de armazenamento (HDD) hot-plug e um par de controladoras hot-plug.
- A solução de armazenamento deve possuir memória cache de, no mínimo, 8 GB por controladora.

ITEM 04 - SERVIÇO/AQUISIÇÃO DE LICENÇA DE USO DE SOFTWARE DE VIRTUALIZAÇÃO -

QUANTIDADE 01

1.0 SISTEMA DE VIRTUALIZAÇÃO
1.1 Cada licença deve dar direito de uso do software em 3 hosts físicos com 2 processadores processadores físicos cada.
1.2 Deverá suportar o uso de até 768 processadores lógicos por servidor físico.
1.3 Deverá suportar até 16 TB de memória RAM por servidor físico.
1.4 Deverá ser instalável nativamente no servidor, não necessitando de Sistema Operacional de terceiro para sua instalação;
1.5 Deverá suportar por servidor físico:
1.7 32 portas 1 Gigabit Ethernet.
1.8 16 portas 10 Gigabit Ethernet.
1.9 16 portas 20 Gigabit Ethernet.
1.10 8 portas 40 Gigabit Ethernet.
1.11 8 portas 50 Gigabit Ethernet.
1.12 4 portas 100 Gigabit Ethernet.
1.13 16 HBA's (Host Bust Adapter).
1.14 Até 1024 máquinas virtuais por host físico.
1.15 Possuir sistema operacional próprio executando diretamente no hardware sem a necessidade de instalação de Sistema Operacional adicional para execução do software de virtualização.
1.16 Permitir a criação de máquinas virtuais com mais de 1 processador, isto é, máquinas virtuais multiprocessadas com até 4 (quatro) processadores em todos os sistemas operacionais suportados.
1.17 Permitir a criação de máquinas virtuais com até 6 TB de memória.
1.18 Permitir a criação de máquinas virtuais com até 10 placas de rede.
1.19 Permitir a criação de máquinas virtuais com 256 processadores virtuais.
1.20 Permitir a criação de discos virtuais de até 62TB
1.21 Suportar tecnologias para melhoria de perfomance de rede como jumbo frames e TCP Segmentation Offloading.
1.22 Deverá suportar a criação de VLANS nas redes virtuais.
1.23 Permitir o isolamento total das máquinas virtuais, impedindo a comunicação entre as máquinas a não ser pelo ambiente de rede em que serão inseridas, evitando assim que o uso de uma máquina virtual interfira na segurança de outra máquina virtual.
1.24 Permitir o acesso por mais de um caminho (multipath) e tolerante a falha (failover) ao SAN ("Storage Area Network").
1.25 Possuir sistema de arquivo que permita ser configurado em storage compartilhado e que mais de um servidor físico consiga acessar o mesmo compartilhamento simultaneamente.
1.26 Permitir conexões com tecnologias de storage SAN, iSCSi e NAS.
1.27 Permitir a instalação em um servidor físico sem disco físico local, podendo ser iniciado através de uma SAN ("Storage Area Network") utilizando o conceito de diskless.
1.28 Permitir que cada máquina virtual tenha endereço IP e MAC address próprio.
1.29 A solução deverá ser fornecida por um único fabricante.
1.30 Permitir a conversão ilimitada de um sistema físico existente com sistema operacional

Windows para uma máquina virtual.
1.31 Permitir a conversão ilimitada de um sistema físico existente com sistema operacional Linux RHEL, SUSE e Ubuntu para uma máquina virtual.
1.32 Suportar a extensão do tamanho do disco virtual enquanto a máquina virtual permanecer ligada.
1.33 Suportar o clone de máquinas virtuais a quente sem interrupção da máquina virtual a ser clonada.
1.34 Deverá possuir recurso de compartilhamento de páginas de memória entre múltiplas máquinas virtuais, ou seja, consolidação de páginas de memórias idênticas de múltiplas máquinas virtuais em um mesmo servidor em apenas uma página.
1.35 SUPORTE FABRICANTE
1.36 Deverá oferecer suporte e atualização de Software pelo período de 36 meses no regime 12x5, prestado obrigatoriamente pelo fabricante do software através de ligação gratuita, email e site do fabricante na internet.
1.37 Treinamento Operacional básico do produto (transferência de conhecimento) para até 2 profissionais do Contratante pelo periodo mínimo de 4 horas.
2 - DESCRIÇÃO QUANTIDADE
2.0 CONSOLE DE GERENCIAMENTO E ADMINISTRAÇÃO DO SISTEMA DE VIRTUALIZAÇÃO 01
2.1 Deverá permitir a gerência centralizada de todo o parque virtualizado, a partir de um único console;
2.2 Este console deve ser único e permitir o gerenciamento de TRÊS (3) servidores físicos instalados com o Sistema de Virtualização;
2.3 Este console não deve ser um ponto único de falha, devendo todas as Máquinas Virtuais permanecerem disponíveis em caso de falha;
2.4 Possuir a funcionalidade de gerenciamento dos recursos de hardware (consumo de processadores, memória RAM, dispositivos de rede, discos rígidos, controladoras de disco/storage), bem como gerenciar a performance das máquinas virtuais instaladas no Servidor de Virtualização, através de console via Browser com tráfego criptografado (SSL).
2.5 Deverá permitir o compartilhamento dos recursos físicos do servidor entre as máquinas virtuais, com a possibilidade de definir a quantidade mínimo e máxima de CPU e memória para cada máquina virtual.
2.6 Deverá permitir o compartilhamento dos recursos físicos do servidor entre as máquinas virtuais, com a possibilidade de definir a quantidade mínima e máxima de CPU e memória para um grupo de máquinas virtuais.
2.7 Deverá permitir o compartilhamento dos recursos físicos do servidor entre as máquinas virtuais, com a possibilidade de definir a saída de banda de rede para cada máquina virtual.
2.8 Deverá permitir o compartilhamento dos recursos físicos do servidor entre as máquinas virtuais, com a possibilidade de definir a prioridade de acesso a disco para cada máquina virtual.
2.9 Permitir a criação de ambiente de alta disponibilidade (cluster ou tecnologia equivalente ou superior) entre as máquinas virtuais, independente se estas estão em servidores físicos diferentes ou não.
2.10 Permitir a funcionalidade de migração de uma máquina virtual de um host físico para outro

