**DESCRITIVO SONDA VIRTUAL WORKSPACE**

ÍNDICE

1. Versão do Produto 3

2. Descrição Resumida 3

3. Objetivo 3

4. Benefícios 3

4.1. Diferenciais Comerciais 3

5. Escopo de Atuação 3

5.1. Arquitetura 4

5.2. Recursos Computacionais 4

5.3. Rede 4

5.4. Backup 5

6. Ofertas 6

7. Segurança 6

7.1. Notificação de Incidente de Segurança 9

8. Monitoramento 9

9. Premissas e Requisitos 9

10. Matriz de Responsabilidade 10

10.1. Matriz de Responsabilidade SVW 10

10.2. Matriz de Responsabilidades – Serviços Gerenciados 10

11. Requisição de Serviços 11

12. Nível de Serviço 11

1. Versão do Produto

|  |  |  |
| --- | --- | --- |
| **Versão** | **Escopo** | **Data de Atualização** |
| Versão 01 | Criação do documento | - |

1. Descrição Resumida

O **SONDA** Virtual Workspace (SVW) é um serviço que oferta a infraestrutura de Desktops como serviço (DaaS), que permite ao usuário acessar o ambiente virtualizado através de navegador web, utilizando o protocolo HTML5. O acesso pode ser realizado a partir de múltiplas plataformas e sistemas operacionais.

A solução permite acesso a aplicações de diferentes sistemas operacionais, como Windows e Linux, de maneira simultânea.

1. Objetivo

O SVW tem como objetivo implementar um novo modelo de trabalho de desktops associado as demandas de mobilidade, flexibilidade e agilidade, utilizando de infraestruturas de TI baseadas na Cloud **SONDA**. Ele visa empregar um novo conceito de uso, padronizando as áreas de trabalho de usuários, simplificando o suporte e ofertando maior segurança aos dados da organização.

1. Benefícios

Os benefícios do serviço SVW são:

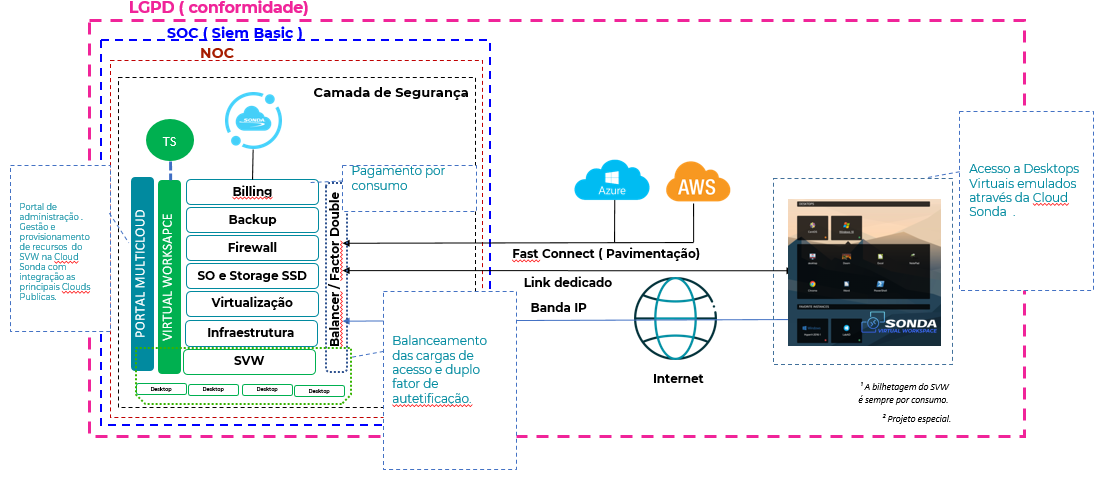
* Padronização dos ambientes de Desktops por perfil de usuário;
* Acesso utilizando o AD do **CLIENTE**;
* Múltiplo fator de autenticação;
* Padronização de suporte simplificando e automatizando a solução de problemas;
* Ambiente gerenciável e escalável;
* Performance estável através de balanceadores de carga para conexões novas e ativas;
* Maior segurança dos dados das estações de trabalho;
* Redução de custos com aquisição de equipamentos de alta performance;
* Eliminação do uso de VPN;
* Iniciativas inovadoras como “Traga seu próprio dispositivo” (BYOD).
  1. Diferenciais Comerciais
* Uso de vários módulos (Web, Linux, Windows) de maneira simultânea;
* Customização da marca do **CLIENTE** na plataforma;
* Utilização de infra certificada pelas normas ISO 27017 e 27018;
* Gestão de monitoramento proativo;
* Possibilidade de uso do múltiplo fator de autenticação de preferência do **CLIENTE**.

