



DESCRITIVO CLOUD SONDA

ÍNDICE

1. VERSÃO DO PRODUTO	3
2. DESCRIÇÃO RESUMIDA	3
3. OBJETIVO	3
4. BENEFÍCIOS	3
4.1. DIFERENCIAIS COMERCIAIS	4
5. ESCOPO DE ATUAÇÃO	4
5.1. ARQUITETURA	4
5.2. RECURSOS COMPUTACIONAIS	5
5.3. GESTÃO DE CAPACIDADE	6
5.4. REDE	6
5.5. STORAGE	6
5.6. BACKUP	7
6. OFERTAS	8
6.1. CLOUD SERVER	8
6.2. CLOUD SERVER SQL DB	9
7. SEGURANÇA	9
8. MONITORAMENTO	12
9. PREMISSAS E REQUISITOS	12
10. MATRIZ DE RESPONSABILIDADE	14
10.1. MATRIZ DE RESPONSABILIDADE CLOUD SONDA	14
10.2. MATRIZ DE RESPONSABILIDADES – SERVIÇOS GERENCIADOS	14
11. REQUISIÇÃO DE SERVIÇOS	15
12. NÍVEIS DE SERVIÇO	15

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-
Versão 02	Revisão de tecnologia	28/08/2025

2. Descrição Resumida

A Cloud **SONDA** é um ambiente de computação em nuvem, com características para atender às necessidades computacionais dos **CLIENTES**, com escalabilidade e elasticidade, permitindo ao **CLIENTE** aumentar ou diminuir os recursos disponíveis, pagando conforme alocação e/ou tempo de utilização.

O core da Cloud **SONDA** é voltado para *Continuous Automation*¹, que possibilita criar integração com as aplicações do **CLIENTE** (API/CLI), controle (políticas voltadas à gestão de identidade), provisionamento (instâncias e *blueprints*), conexões (hardware, network, storage) e solução de IaaS (*Infrastructure as a Service*) que oferece capacidade computacional na nuvem sob demanda.

A solução consiste no provisionamento de recursos de processamento (vCPU), memória (vGB) e armazenamento (GB), permitindo que cada **CLIENTE** tenha sua necessidade atendida de acordo com as instâncias virtuais ofertadas pela **SONDA**.

A Cloud **SONDA** possui integração avançada com o **SONDA** Hybrid, que amplifica a automação e orquestração de recursos em ambientes híbridos de Cloud Públicas e Privada. Com essa integração, as empresas podem provisionar, gerenciar e monitorar máquinas virtuais, armazenamento e redes de forma centralizada e automatizada. Essa abordagem integrada garante maior flexibilidade, reduzindo o tempo de resposta para o provisionamento de recursos e facilitando o gerenciamento de cargas de trabalho complexas.

3. Objetivo

O serviço tem como objetivos:

- Disponibilizar recursos computacionais em nuvem escalável à necessidade de negócio;
- Disponibilizar ao **CLIENTE** portal para gerenciamento dos serviços contratados;
- Satisfazer os requisitos de negócios do **CLIENTE** através de serviços disponíveis, confiáveis, escaláveis e seguros;
- Manter conformidade com os padrões da indústria;
- Cumprir com os níveis de serviços estabelecidos através dos SLAs;
- Agilizar o processo de criação de instâncias virtuais e componentes adicionais;
- Gestão de Governança baseadas nas melhores práticas (GDPR, HIPAA, ITIL, COBIT, ISO 20000, ISO 27001, ISO 27017, ISO 27018, TR3 e TIER III).

4. Benefícios

Os benefícios do serviço Cloud **SONDA** são:

- Gerenciamento das instâncias virtuais e componentes adicionais via portal de autosserviço;

¹ **Continuous Automation:** Prática de automatizar todos os aspectos do ciclo de vida de um aplicativo para construir e implantar software e mudanças de forma rápida, consistente e segura.