host físico, sem necessidade de interrupção dos serviços da máquina virtual.
2.11 A solução deverá ser capaz de otimizar a utilização de disco da máquina virtual, armazenando em Storage somente o que a máquina virtual estiver utilizando, ou seja, não alocando todo o conteúdo do disco virtual quando não for necessário.
2.12 Possuir funcionalidades de detecção de falha de uma máquina física, migrando automaticamente as máquinas virtuais afetadas para controle de outra máquina física e procedendo, sua ativação automaticamente. Deverá suportar um grupo de até 32 servidores simultaneamente.
2.14 Permitir a criação através de interface gráfica de switches virtuais, comunicação local, não necessitando de placas de redes físicas, permitindo que redes complexas sejam construídas e as aplicações sejam desenvolvidas, testadas e distribuídas, tudo em um único computador físico.
2.15 Possuir tecnologia que permita tomar vantagem das redes 10Gb Ethernet, tirando a carga de roteamento de pacotes da camada de virtualização para ser executada direto na placa de rede física reduzindo ciclos de CPU e latência.
2.16 Permitir priorizar automaticamente determinado recurso (CPU e memória) a determinada máquina virtual no caso de concorrência de recurso sem necessidade de desligar a máquina virtual.
2.17 Permitir que ferramentas de backup, tais como, Tivoli, Netbackup, VEEAM Backup realizem backup e recuperação incrementais, diferenciais e de imagem completa de máquinas virtuais bem como em nível de arquivo para os sistemas operacionais Windows e Linux centralizado sem agentes. O backup passa a ser feito na camada de virtualização, o gerenciamento é feito por serviço de backup eliminando o peso do backup sobre os servidores físicos ou máquinas virtuais.
2.18 Permitir realizar o backup de imagens de múltiplas máquinas virtuais simultaneamente sem a necessidade de desligá-las.
2.19 Permitir a criação de novas máquinas virtuais através de modelos já criados (biblioteca de templates), e prontos para serem instalados em qualquer servidor físico que componha o ambiente de servidores consolidados.
2.20 Permitir a visualização gráfica da topologia da infraestrutura virtual.
2.21 Permitir o monitoramento em tempo real e otimizar a utilização dos recursos não utilizados pelos hardwares.
2.22 Permitir monitoramento da utilização individual de cada servidor físico e de cada máquina virtual criada.
2.23 Permitir configurar faixas de alarme para monitoração de CPU, memória, rede e disco que alertem após um período de tempo pré-definido no estado de alerta.
2.24 Permitir a monitoração e notificação de alertas parametrizados através de e-mail, traps SNMP e scripts.
2.26 Permitir parar, iniciar, suspender, reiniciar máquinas virtuais.
2.27 Permitir o ajuste de uso de CPU e memória por máquina virtual.
2.28 Permitir adicionar CPU e memória a uma máquina virtual sem parada de produção.
2.29 Permitir adicionar e remover placas de rede e discos a uma máquina virtual sem parada de produção.
2.30 Permitir o armazenamento dos dados e estatísticas de monitoração da console central em um SGDB (Sistema de gerenciamento de banco de dados) ORACLE ou Microsoft SQL Server.

2.31 Permitir armazenar dados e estatísticas de monitoração por até dois anos.
2.32 Permitir a redução da complexidade de gerenciamento, combinando servidores físicos em clusters para maior disponibilidade, e controle de recursos mais flexível.
2.33 Permitir coletar informações de performance de servidores físicos, analizar e sugerir cenários para a consolidação dos servidores físicos em máquinas virtuais. A consolidação sugerida pode ser feita com servidores físicos existente ou adicionando novos servidores com suas respectivas configurações de hardware.
2.35 Ser capaz de configurar através de interface gráfica a associação de uma ou mais placas de rede a uma máquina virtual, permitindo a distribuição de carga entre as placas de rede e configuração de tolerância a falhas.
2.36 Permitir múltiplos snapshots de uma máquina virtual.
2.37 Possuir API para integração com a console de gerenciamento das máquinas virtuais.
2.38 Permitir a integração com a console de gerenciamento através de Web Service.
2.39 SEGURANÇA
2.40 Permitir a integração com o sistema de diretório MICROSOFT ACTIVE DIRECTORY OU LDAP, possibilitando integrar a estrutura de usuários com a hierarquia de segurança dos grupos de servidores e máquinas virtuais sem precisar alterar o esquema do serviço de diretório.
2.41 Possuir funcionalidade para automatização da aplicação de atualizações no sistema operacional utilizado para virtualização.
2.43 Permitir gerenciar o acesso a console de administração de forma granular. Dessa forma, cada usuário ou grupo terá uma quantidade de ações que ele pode executar na console de adminstração.
2.44 A console de gerenciamento deverá permitir no mínimo a granularidade de acesso para as seguintes ações:
2.45 Ligar uma ou mais máquinas virtuais.
2.46 Desligar uma ou mais máquinas virtuais.
2.47 Criar máquinas virtuais.
2.48 Remover máquinas virtuais.
2.49 Criar templates de máquinas virtuais.
2.50 Criação de cluster de máquinas virtuais.
2.51 Adicionar e remover um servidor físico à console de gerenciamento.
2.52 Criar grupos de permissão e associar a usuários.
2.53 Criar e apagar alarmes de monitoração.