1. Escopo de Atuação

A plataforma SVW utiliza a infraestrutura da Cloud **SONDA** em sua implementação, com isto temos um ambiente escalável, seguro e com todo o suporte de profissionais altamente capacitados.

* 1. Arquitetura

Seguindo o conceito de Alta Disponibilidade, a Infraestrutura está disponibilizada em cluster, garantindo a disponibilidade dos servidores virtuais em caso de falhas em hosts que suportam o ambiente do SVW. Além disso, possui integração com as ferramentas de Monitoramento, ITSM, Backup e segurança.



* 1. Recursos Computacionais

**Licenciamento e Serviços**

As licenças e serviços incluídos nas máquinas virtuais que suportam o ambiente do SVW são:

* Plataforma de Virtualização (VMware);
* Plataforma de Orquestração e automação de Workspace;
* Sistema Operacional;
* Antivírus;
* Snow (Gestão de Licenciamento);
* Onetouch (Command Center, licenças de CA e sistema de suporte);
* Equipe de gestão do ambiente Cloud;
* vCPU;
* vRAM;
* Disco Virtual (GB);
* Backup.
  1. Rede

O endereçamento de rede para ativação do **CLIENTE** será definido durante o planejamento do projeto.

As redes dos **CLIENTES** serão de prefixo /26 (totalizando 60 IPs disponíveis para uso). Para ambientes com necessidade de maior alocação de endereços, será necessário avaliar o projeto com a **SONDA**.

A instância virtual terá duas interfaces de rede. A primeira interface atende a rede de produção e segunda interface atende a rede de monitoramento/gerenciamento da **SONDA**.

Endereços IP Públicos – usados para comunicação de entrada (através de NAT), com a internet. Não é possível atribuir um endereço público a uma interface de rede virtual.

Endereço IP Privados – usados para comunicação entre instâncias virtuais, rede local e a internet (através de NAT). A instância virtual terá um endereço IP de produção e de monitoramento/gerenciamento.

O método de alocação de IP privado padrão é dinâmico, o endereço IP é alocado quando a instância é criada.

* 1. Backup

Uma política de Backup ao ser construída leva em consideração três variáveis: Tipo de Dados, Categoria do Backup e Retenção do Backup. Essas variáveis combinadas constituem uma política que entrega RPO[[1]](#footnote-1) e RTO[[2]](#footnote-2) específicos e aderentes às mais diversas características de negócio e/ou aplicações.

**Tipo de Dados**

* Cada dado e aplicação deve ser tratada de forma diferente, de acordo com suas características e necessidade, e o tipo de dados considerado para o SVW é o Backup de Servidor Virtual.

**Categoria do Backup**

* A categoria do Backup evidencia a criticidade para realização do backup e o nível de serviço desejado pelo **CLIENTE** na prestação dos serviços.

**Retenção**

* As retenções de um Backup levam em consideração o período em que determinada informação fica armazenada dentro do dispositivo de armazenamento de dados. Definimos a retenção da seguinte maneira:
  + Baixa: com períodos de curto prazo normalmente até 30 dias – (Armazenamento realizado em backup para disco – object storage);
  + Média: Retenções de médio prazo com até 12 meses (Armazenamento realizado em ambiente object storage);
  + Longa: Retenções de longo prazo de até 5 anos (armazenamento realizado em ambiente object storage).

**Cópias de Segurança**

Os backups são realizados através de um Grid que possui 3 nodes (cada node em locais diferentes) replicados entre eles. Em caso de indisponibilidade de 1 dos nodes os dados poderão ser acessados pelos outros 2 nodes.

**Criptografia do backup**

* Armazenamento de dados.
  + Os dados armazenados em disco são gravados deduplicados pela ferramenta de backup e só podem ser reintegrados (acessados como arquivos) com acesso a base de deduplicação;
  + Os dados armazenados em Fita Física possuem criptografias que são realizadas através do robô durante o processo de gravação sendo permitido a leitura destes dados apenas pelo robô que realizou a criptografia dos dados.

**Políticas**

* As opções de políticas de backup disponíveis para seleção através do portal são:
  + Sem Backup (caso o **CLIENTE** opte por não contratar o backup);
  + Baixa;
  + Média;
  + Longa.
* Backup para servidor virtual.