- Possibilidade de gerenciamento de múltiplos projetos, tenants, funções e automações, através do portal;
- Pré-visualização dos valores de recursos durante a fase de provisionamento (Showback);
- Cobrança mensal por alocação e/ou tempo de utilização, conforme tipo do recurso;
- Estimativa do valor do template escolhido a ser enviado na fatura, sem a necessidade de orçar o custo manualmente, evitando surpresas nas faturas;
- Flexibilidade dos recursos computacionais sem a necessidade de investimentos altos para compra e manutenção do hardware físico;
- Gestão de logs e auditoria;
- Para a infraestrutura que hospeda o Produto Cloud **SONDA** é realizada a retenção de logs conforme a norma ISO 27017, a qual a **SONDA** foi certificada, com isso é possível realizar a auditoria para rastreamento de acesso aos componentes da infraestrutura, bem como o portal da solução que possui duplo fator de autenticação promovendo maior segurança ao **CLIENTE**.

4.1. Diferenciais Comerciais

- Produto certificado pelas normas ISO 27017 e 27018;
- Todos os discos de Sistema Operacional e armazenamento são de alta performance (SSD) com custo acessível;
- Sem custo adicional para transferência de dados;
- Gestão de monitoramento proativo;
- Em caso de remoção de instâncias virtuais o próprio **CLIENTE** pode recuperar no período de 24h;
- Portal de Gestão de Capacidade (Uso de CPU, Memória e disco);
- Gestão otimizada dos custos por meio do **SONDA Hybrid**, com recomendações e comparações de preços entre nuvens públicas, desde que a comparação seja realizada entre itens idênticos e o **CLIENTE** tenha integração com o provedor de cloud desejado no **SONDA Hybrid**.

5. Escopo de Atuação

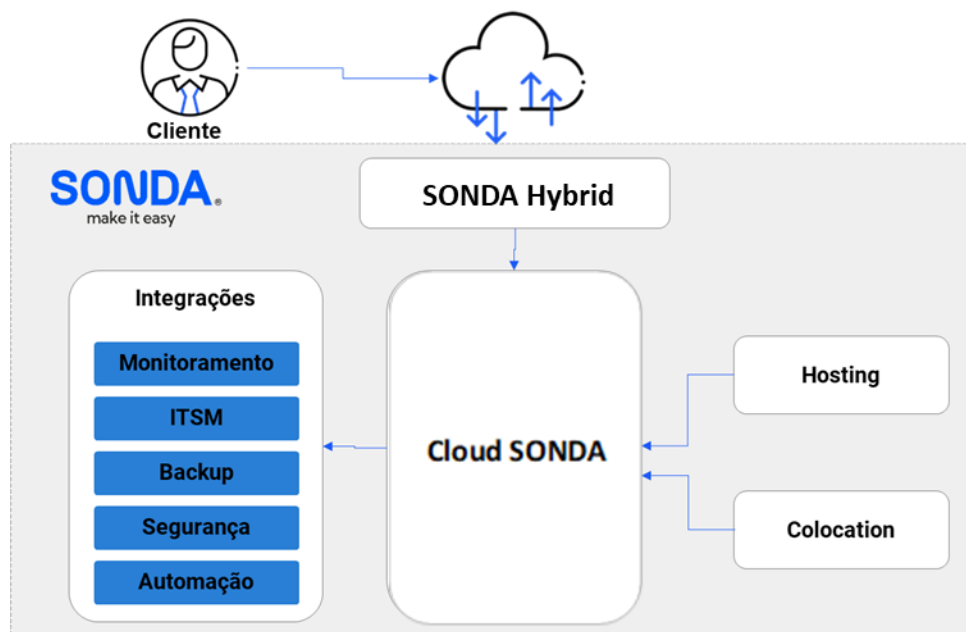
A solução de Cloud **SONDA** está implantada sob plataforma que mantém a confiabilidade, o desempenho e a segurança da infraestrutura de hosts para as instâncias virtuais.