Cronograma de Atividades (SWITCHES):
• Planejamento
• Análise da infraestrutura atual
• Dimensionamento da infraestrutura nova
• Configuração dos switches em Stacking
• Configuração das VLANS/TRUNKS necessários
• Configuração de LACP necessários
• Configuração de TRUNK entre o Swicth Core atual com os novos se suportado

• Testes e validação • Monitoramento e controle • Monitoramento da operação da infraestrutura nova • Encerramento Cronograma de Atividades (STORAGE): • Planejamento • Análise da infraestrutura atual • Dimensionamento da infraestrutura nova • Conectividade nos equipamentos de rede fornecendo alta disponibilidade • Configuração da interface de gerenciamento • Criação das LUNS • Configuração da segurança de acesso para os hosts VMware • Testes e validação • Monitoramento e controle • Monitoramento da operação da infraestrutura nova • Encerramento
LOTE 03 - SERVIDOR DE BACKUP NETWORK ATTACHED STORAGE (NAS) – QUANTADE 01
Deverá ter capacidade de no mínimo 96TB de armazenamento RAW; Deverá ter no mínimo 12 baias de HDD; Suportar no mínimo os padrões RAID, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 e RAID 10; Suportar no mínimo a migração de RAID 1 para RAID 5 e RAID 5 para RAID 6; Processador Quad Core de no mínimo 2.1GHz; Mínimo de memória do sistema 32 GB RAM DDR4; Suporte a expasão PCIe para Rede/Adaptadores M.2 SATA/NVME para Cache; Tipo de drive suportados HDs e SSDs SATA 3Gb/s ou 6Gb/s; Gavetas hot-swappable; Deverá ter no mínimo 04 (quatro) portas Ethernet RJ45 10/100/1000Mb (GbE); Deverá permitir gerenciamento e configuração via protocolo HTTP e HTTPS; Indicador LED: Status do sistema, HDD, LAN; Botão: Alimentação, Reset; Aviso do sistema: Alarme; Ter as certificações: EAC, VCCI, CCC, RCM, FCC, CE, BSMI; Deverá ter garantia de no mínimo 03 (três) anos; Suportar expansão de módulo; Deverá ter KIT para instalação em Rack 19"; Cronograma de Atividades (NAS): • Planejamento • Análise da infraestrutura atual • Dimensionamento da infraestrutura nova

• Conectividade nos equipamentos de rede fornecendo alta disponibilidade • Configuração da interface de gerenciamento • Criação das LUNS para entrega aos hosts VMware • Configuração da segurança de acesso para os hosts VMware • Testes e validação • Monitoramento e controle • Monitoramento da operação da infraestrutura nova • Encerramento
LOTE 04 - NOBREACK – QUANTIDADE 01
SISTEMA ININTERRUPTO DE ENERGIA (UPS) para Rack de até 4U com as seguintes características mínimas: SAÍDA: Capacidade de saída 6.0kWatts / 6.0kVA Voltagem nominal de saída 230V Distorção de voltagem de saída menor que 2% Frequência de saída 50/60Hz +/- 3 Hz Other Output Voltages 220, 240 Tipo de onda: Senoidal Conexões de saída (4) IEC 320 C19 (Bateria) (6) IEC 320 C13 (Bateria) (1) Hard Wire 3-wire (H N + G) (Bateria) (2) IEC Jumpers (Bateria) Bypass interno (automático e manual) ENTRADA: Voltagem de entrada nominal 230V Frequência de entrada 40 - 70 Hz (auto sensing) Variação de voltagem de entrada: 160 a 275V BATERIA: Bateria livre de manutenção, à prova de vazamento, selada, do tipo chumbo-acido. Tempo médio de recarga 1.5 horas Tempo de vida útil de 3 à 5 anos. Capacidade Volt-Amp-Hora 902 GERENCIAMENTO: Porta de gerenciamento RJ-45 10/100 Base-T, RJ-45 Serial, Smart-Slot, USB OPERAÇÃO: Temperatura de operação de 0 a 40 graus celcius. CONFORMIDADE: Aprovado por: CE, CE Mark, EAC, EN/IEC 62040-1, EN/IEC 62040-2, IRAM, RCM, VDE GARANTIA: Garantia de 3 anos para equipamento e 2 anos para bateria

BATERIA EXTRA: (3 unidades)
Bateria livre de manutenção, à prova de vazamento, selada, do tipo chumbo-acido.
Tempo de vida útil de 3 à 5 anos.
Capacidade Volt-Amp-Hora 1920
Garantia de 2 anos.
Temperatura de operação de 0 a 40 graus Celsius.

LOTE 05 - APPLIANCE PARA SEGURANÇA DA INFORMAÇÃO – (UTM / LICENÇA ANUAL) - QUANTIDADE 01

1. **Especificações Gerais**
   - 1.1. Distribuidor deve ter presença nacional de suporte.
   - 1.2. O contratante deve possuir a opção de abrir solicitações de suporte diretamente com o fabricante.
   - 1.3. O Appliance proposto deve fornecer logs e relatórios embarcados contendo no minimo os itens abaixo:
     - 1.3.1. Dashboard com informações do sistema:
       - 1.3.1.1. Informações de CPU
       - 1.3.1.2. Informações do uso da rede.
       - 1.3.1.3. Informações de memória.
       - 1.3.1.4. Informações de sessões ativas.
       - 1.3.1.5. Permitir visualizar número politicas ativas.
       - 1.3.1.6. Visualizar numero de access points do fabricante conectados.
       - 1.3.1.7. Visualizar numero de usuários conectados remotamente.
       - 1.3.1.8. Visualizar numero de usuários conectados localmente.
     - 1.3.2. Relatórios com informações sobre as conexões de origem e destino por países.
     - 1.3.3. Relatórios informando as conexões dos hosts.
     - 1.3.4. Visualizar relatórios por periodo de tempo, permitindo o agendamento e o envio destes relatórios por email.
     - 1.3.5. Permitir exportar relatórios para as seguintes extensões/plataformas:
       - 1.3.5.1. PDF
       - 1.3.5.2. HTML
       - 1.3.5.3. Excell
     - 1.3.6. Permitir visualizar relatório de politicas ativas associado ao ID da politica criada.
     - 1.3.7. Relatório que informe o uso IPSEC por host e usuário.
     - 1.3.8. Relatório que informe o uso L2TP por host e usuário.
     - 1.3.9. Relatório que informe o uso PPTP por usuários.
     - 1.3.10. Relatório abordando eventos de VPN.
     - 1.3.11. Proporcionar sistema de logs em tempo real, com no minimo as seguintes informações:
       - 1.3.11.1. Logs do sistema.
       - 1.3.11.2. Logs das politicas de segurança
       - 1.3.11.3. Logs de autenticação
       - 1.3.11.4. Logs de administração do appliance.
     - 1.3.12. Permitir ocultar dos relatórios usuários e IPs cadastrados.
   - 1.4. Ter relatórios customizados e em compliance com pelo menos estes orgãos: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA.