1. Ofertas

O **SONDA** Virtual Workspace é oferecido de acordo com a quantidade de usuários que terão acesso ao ambiente, com base nisto é criada a infraestrutura necessária para atender os requisitos na Cloud **SONDA**.

Por definição o ambiente deverá ser planejado com a quantidade múltipla de cinquenta usuários, por exemplo, sendo necessários acesso de 95 usuários, o ambiente deverá ser planejado para 100 usuários.

O SVW tem a oferta mínima de 50 usuários, o aumento do ambiente deverá considerar o incremento mínimo de 50 usuários por upgrade.

Para cada usuário é necessário contratar uma licença de Windows RDS.

Para este produto, são definidos os ranges com a quantidade de usuários padrão, baseados em vCPU e memória, conforme quadro abaixo:

|  |  |  |
| --- | --- | --- |
| **Quantidade Usuários** | **vCPU** | **vRAM** |
| 50 | 15 - 20 | 30 - 40 |
| 100 | 30 - 40 | 60 - 80 |
| 150 | 45 - 60 | 90 - 120 |
| 200 | 60 - 80 | 120 - 160 |
| 250 | 75 - 100 | 150 - 200 |
| 500 | 120 - 160 | 240 - 320 |
| 1000 | 300 - 400 | 600 - 800 |

1. Segurança

Os Serviços de Segurança Gerenciados da **SONDA** têm como objetivo o princípio de defesa em profundidade onde é aplicado em cada camada, tecnologia, processos e controles baseados no framework CIS (Center of Internet Security Framework) e a na norma ISO/IEC 27000.

Este produto engloba os itens de Segurança listados abaixo:

* **Certificado**

A Cloud **SONDA** possui um certificado SSL[[3]](#footnote-3) válido, no qual todas as requisições HTTP[[4]](#footnote-4) são redirecionadas para HTTPS[[5]](#footnote-5), incluindo todos os subdomínios e hostnames.

O HTTPS ajuda a evitar que dados sejam alterados durante a comunicações entre os websites e os navegadores dos usuários, garantindo:

* + Integridade: garante que as mensagens não foram alteradas durante comunicação;
  + Confidencialidade: a mensagem será lida apenas pelo destinatário real;
  + Autenticação: comprovação de que o servidor é realmente o servidor esperado.
* **Criptografia**

A criptografia no HTTPS funciona com um par de chaves, sendo uma chave pública e outra privada. Cada vez que um usuário solicita uma conexão ao site, o servidor envia a chave pública para este usuário. Com esta chave, o usuário tem a garantia de que toda a comunicação chegará apenas para o servidor, já que a chave privada se encontra no servidor.

* **EndPoint Protection**

É importante manter sua instância segura, como padrão, as instâncias virtuais com o Sistema Operacional Windows e Linux contam com a solução de Endpoint Protection.

* **Identidades gerenciadas**

O gerenciamento das credenciais de acesso dos profissionais **SONDA** é realizado através de uma solução de cofre de senha que fornece uma maneira de armazenar com segurança as credenciais.

Nossos analistas e especialista não conhecem e não tem posse da senha para autenticar nas instâncias virtuais. A senha é alterada após cada solicitação de uso.

Nota: Para os acessos do **CLIENTE** no portal Cloud **SONDA** é realizado o levantamento e criação em fase de projeto. Para resolução de problemas, criação, alteração ou exclusão de usuário na Cloud **SONDA** deve ser aberto um chamado por profissionais autorizados do **CLIENTE**.

* **Política de senha do usuário**

A construção de qualquer senha deve considerar o uso e a composição entre caracteres alfabéticos, maiúsculos, minúsculos, números e alfanuméricos. Toda senha deve ter no mínimo 14 (quatorze) caracteres, por exemplo: Abcd$125de3647. A senha não poderá repetir nenhuma das últimas 13 (treze) senhas já previamente utilizadas.

* **Controle de acesso baseado em função**

Podemos segmentar as tarefas dentro da equipe e permitir apenas as ações necessárias baseada na função.

* **Anti-DDoS**

A **SONDA** atua com uma solução de Anti-DDoS[[6]](#footnote-6) on-premise para mitigação de ataques de aplicação tais como: TCP Syn Flood, TCP RST Flood, TCP FIN Flood, TCP ACK Flood, ICMP Flood, UDP Flood, UDP Amplify.