Automatização e orquestração dos processos de governança e gestão do ambiente, possibilitando ao **CLIENTE**, por meio do portal, visualizar e interagir com seu ambiente contratado.

Cada instância virtual contempla, por padrão: Licenciamento, vCPU, vGB RAM, Sistema Operacional, Monitoramento e Segurança.

5.1. 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. Além disso, possui integração com as ferramentas de Monitoramento, ITSM, backup, segurança, entre outras.



5.2. Recursos Computacionais

- **Licenciamento e Serviços**

As licenças e serviços incluídos nas máquinas virtuais são:

- Plataforma de Virtualização;
- Sistema Operacional;
- SQL Server (Em caso de máquina virtual de banco de dados);
- Antivírus;
- Snow (Gestão de Licenciamento);
- One Touch (Command Center, licenças de ITSM e sistema de suporte);
- Equipe de gestão do ambiente cloud;
- vCPU²;
- vGB RAM³;

- **Sistema Operacional**

Os sistemas operacionais suportados no ambiente são:

- MS Windows Server 2019;
- MS Windows Server 2022;
- MS Windows Server 2025;
- Red Hat Enterprise Linux 8;
- Linux SUSE 15;

² vCPU: É o termo utilizado para informar a unidade de processamento virtual que são alocados ao servidor virtual.

³ vGB RAM: É o termo utilizado para informar a quantidade de memória alocada para o servidor virtual.

- Linux Ubuntu 22.04;
- Rocky Linux 9.

Nota: A versão sistema operacional deve ser suportado pelo o fabricante, caso sistema operacional ficar sem suporte, a máquina virtual deve ser atualizada para uma versão suportada pelo o Fabricante.

- **Banco de dados**

As versões do Microsoft SQL Server suportadas são:

- SQL Server 2022 Standard/Enterprise.

Nota: A versão do Banco de dados deve ser suportada pelo o fabricante, caso a versão do banco de dados ficar sem suporte, a máquina virtual deve ser atualizada para uma versão suportada pelo o Fabricante.

O valor a ser faturado referente a VM é calculado com base no consumo padrão de 720 horas mensais para meses com 30 (trinta) dias. O valor final pode variar conforme o total de horas do mês e a disponibilidade do recurso, impactando o cálculo mensal do Charge Back. Por exemplo, em um mês de 30 dias, se o recurso estiver disponível durante todo o mês, serão cobradas 720 horas. Caso o recurso seja disponibilizado a partir do dia 28, a cobrança será proporcional ao número de horas efetivamente disponibilizadas.

5.3. Gestão de Capacidade

O **CLIENTE** acessará as suas informações por meio do portal **SONDA** Hybrid, podendo visualizar o consumo de recursos CPU, Memória e Disco, em um panorama geral do ambiente.

OBS: Os percentuais de utilização de CPU, memória e disco apresentados no portal não refletem o uso em tempo real; o portal exibe a média de utilização da última hora

5.4. 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 necessária avaliação/aprovação do projeto.

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.

5.5. Storage

Os discos virtuais são provisionados em *block storage* que possuem a mesma proteção de um armazenamento dedicado, porém em uma estrutura compartilhada.

Os discos virtuais provisionados no ambiente serão armazenados em uma infraestrutura que utiliza classe de armazenamento de alta performance (SSD - unidade de estado sólido).

O volume root (disco de Sistema Operacional), terá o tamanho mínimo de 50 GB para Linux e 100 GB para Windows. Para os volumes adicionais, quando solicitados, serão criados com área máxima de 2 TB. Para conseguir uma área adicional de mais de 2 TB deverá ser aberto um chamado para atendimento da demanda.

O **CLIENTE** poderá utilizar apenas uma oferta de Storage por ambiente.