1.5. Possuir no mínimo 6 interfaces 10/100/1000;
1.6. A solução proposta deve cumprir as normas da CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC.
1.7. A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte:
1.7.1. Suportar no mínimo xxx.000 (xxx e xxx e xxxx mil) novas conexões por segundo;
1.7.2. Suportar no mínimo x.xxx.xxx (xxx milhões xxx mil) conexões simultâneas;
1.7.3. Possuir no mínimo xx.000 Mbps (xxx mil) de rendimento (throughput) do Firewall para pacotes UDP;
1.7.4. No mínimo xxx (xxx mil e xxxx) Mbps de rendimento (throughput) do IPS;
1.7.5. Possuir no minimo xxxx Mbps de throughput de VPN AES.
1.8. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real:
1.8.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo.
1.8.2. Possuir no mínimo xxx Mbps de rendimento (throughput) de IPS mundo real.
1.8.3. Possuir no mínimo xxx Mbps de rendimento (throughput) de funcionalidades next generation em mundo real;
1.8.4. Possuir no mínimo xxx de rendimento (throughput) de VPN AES mundo real.
1.9. Entende-se como mundo real testes realizados utilizando ambientes e protocolos usados no mundo corporativo.
1.10. A solução proposta deve possuir licenças baseado nos recursos de hardware.
1.11. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.12. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP.
1.13. A solução proposta deve possuir no minimo xxx GB de espaço em disco SSD para o armazenamento de eventos e relatórios.
1.14. Possuir slot de FleXi Port
1.15. Possuir portas USB 2.0 e 3.0.
1.16. Possuir porta VGA.
1.17. Possuir ao menos uma porta COM (RJ45).
1.18. Possuir painel de LCD na parte frontal do appliance com funcionalidades basicas para ajudar na gerencia do equipamento.
1.19. Número irrestrito de usuários/IP conectados.
1.20. Appliance com **x**U para montagem em rack.

2. Especificações da Administração, Autenticação e Configurações em geral

2.1. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e Console.
2.2. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário.
2.3. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos e via FTP, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.
2.4. A solução proposta deve suportar implementações em modo Router (camada 3) e Transparente (camada 2) individualmente ou simultâneos.
2.5. A solução proposta deve suportar integrações com, Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.
2.6. A solução proposta deve suportar em modo automático e transparente "Single Sign On"

na autenticação dos usuários do active directory e eDirectory.

2.7. Os tipos de autenticação devem ser, modo transparente, por autenticação Kerberus/NTLM e cliente de autenticação nas máquinas.
2.8. Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.
2.9. Certificados de autenticação para iOS e Android.
2.10. A solução proposta deve suportar integração com Dynamic DNS de terceiros
2.11. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
2.12. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
2.13. A solução proposta deve suportar NTP.
2.14. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
2.15. A solução proposta deve ter suporte multilíngue para console de administração web.
2.16. A solução proposta deverá suportar fazer um roll back de versão.
2.17. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
2.18. A solução proposta deve suportar instalação de LAN by-pass no caso do appliance estar configurado no modo transparente.
2.19. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar.
2.20. A solução proposta deve suportar SNMP v1, v2c e v3.
2.21. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
2.22. A solução proposta deve possuir serviço de "Host Dynamic DNS" sem custo e com segurança reforçada.
2.23. A solução proposta deve ser baseado em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.
2.24. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
2.25. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação)
2.26. A solução proposta deve ter suporte a ambientes de terminais (Microsoft e Citrix) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
2.27. A solução proposta deve suportar:
  2.27.1. Serviço de DHCP/DHCPv6;
  2.27.2. Serviço de DHCP/DHCPv6 Relay Agent;
  2.27.3. Suporte a DHCP sobre VPN IPSec;
2.28. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.
2.29. Gráficos, relatórios e ferramentas avançadas de opoio para troubleshooting.
2.30. Permitir exportar informações de troubleshooting para arquivo PCAP.
2.31. Permitir o factory reset e troca do idioma via interface gráfica.
2.32. Atualização de firmware de forma automatizada
2.33. Reutilização de definições de objetos de rede, hosts, serviços, periodo de tempo, usuários , grupos, clientes e servers.
2.34. Portal de acesso exclusivo para usuários poderem realizar atividades

administrativas que envolve apenas funcionalidades especificas a ele.

2.35. Controle de acesso e dispositivos por zoneamento.

2.36. Integrar com ferramenta de gerenciamento centralizado disponibilizado pela própria fabricante.

2.37. Opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada dentro do proprio appliance ofertado.

2.38. Traps SNMP ou email para notificações do sistema.

2.39. Suportar envio de informações via Netflow e possuir informações via SNMP.

2.40. Suporte a TAP mode para POCs e trials.

2.41. Ter funcionalidade que permita que o administrador manualmente atribua e/ou desatribua cores do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.

2.42. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

3. Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet

3.1. A solução proposta deve suportar o balanceamento de carga e redundância para mais de 2 (dois) links de Internet.

3.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.

3.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.

3.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.

3.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

3.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).

3.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

4. Especificações de Alta Disponibilidade

4.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo.

4.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.

4.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.