Além disso, quando um ataque volumétrico de grande escala é iniciado, o “Scrubing Center” da **SONDA** é acionado – um centro de mitigação de ataques localizado fora do Data Center - que desvia todo o tráfego para este centro. A partir disso, o que é considerado ataque será descartado e o tráfego válido será devolvido para a rede e encaminhado normalmente para o destino.

* **Firewall e IPS**

Utilizamos um firewall “next generation”, que contribui para a capacidade do serviço de prevenir, detectar e responder a incidentes de segurança. Além de ser responsável pela configuração e segurança da rede.

A proteção aplicada permite filtrar as comunicações por aplicação, atuando diretamente na Camada 7. Desta forma, o firewall consegue identificar os tipos de aplicação e conexão que trafegam no ambiente e inferir se esses casos tratam de acessos legítimos ou não.

Para cada **CLIENTE** será entregue um domínio virtual dedicado de Firewall com as seguintes características:

|  |  |
| --- | --- |
| **Indicadores Máximos por CLIENTE** | **Valores** |
| Firewall Throughput (Pacotes UDP) | 100Mbps |
| Sessões Concorrentes (TCP) | 380k |
| Novas Sessões/Segundo (TCP) | 1800 |
| Máximo regras de controle de tráfego | 100 |
| Máximo VPNs (site-to-site) | 20 |
| Máximo VPNs (client-to-site) | 100 |
| Limite de banda internet | Mínimo 2 Mbps |
| Máximo IPs públicos realizando NAT estático 1 para 1 (não será implementado PAT) | 4 IPs |

Para qualquer configuração fora dos padrões acima, é necessário a análise do projeto para definição de arquitetura (projeto especial).

Como forma de complementar à análise, são aplicados o IDS (Sistema de Detecção de Intrusão) e o IPS (Sistema de Prevenção de Intrusão) no ambiente, a fim de avaliar as assinaturas de todas as conexões e identificar possíveis acessos indevidos.

* **Segurança Física**

O Data Center **SONDA** possui equipe de segurança física em Regime 24x7, Portaria Blindada, Controle de Acesso em todas as portas, sendo a entrada no Data Center controlada com dupla autenticação (Cartão + Biometria), Mais de 100 Câmeras de alta resolução em todo a edificação além de sistema de Monitoramento e Gravação de Imagens.

* **Segurança de Rede Interna – SONDA**

A infraestrutura de rede interna da **SONDA** conta com vários recursos para garantir a segregação de seus **CLIENTES e** dados, com uma arquitetura preparada para um ambiente multi locatário.

* 1. Notificação de Incidente de Segurança

Incidente de segurança é qualquer ocorrência que possa comprometer o bom andamento dos sistemas da **SONDA** e dos seus **CLIENTES.** Exemplos incluem o uso não autorizado de senhas, a adulteração de informações em um banco de dados, o envio ou recepção de mensagens ameaçadoras, roubo de informação, ocorrência de vírus, ou qualquer outro fato que contrarie as disposições dessa política.

Qualquer incidente de segurança deve ser reportado à Equipe de Segurança de informação através do e-mail [segurancainfo.qualidade@sonda.com](mailto:segurancainfo.qualidade@sonda.com).  
Os incidentes recebidos por este canal serão analisados pela equipe de Segurança da Informação da **SONDA**, de acordo com as diretrizes organizacionais e melhores práticas internacionais.

1. Monitoramento

Para uma gestão preventiva e preditiva a **SONDA** disponibiliza artefatos para que o **CLIENTE** possa ficar seguro tendo a certeza que o ambiente é gerido e acompanhado a todo instante pela equipe **SONDA**. É disponibilizada a ferramenta de Enterprise Application Integration (EAI) para abertura automática de chamados ao detectar qualquer anomalia no ambiente e a ferramenta DEVOPS de Dispacher Automatico para encaminhar para a equipe responsável pela tratativa, diminuindo o tempo de resposta de qualquer anormalidade apresentada.

Todas as instâncias virtuais criadas são monitoradas continuamente, possibilitando a análise de disponibilidade (up/down) e capacidade (cpu, memória e disco) dos servidores.