O valor a ser faturado referente ao Storage é calculado com base no volume de Storage, multiplicado pelo valor por gigabyte, considerando o consumo padrão de 720 horas mensais para meses com 30 (trinta) dias. O valor final pode variar conforme o total de horas do mês e a disponibilidade do recurso, impactando o cálculo mensal do Charge Back. Por exemplo, em um mês de 30 dias, se o recurso estiver disponível durante todo o mês, serão cobradas 720 horas. Caso o recurso seja disponibilizado a partir do dia 28, a cobrança será proporcional ao número de horas efetivamente disponibilizadas.

5.6. 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 RPO⁴ e RTO⁵ 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 os tipos de dados considerados para a Cloud **SONDA** são:

- Backup de Servidor Virtual;
- Backup de SGBD (SQL Server).
- Backup de outros bancos de dados, como por exemplo, PostgreSQL, MariaDB e MySQL, é necessário a configuração do backup via dump, sendo responsabilidade do **CLIENTE**.

- **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, 30 dias – (Armazenamento realizado em ambiente block storage, ou outro meio que a **SONDA** definir, mantendo-se as condições de SLA);
- **Média:** Retenções de médio prazo, 12 meses (Armazenamento realizado em ambiente object storage, ou outro meio que a **SONDA** definir, mantendo-se as condições de SLA);
- **Longa:** Retenções de longo prazo, 5 anos (Armazenamento realizado em ambiente object storage, ou outro meio que a **SONDA** definir, mantendo-se as condições de SLA).

O valor a ser faturado referente ao Backup é calculado com base no volume de Backup, multiplicado pelo valor por gigabyte, considerando o consumo padrão de 720 horas mensais para meses com 30 (trinta) dias. O valor

⁴ **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.

⁵ **RTO** (Recovery Time Objective): Indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha.

final pode variar conforme o total de horas do mês e a disponibilidade do recurso, impactando o cálculo mensal do Charge Back. Por exemplo, em um mês de 30 dias, se o recurso estiver disponível durante todo o mês, serão cobradas 720 horas. Caso o recurso seja disponibilizado a partir do dia 28, a cobrança será proporcional ao número de horas efetivamente disponibilizadas.

Para mais detalhes consulte o Descritivo de Backup.

6. Ofertas

No produto Cloud **SONDA** existem 2 modelos de servidores virtuais:

- **Cloud Server:** servidores virtualizados em Windows ou Linux;
- **Cloud SQL DB:** servidores com banco de dados Microsoft SQL Server virtualizados;

Para este produto, são definidos ranges de configuração de vCPU e vGB RAM, os quais deverão ser respeitados, conforme a disponibilidade apresentada no portal **SONDA** Hybrid.

NOTA: Os templates não contemplam disco, deve ser adicionado o vendável com a quantidade de disco necessária para a solução do **CLIENTE**.

6.1. Cloud Server

Utilizando uma plataforma de virtualização, este subproduto é uma oferta de IaaS (*Infrastructure as a Service*) que consiste na utilização e gestão dos recursos de processamento e armazenamento do ambiente de cloud.

Para atender a demanda, existem modelos distintos baseados no Sistema Operacional utilizado, conforme abaixo:

- **Cloud Server com SO Windows**

Incluso na precificação:

- Licenças do Virtualizador;
- Licenças do Windows Server Data Center Edition;
 - Suporte Premier Microsoft⁶;

- **Cloud Server com SO Linux Red Hat**

Incluso na precificação:

- Licenças do Virtualizador;
Para uso do Red Hat Enterprise Linux, adicionamos o valor de subscrição para suporte e atualizações, considerando 01 (uma) licença por servidor virtual conforme regra do fornecedor. Há dois tipos de licenças: Small e Large Instance, sendo:
 - Small Instance: servidores virtuais com vCPU menor ou igual a 4;
 - Large Instance: servidores virtuais com vCPU maior que 4.