4.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

4.5. A solução proposta deve suportar sincronização automática e manual entre os appliances em "cluster".

4.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

5. Proteção básica de firewall

5.1. Especificações do Firewall e roteamento

5.2. A solução deve ser Standalone Appliance e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.

5.3. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-to-one", NAT Dinâmico e PAT.

5.4. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino,

IP/Subnet/Grupo e Porta de Destino na regra do Firewall.

5.5. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso.

5.6. A solução proposta deve suportar arquitetura de segurança baseado em Zonas.

5.7. A solução proposta deve ter predefinido aplicações baseados na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".

5.8. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.

5.9. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).

5.10. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.

5.11. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.

5.12. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como: a senha padrão não foi alterada, acesso não seguro está permitindo ou a licença irá expirar em breve.

5.13. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.

5.14. A solução proposta deve suportar IPv6.

5.15. A solução proposta deve suportar implementações de IPv6 Dual Stack.

5.16. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.

5.17. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.

5.18. A solução proposta deve suportar DNSv6.

5.19. A solução proposta deve oferecer proteção DoS contra ataques IPv6.

5.20. A solução proposta deve oferecer prevenção contra Spoof em IPv6.

5.21. A solução proposta deve suportar 802.3ad para Link Aggregation.

5.22. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.

5.23. A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.

5.24. Flood protection, DoS, DDoS e Portscan.

5.25. Bloqueio de Países baseados em GeoIP.

5.26. Suporte a Upstream proxy.

5.27. Suporte a VLAN DHCP e tagging.

5.28. Suporte a Multiple bridge.

5.29. Funcionalidades do portal do usuário

5.29.1. Autenticação de dois fatores(OTP) para IPSEC e SSL VPN, portal do usuário, e administração web(GUI).

5.29.2. Download dos clientes de autenticação disponibilizados pela ferramenta.

5.29.3. Download do cliente VPN SSL em plataformas Windows.

5.29.4. Download das configurações SSL em outras plataformas.

5.29.5. Informações de hotspot.

5.29.6. Autonomia de troca de senha do usuário.
5.29.7. Visualização do uso de internet do usuário conectado.
5.29.8. Acesso a mensagens quarentenadas.

5.30. Opções base de VPN

5.30.1. Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.
5.30.2. L2TP e PPTP.
5.30.3. VPN SSL, IPSEC.
5.30.4. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

5.31. Funcionalidades base de QoS e Quotas

5.31.1. QoS aplicado a redes e usuários de download/Upload em trafegos baseados em serviços.
5.31.2. Otimização em tempo real do protocolo Voip.
5.31.3. Suporte a marcação DSCP.
5.31.4. Regras associadas por usuário.
5.31.5. Criar regras que limitem e garatam upload e download.
5.31.6. Permitir criar regra de QoS individualmente e compartilhada.

5.32. Segurança de redes Wifi

5.32.1. Fornecer gerencia dos access points do mesmo fabricante remotamente.
5.32.2. Plug and play no deploy dos access points.
5.32.3. Permitir criar SSIDs com bridge to LAN, bridge to VLAN e zona separada.
5.32.4. Suporte a multiplas SSIDs, incluindo hidden SSIDs.
5.32.5. Suporte WPA2 Personal e Enterprise.
5.32.6. Suporte a IEEE 802.1X (RADIUS authentication).
5.32.7. Suporte a 802.11r (fast transition).
5.32.8. Suporte a hotspot, customização de vouchers, senha do dia e termos de aceitação.
5.32.9. Acesso a rede wireless baseada em horário.
5.32.10. Escolha do melhor canal feita automaticamente pela ferramenta, buscando a melhor performance.
5.32.11. Suporte a login em HTTPS.
5.32.12. Detecção de Rogue AP.
5.32.13. O access point deve poder operar e ser gerenciado (tendo alteração de configurações) de forma idependente de uma controladora central, onde em caso de interrupção de link isto não afetará sua gerencia. Para isto deve-se ter uma controladora local e esta controladora deve ser gerenciada de forma central.

6. Proteção Web

7. Filtragem e Segurança Web

7.1. Proporcionar transparência total de autenticação no proxy, provendo segurança anti-malware e filtragem web.
7.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agragadas a pelo menos 92 categorias oferecidas pela solução.
7.3. Realizar autenticação dos usuários nos modos transparente e padrão.
7.3.1. As autenticações devem ser feitas via NTLM.
7.4. Possuir sistema de quotas aplicado por usuários e grupos.
7.5. Permitir criar politicas por horário aplicado a usuários e grupos.
7.6. Possuir sistema de malware scanning que realize as seguintes ações:
7.6.1.Bloquear toda forma de vírus

7.6.2. Bloquear malwares web
7.6.3. Previnir infecção de malwares, trojans e spyware em trafegos HTTPS, HTTP,FTP e emails baseados em acesso web(via navegador).
7.6.4. Proporcionar proteção de web malware avançado com emulação de Javascript.
7.7. Prover proteção em tempo real de todos os acessos web.
7.7.1. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.
7.8. Provêr pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.
7.9. Fornecer Pharming Protection.
7.10. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.
7.11. Permitir criação de regras customizadas baseadas em usuário e hosts.
7.12. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.
7.13. Validação de certificado.
7.14. Provêr cache de navegação, contribuindo na agilidade dos acessos a internet.
7.15. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
7.16. Integração com o youtube for schools.
7.17. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura(SafeSearch): Google, Bing e Yahoo.
7.18. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
7.19. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
7.20. Permitir a customização da pagina HTML que apresenta as mensagens e alertas para os usuários finais.
7.21. Permitir visualizar as alterações feitas nos itens 7.17 e 7.18 antes de salvar as modificações.
7.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
7.22.1. Range aceitável de 1 a 25600KB.
7.23. Bloquear trafego que não segue os padrões do protocolo HTTP.
7.24. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
7.25. Nas exceções, permitir definir operadores “AND” e “OR”.
7.26. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
7.27. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
7.28. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por politicas.
7.29. Permitir criar regras de exceções por endereços IPs de origem.
7.30. Permitir criar regras de exceções por endereços IPs de destino
7.31. Permitir criar exceções por grupo de usuários.
7.32. Permitir criar exceções por categorias de sites.
7.33. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.
7.34. Ter grupos de categorias pré-configuradas na solução apresentando nomes

sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras.