1. Premissas e Requisitos

Abaixo são listadas as premissas e restrições do serviço:

* É necessário que o **CLIENTE** possua um AD (Active Directory), para autenticação com o SVW;
* A licença do Sistema Operacional é de responsabilidade **SONDA** não podendo utilizar a licença do **CLIENTE**;
* Nos servidores Windows onde o licenciamento é de responsabilidade da **SONDA**, não é necessário adquirir a Cal de acesso para conexão a estes servidores;
* Todo software Microsoft instalado no ambiente do SVW, deve ter as suas licenças adquiridas junto a **SONDA**;
* As configurações de DNS podem ser realizadas de duas formas:
  + Opção 1 – DNS ser configurado nos servidores da **SONDA**:
    - Neste caso, o **CLIENTE** deverá fornecer as zonas e os registros a serem configurados e atualizar os registros no Registro.br, sendo esta atualização de responsabilidade do **CLIENTE**.
  + Opção 2 – DNS não ser configurado nos servidores da **SONDA:**
    - Neste caso, o **CLIENTE** deverá atualizar as zonas com o endereço IP fornecido pela **SONDA**.
* A banda escolhida é compartilhada para a solução e não por máquinas virtuais;
* A solução não contempla Link Dedicado, a banda IP deve ser adquirida como serviço **SONDA**;
* Os acessos às máquinas virtuais só poderão ser realizados via VPN (Client-to-Site e/ou Site-to-Site);
* Não é possível reduzir o tamanho de um disco virtual;
* Disco virtual não pode ser compartilhado entre duas ou mais máquinas virtuais simultaneamente;
* O “resize” de vCPU e vGB RAM do servidor virtual reinicia automaticamente a máquina virtual;
* A reserva de recurso computacional (vCPU/vGB RAM) por servidor virtual não é permitida;
* Caso o **CLIENTE** exclua a instancia virtual, o mesmo tem até 24 horas para restaurar através do portal se necessário. Caso tenha passado o período de 24 horas após a exclusão, para retornar com as informações será necessário abrir uma requisição na **SONDA** para restaurar o backup e recuperar os dados. A quantidade de restore será limitada de acordo com a política de Backup contratada;
* Caso seja necessário efetuar o restore de um servidor por falha na infraestrutura da **SONDA**, o procedimento de restauração será o mesmo contemplado no item anterior, porém sem limitação de quantidade de restore;
* Caso o **CLIENTE** solicite a gestão compartilhada do recurso o mesmo assume os riscos operacionais e de segurança do ambiente em procedimentos que seus colaboradores executarem, e também ficará responsável pelo licenciamento das ferramentas que forem instaladas posteriormente a entrega;
* Caso a versão do Sistema Operacional e/ou do Banco de dados deixar de ter suporte pelo o fabricante o **CLIENTE** deve disponibilizar os pré-requisitos e recursos para a atualização da versão;
* Caso o **CLIENTE** necessitar de utilizar SO que não tenha mais suporte pelo o Fabricante a **SONDA** não garante a completude e funcionamento correto dos serviços ofertados, será emitido Carta de Risco;
* Para qualquer atividade de requisição fora do item Requisições de Serviços deste documento deverá ser negociado e o **CLIENTE** deverá apresentar procedimento e validá-lo em conjunto com a **SONDA**.
* O ambiente deverá ser configurado com perfil móvel de dados, para que o usuário tenha acesso a todos os seus dados em diferentes hosts de conexão;
* A quantidade de usuários criados para acesso ao SVW deverá ser sempre inferior ou da mesma quantidade a capacidade contratada pelo **CLIENTE**.
* Será realizada mensalmente auditoria da quantidade de licenças de acesso, caso esteja acima do contratado, será realizada a cobrança da quantidade total de licenças SVW utilizadas.

1. Matriz de Responsabilidade

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASIC, onde: **R** - Responsável; **A** - Aprovador; **S** - Suporte; **I** – Informado e **C** – Consulta.

* 1. Matriz de Responsabilidade SVW

No quadro abaixo estão listadas as responsabilidades referentes ao Produto.

|  |  |  |  |
| --- | --- | --- | --- |
| **Contratação Opcional** | **Atividades** | **SONDA** | **CLIENTE** |
| Não | Aplicação de patches e fixes de correção e/ou segurança na infraestrutura da plataforma | R | A |
| Não | Instalação de S.O. | R |  |
| Não | Instalação do Banco de Dados | R |  |
| Não | Licenciamento de Antivírus | R |  |
| Não | Licenciamento do Sistema Operacional | R |  |
| Não | Gestão dos serviços NAT | R | S |
| Sim | Licenciamento do Banco de Dados | R | S |

* 1. Matriz de Responsabilidades – Serviços Gerenciados

No quadro abaixo está listado as responsabilidades dos Serviços de Gestão ofertados junto com o produto SVW:

|  |  |  |  |
| --- | --- | --- | --- |
| **Contratação Opcional?** | **Atividades** | **SONDA** | **CLIENTE** |
| Não | Atualização de Antivírus na infraestrutura da plataforma | R | I |
| Não | Configuração de Monitoramento e Antivírus na infraestrutura da plataforma | R |  |
| Não | Instalação de aplicação de negócio |  | R |
| Não | Licenciamento de Softwares instalados de terceiros |  | R |
| Não | Administração de Usuários / Permissão do Portal Cloud **SONDA** | R | S |
| Não | Análise de desempenho e performance da infraestrutura da plataforma | R | S |
| Não | Backup da Plataforma | R | S |

**Nota:**

* Requisições e Matriz de Responsabilidade de serviços relacionados à infraestrutura do **CLIENTE** se encontram no descritivo do produto específico.
* O **CLIENTE** pode ser o responsável pela gestão computacional do ambiente através do portal da Cloud **SONDA**.

Nos quadros acima existem atividades que são opcionais para o **CLIENTE**, ou seja, é permitido ao mesmo que escolha a **SONDA** como prestadora do serviço ou um outro parceiro. Para essas atividades a coluna “Contratação opcional” é preenchida com “SIM”. Portanto, toma-se como premissa, essas atividades como escopo padrão, sendo de responsabilidade do **CLIENTE** sinalizar caso não queira que elas sejam de responsabilidade da **SONDA**.

1. Requisição de Serviços

A tabela abaixo lista as requisições de serviços disponíveis para solicitações dos **CLIENTES** assim como seu tempo de solução e horário de cobertura.

|  |  |  |
| --- | --- | --- |
| **Requisição** | **Classificação** | **Tempo de Solução** |
| Criar máquina virtual | C | Conforme TS contratado /Via Portal |
| Remover máquina virtual | C | Conforme TS contratado /Via Portal |
| Criar disco virtual | B | Conforme TS contratado /Via Portal |
| Remover disco virtual | B | Conforme TS contratado /Via Portal |
| Alterar memória de máquina virtual | B | Conforme TS contratado /Via Portal |
| Alterar vCPU de máquina virtual | B | Conforme TS contratado /Via Portal |
| Criar, Modificar e Remover usuários e permissionamento | B | Conforme TS contratado |
| Criar, Modificar e Remover políticas de backup (Alterar retenção: Baixa / Média / Longa) | C | Gestão de Mudança |
| Solicitar disco acima de 2TB | B | Gestão de Mudança |

1. Nível de Serviço

|  |  |  |  |
| --- | --- | --- | --- |
| **Serviço** | **Nome** | **Descrição** | **Meta** |
| **SONDA** VIRTUAL WORKSPACE | Disponibilidade | Percentual de tempo que o serviço estará disponível, incluindo acessibilidade e funcionalidade, excluindo desse tempo as atividades de paralisação programada e demais exceções mencionadas em contrato. | 99,9 % |



1. **RPO** (Recovery Point Objective): Indicador utilizado para que a empresa saiba a quantidade de recursos mínimos a serem recuperados em caso de falhas ou perda de dados. [↑](#footnote-ref-1)
2. **RTO** (Recovery Time Objective): Indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha. [↑](#footnote-ref-2)
3. **SSL** (Secure Sockets Layer): Tecnologia global de segurança padrão que permite a comunicação criptografada entre um navegador da Internet e um servidor da web. [↑](#footnote-ref-3)
4. **HTTP**: Protocolo de comunicação entre sistemas de informação de hipermídia, distribuídos e colaborativos; a base da comunicação com a internet, também conhecida como World Wide Web, pois permite a transferência de dados entre redes de computadores. [↑](#footnote-ref-4)
5. **HTTP**S: Esse protocolo é a combinação dos protocolos HTTP e [SSL](https://www.rotamaxima.com.br/ssl-fator-rankeamento-seo/) (Secure Sockest Layers). Os motivos para o HTTPS ser considerado o mais seguro é porque ele faz a encriptação dos dados fornecidos, requer a autenticação dos servidores, dentre outras ferramentas que asseguram que os dados enviados e recebidos pelos usuários estejam seguros. [↑](#footnote-ref-5)
6. **Anti-DDoS**: Proteção completa contra DDoS na rede local e no backbone internet;

   **DDoS** (Distributed Denial of Service, em inglês) = DoS (Denial Of Service, em inglês) conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. A dirença entre DoS do DDoS é que do DoS envolve apenas 1 atacante quando o DDoS um computador mestre pode gerenciar até milhões de computadores atacantes. [↑](#footnote-ref-6)