7.35. Permitir editar grupos de categorias pré-estabelecidos pela solução.

7.36. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

7.36.1. Nome da regra;

7.36.2. Permitir criar uma descrição para identificação da regra.

7.36.3. Ter a possibilidade de classificação de pelo menos:

7.36.3.1. Produtivo;

7.36.3.2. Não produtivo;

7.36.3.3. Permitir aplicar Traffic shaping diretamente na categoria.

7.36.3.4. Na especificação das URLs e dominios que farão parte da regra, deve-se permitir cadastrar por dominio e palavra chave.

7.36.3.5. Deve permitir importar uma base com dominios e palavras chaves na hora da criação da categoria, a base com informações de dominios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.

7.36.3.6. Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista dominios que poderá ser mantida pelo administrador ou um terceiro.

7.37. Ter função para criar grupos de URLs.

7.38. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.

7.39. Permitir o administrador poder especificar um certificado autoritario próprio para ser utilizado no escaneamento HTTPS.

7.40. Deve permitir que em uma mesma politica seja aplicada ações diferentes de acordo com o usuário autenticado.

7.41. Nas configurações das politicas, deve-se existir pelo menos as opções de: Liberar categoria/URL, Bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.

7.42. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.

7.43. Permitir criar cotas de navegação com os seguintes requisitos:

7.43.1. Tipo do ciclo, especificando se o limite será por duração de acesso a internet ou se será especificado uma data limite para o acesso.

8. Controle e Segurança de Aplicações

8.1. Prover controle para mais de 2700 aplicações diferentes.

8.2. Controlar aplicações baseadas em categorias, caracteristica(Ex: Banda e produtividade consumida), tecnologia(Ex:P2P) e risco.

8.3. Permitir criar regras de controle por usuário e hosts.

8.4. Permitir realizar traffic shaping por aplicação e grupo de aplicações.

8.5. Possibilitar que as regras criadas baseadas em aplicação permitam:

8.5.1.Bloquear o trafego para as aplicações

8.5.2.Liberar o trafego para as aplicações

8.5.3.Criar categorização das aplicações por risco:

8.5.3.1. Risco muito baixo

8.5.3.2. Risco baixo

8.5.3.3. Risco medio

8.5.3.4. Risco alto

8.5.3.5. Risco muito alto

8.5.4. Permitir visualizar as aplicações por suas caracteristicas, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneraveis, que geram perda de produtividade, entre outras.

8.5.5. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes , entre outros.

8.6. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube mas bloquear o upload de videos, e etc.

8.7. Permitir agendar um horário e data especifico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

9.

10. Proteção de Redes

11. Prôver funcionalidade de Intrusion Prevention System (IPS)

11.1. Proporcionar alta performance na inspeção dos pacotes

11.2. Possuir mais de 7000 mil assinaturas conhecidas.

11.3. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.

11.4. Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.

11.5. Possuir funcionalidade Anti-DoS.

11.5.1. Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:

11.5.1.1. SYN Flood

11.5.1.2. UDP Flood

11.5.1.3. TCP Flood

11.5.1.4. ICMP Flood

11.5.1.5. IP Flood

11.6. Possuir tamplates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ, e etc.

11.7. Possuir proteção contra spoofing.

11.8. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.

11.9. Possuír funcionalidade para o administrador poder criar bypass de DoS.

11.10. Permitir o administrador clonar tamplates existentes para ter como base na hora da criação de sua politica customizada.

12. Possuir proteção avançada contra ameaças persistentes (APT)

12.1. Detectar e bloquear trafico de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.

12.2. Possuir logs e relatórios que informem todos eventos de APT.

12.3. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.

12.4. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.

13. Proteção para Emails

14. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.

14.1. Possuir serviço de reputação para monitoramento dos fluxos dos emails, sendo assim, o antispam deverá bloquear emails considerados com má reputação na internet e

pelo fabricante.

14.2. Bloquear SPAN e MALWARES durante a transação SMTP.

14.3. Possuir duas engines de antivirus para duplo escaneamento.

14.4. Ter proteção em tempo real, a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos emails que passam pela solução e assim tomar ações automáticas de segurança caso necessário.

14.5. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.

14.6. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloquea-los caso estejam em anexo.

14.7. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customiza-los de acordo com o desejado.

14.8. Ter suporte a criptografia TLS para SMTP, POP e IMAP.

14.9. Ter a possibilidade de agregar RBLs do fabricante e terceiras para ajudar na composição de segurança da ferramenta.

14.10. As ações dos emails considerados SPAN devem ser:

14.10.1. Drop

14.10.2. Warn

14.10.3. Quarantine

14.11. Poder definir um prefixo no subject de cada email considerado SPAM, como por exemplo: [SPAN] Marketing etc etc etc.

14.12. Permitir visualizar os emails que encontram-se na fila para serem enviadas.

14.13. Possuir funcionalidade que permita a adição de um banner no final dos Emails analisados pela solução.

14.14. Possuir funcionalidade de allowlist e blocklist.

14.15. Possuir funcionalidade que rejeite emails com HELO invalido e/ou que não possuam RDNS.

14.16. Permitir que o escaneamento seja feito tanto para emails de entrada quanto para os de saida.

15. Quarentena de Email

15.1. Possuir quarentena para os emails e opções de notificações para o administrador.

15.2. Emails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.

15.3. O usuário deve poder gerenciar sua querentena de emails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.

15.3.1. As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.

15.3.2. Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.

16. Possuir funcionalidade de criptografia de emails e DLP para os dados

16.1. Possuir funcionalidade de encriptação de emails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.

16.1.1. Os emails criptografados poderão ter seu conteúdo armazendo em um arquivo PDF.

16.1.2. Ter como funcionalidade a possibilidade de o usuário poder registrar sua própria senha de segurança para que seja possível abrir os emails criptografados.

16.1.3. Possuir também funcionalidade para geração de senhas aleatórias para

desencriptação do conteúdo.

16.1.4. Permitir enviar anexos junto aos emails criptografados.

16.1.5. Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não deve-se utilizar qualquer software adicional, plugin, ou client instalado no equipamento.

16.2. Possuir funcionalidade de DLP nos Emails

16.2.1. A engine de DLP deve ser automatica na hora de escanear os emails e anexos, assim identificando todos os dados sensíveis encontrados no email sem qualquer intervenção.

16.2.2. Possuir tamplates de dados considerados sensíveis pré-estabelecidos pelo fabricante (CCLs) com os padrões PII,PCI,HIPAA, com a intenção de ajudar o administrador na criação das regras desejadas e seguir as principais normas do mercado, elas deverão ser mantidas pelo fabricante.

16.2.3. Ter a opção de criar exceções individuais para cada tipo de situação.

16.2.4. As regras devem corresponder para as redes de origem e alvos especificos como a especificados por URLs.

16.2.5. Suporte a operadores lógicos

16.2.6. Poder definir tamanho máximo para escaneamento.

16.2.7. Permitir bloquear e liberar ranges IP.

16.2.8. Suporte para utilização de Wildcards

16.2.9. Anexar automáticamente um prefixo/sufixo para autenticação.

17. Proteção para proteção de servidores WEB (WAF)

17.1. Possuir funcionalidade de proxy reverso

17.2. Possuir engine de URL hardening e prevenção a directory traversal.

17.3. Possuir engine Form hardening.

17.4. Proteção contra SQL injection

17.5. Proteção contra Cross-site scripting

17.6. Possuir duas engines de antivirus disponíveis para analise de malware.

17.6.1. Permitir definir o fluxo que o antivirus irá atuar, se será no upload ou download.

17.6.2. Permitir limitar o tamanho máximo em que o antivirus irá atuar.

17.6.3. Permitir bloquear conteúdo considerado unscannable.

17.7. Possuir HTTPS (SSL) encryption offloading.

17.8. Proteção para cookie signing com assinaturas digitais.

17.9. Possuir Path-based routing.

17.10. Suporte ao protocolo do Outlook anywhere.

17.11. Possuir autenticação reversa para acesso aos servidores web.

17.11.1. Permitir criar tamplates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.

17.12. Ter abstração de servidores virtuais e físicos.

17.13. Proporcionar função de load balancer para que os visitantes possam ser jogados para diversos servidores de forma transparente.

17.14. Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.

17.15. Bloquear clients com má reputação.

17.16. Bloquear protocolos com anomalias.

17.17. Limitar numero de requisições.

18. Proteção de Sandbox na nuvem

18.1. Prover ambiente de sandbox na núvem provido pelo próprio fabricante.

18.2. Realizar inspeções de executáveis e documentos que possuam conteúdo

executáveis.

18.3. Possuír suporte aos principais executáveis windows como: **.exe, .com e .dll**

18.4. Possuir suporte aos principais documentos do Word como: **.doc, .docx, .docm e .rft.**

18.5. Realizar analise em documentos PDF.

18.6. Realizar analise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: **ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet**

18.7. Suporte a mais de 20 tipos de arquivos e extensões.

18.8. Realizar analises dinamicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.

18.9. Relatórios detalhados das ameaças bem como visibilidade dos alertas na dasheboard da solução.

18.10. O tempo em média das analises devem ser menores do que 120 segundos.

18.11. Suportar a analise de links de download em tempo real.

18.12. Permitir escolher pelo menos duas regiões para as quais os arquivos para analise devem ser enviados.

18.12.1. Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para analisa.

18.13. Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.

18.14. O appliance deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalide de sandbox.

19. Centralizador de gerenciamento

19.1. A solução deverá prôver uma ferramenta distribuida pelo mesmo fabricante para gerenciamento centralizado de todos os appliances adquiridos pela contratante.

19.2. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar politicas de gerenciamento para um ou mais equipamentos e aplica-los todos de uma única vez.

19.2.1. As politicas de configurações devem ter no minimo as seguintes opções:

19.2.1.1. Proteção e politicas de acesso web

19.2.1.2. Controle de aplicativos

19.2.1.3. IPS

19.2.1.4. VPN

19.2.1.5. Email

19.2.1.6. Firewall

19.3. A solução deverá oferecer funcionalidade que permita o administrador criar tamplates de configuração para que o administrador possa aproveitar as mesmas regras para novos appliances.

19.4. Deverá haver na dasheboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.

19.5. Possuir multiplas formas de customização de warning thresholds.

19.6. Possuir flexibilização na hora da criação de grupos de appliances gerenciados, sendo possível diferencia-los como por exemplo: Região, modelo e ou outro parâmetros.

19.7. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos com diferentes funções.

19.8. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

19.9. Deve ser possível integrar tanto com appliances físicos quanto virtuais.

19.10. Possuir funcionalidade que permita o centralizador de gerencia, também gerenciar

os updates de firmware de todos os appliances.

19.11. O gerenciador poderá ser oferecido como hardware appliance oferecido pela fabricante, virtual, onde permite a contratante instalar ele em um ambiente virtual e software, permitindo o software ser instalado em um hardware baseado em intel.

19.12. Poder gerenciar até 1000 appliances em uma única console.

20. Ferramenta de relatórios centralizado

20.1. Permitir que todos os appliances do fabricante possam centralizar seus relatórios em um único appliance especializado para esta função.

20.2. Permitir a customização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.

20.3. Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via email para todos os emails cadastrados.

20.4. Ter relatórios customizados e em compliance com pelo menos estes orgãos: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA.

20.5. Ter facil identificação das atividades de rede e ataques em potêncial.

20.6. Armazenar histórico dos relatórios em disco local.

20.7. Possuir relatórios unicos para cada um dos módulos ofertados pela solução.

20.8. Possuir multi-formato de relatórios, pelo menos tabular e gráfico.

20.9. Permitir exportar relatórios para: PDF, Exchel e HTML.

20.10. Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipedia, Rediff,eBay.

20.11. Possuir relatórios que informem principais atividades em cada módulo.

20.12. Ter logs em tempo real.

20.13. Ter logs arquivados para consulta posterior.

20.13.1. Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.

20.14. Possuir logs de auditoria.

20.15. Ter sua gerencia totalmente baseada em acesso web.

20.16. Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades especificas na ferramenta.

20.17. Possuir multiplas dasheboards onde deve-se haver uma exclusivamente para os relatórios e outro exclusivamente para tratar dos recursos e saude do appliance.

20.18. Deve-se detectar automaticamente um equipamento do mesmo fabricante quando este reportar-se ao centralizador de relatórios, onde o administrador do sistema poderá dar um aceite ou não neste appliance que esta realizando a tentiva de integração.

20.19. Permitir agrupamento dos equipamentos por tipo do dispositivo e modelo do equipamento.

20.20. O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.

20.21. Possuir gerenciamento somente de appliances favoritos.

20.22. Ter total gerencia sobre a retenção dos dados armazenados neste equipamento.

20.23. Ter disponibilidade em appliance virtual e software caso necessário instalar o appliance em um hardware baseado em intel.

20.23.1. Possuir suporte no mínimo aos virtualizadores:

20.23.1.1. Vmware

20.23.1.2. Hyper-V

20.23.1.3. Citrix

20.23.1.4. KVM

20.23.2. Possuir capacidade de armazenamento ilimitado, tendo apenas o disco como limitador.

21. Serviços

21.1. Possuir atendimento e suporte multi idiomas, inglês, espanhol e Portugues(BR), seguindo o horário oficial de Brasilia.

21.2. O fabricante e distribuidor devem possuir uma base de conhecimento bem estabelecida para que a contratante possa consultar e informar-se sobre o produto contratado.

21.3. Possuir painel para abertura de chamados com o distribuir para que a equipe de suporte possa prestar auxilio e orientação para a contratante em caso de problemas ou dúvidas na solução caso necessário.

21.3.1. Caso haja necessidade, a contratante poderá solicitar conexão remota de um técnico em seu ambiente tendo como objetivo agilizar a prestação do suporte requisitado.

21.4. A contratante poderá requisitar ao contratado total apoio para acessar documentações e orientações para realizar as melhores práticas nas configurações e deploy da solução em seu ambiente.

21.5. A contratada deverá ter suporte em horário comercial (10x5) e ter a possibilidade de atendimento fora do horário comercial e caráter emergêncial.

21.6. Possuir pelo menos 4 DDDs em diferentes regiões para contato telefonico.

21.7. Ter uma SLA para inicio de atendimento de no máximo 4 horas.

21.8. O distribuidor e fabricante devem proporcionar treinamentos online de seus produtos bem como proporcionar certificados oficiais do fabricante para a contratante.

21.9. O distribuidor deverá ser um centro de treinamentos oficial da fabricante.

21.10. A contratada deverá ter a possibilidade para realizar todo o processo de RMA de um equipamento que estiver dentro do periodo contratado e apresentar falhas que sejam constatados pela equipe de suporte como irreparáveis.

21.11. A contratada deverá oferecer uma modalidade de suporte adicional caso a contratante necessite de qualquer serviço adicional que não esteja especificado na guia de serviços deste documento.

LOTE 06 – CABOS DE CONECTIVIDADE

16 CABOS SFP+ DAC 3MTs PASSIVO

24 x Patch Cord RJ-45 Cat 6 3MTs Certificado - Azul Padrão de montagem: T568A

24 x Patch Cord RJ-45 Cat 6 3MTs Certificado - Cinza Padrão de montagem: T568A

24 x Patch Cord RJ-45 Cat 6 3MTs Certificado - Vermelho Padrão de montagem: T568A

24 x Patch Cord RJ-45 Cat 6 3MTs Certificado - Verde Padrão de montagem: T568A

SERVIÇOS DE IMPLANTAÇÃO VÁLIDO PARA TODOS OS LOTES

SERVIÇO DE IMPLANTAÇÃO DAS SOLUÇÕES:

Para todos os lotes deverá ser desenvolvido um cronograma inicial de atividades contemplando os serviços de implementação da parte física das soluções ofertadas.

Após a instalação e configuração deste cronograma, deverá ser executado os serviços lógicos da

seguinte forma:

- Planejamento;
- Análise;
- Dimensionamento de Infraestrutura;
- Conectividade dos equipamentos;
- Configurações;
- Testes e validações;
- Monitoramento e controle.

Instalação física dos equipamentos:
• Todos os equipamentos devem ser instalados em local definido pela Prefeitura Municipal de Canela, Rua Dona Carlinda, 455 – Centro – Canela/RS, obedecendo a norma TIA-942, onde deverão contemplar todas as réguas de energia, calhas, guias de cabo, bandejas entre outros componentes necessários a instalação completa.

Condições gerais:
Todo o trabalho de migração deverá ser feito de forma que ocasione o mínimo de impacto para os usuários da rede.
Todos os serviços deverão ser executados em horário comercial, salvo situações onde a infraestrutura não permita. Nestes casos será agendado com o cliente de forma antecipada e não haverá cobrança adicional.
Será fornecido repasse de conhecimento para equipe de TI, para até quatro pessoas mediante entrega da documentação personalizada.

Todos os custos com deslocamento, estadia, alimentação e similares serão pagos pela Contratada.
Após a entrega definitiva do projeto e o aceite do cliente, deverá ser oferecido para os serviços realizados, suporte técnico para a nova infraestrutura durante 120 dias.