- **Cloud Server com SO Linux SUSE**

⁶ **Premier Microsoft** é o suporte do sistema operacional Windows está relacionado a problemas ocasionados pela infraestrutura, como o “crash” de um servidor. Falhas ocasionadas por má administração por parte do **CLIENTE** não contemplam suporte do fornecedor

Incluso na precificação:

- Licenças do Virtualizador;
Para o uso do SUSE Linux Enterprise Server, adicionamos o valor de subscrição para suporte e atualizações, considerando 1 (uma) licença por servidor virtual. Conforme regras do fornecedor, as licenças são distribuídas em três ranges de vCPU:
 - Servidores virtuais com vCPU menor ou igual a 2;
 - Servidores virtuais com vCPU igual a 3 ou 4;
 - Servidores virtuais com vCPU maior ou igual a 5.

- **Cloud Server com SO Linux (Rocky Linux, Ubuntu)**

Incluso na precificação:

- Licenças do Virtualizador;
O sistema operacional Ubuntu é baseado em GPL (*General Public License*), a designação de licença de software livre para distribuições Linux e não disponibilizamos a versão suportada pela Canonical.

6.2. Cloud Server SQL DB

Sob a plataforma de virtualização, este subproduto é uma oferta de IaaS (*Infrastructure as a Service*) contemplando o banco de dados Microsoft SQL Server em sua configuração, visando atender as principais necessidades do mercado com relação ao armazenamento de dados estruturados.

Como padrão, compõem a sua configuração:

- Licenças do Virtualizador;
- Licenciamento do Sistema Operacional Windows;
- Suporte Premier Microsoft⁷;
- Todas as características da versão Standard e Enterprise do Microsoft SQL Server.

Através da funcionalidade BYOL (*Bring Your Own License*), o **CLIENTE** que possui contrato de *Software Assurance* (SA) com a Microsoft pode optar por utilizar sua própria licença do banco de dados.

7. 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**

⁷ **Premier Microsoft** é o suporte do sistema operacional Windows está relacionado a problemas ocasionados pela infraestrutura, como o “crash” de um servidor. Falhas ocasionadas por má administração por parte do **CLIENTE** não contemplam suporte do fornecedor

A Cloud **SONDA** possui um certificado SSL⁸ válido, no qual todas as requisições HTTP⁹ são redirecionadas para HTTPS¹⁰, incluindo todos os subdomínios e *hostnames*.

O HTTPS ajuda a evitar que dados sejam alterados durante as 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*.

- **Identities 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 **SONDA** Hybrid 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.

⁸ **SSL** (*Secure Sockets Layer*): Tecnologia global de segurança padrão que permite a comunicação criptografada entre um navegador da Internet e um servidor da web.

⁹ **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.

¹⁰ **HTTPS**: Esse protocolo é a combinação dos protocolos HTTP e SSL (*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.

- **MFA**

O MFA (Multi-Factor Authentication) adiciona uma camada de segurança ao processo de login. O Portal **SONDA** Hybrid fornece uma autenticação adicional, no qual é necessário digitar um código recebido no telefone do usuário, ou seja, verificação em duas etapas e segurança adicional para a conta do usuário utilizando o seu próprio dispositivo móvel.

- **Anti-DDoS**

A **SONDA** atua com uma solução de Anti-DDoS¹¹ 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 *Scrubbing 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).

¹¹ **Anti-DDoS**: Proteção completa contra DDoS na rede local e no backT 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 diferença entre DoS do DDoS é que o DoS envolve apenas 1 atacante quando o DDoS um computador mestre pode gerenciar até milhões de computadores atacantes.

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** Ativas 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 toda 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 **CLEINTES** e dados, com uma arquitetura preparada para um ambiente multi locatário.

7.1. 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.

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.

8. Monitoramento

Para atuar de forma preventiva e preditiva, a **SONDA** oferece o serviço de Monitoramento que coleta dados dos itens monitorados e identifica condições que indicam a saúde do ambiente, sinalizando possíveis riscos ou sucessos operacionais.

O **CLIENTE** tem acesso ao portal da ferramenta de monitoramento, onde pode visualizar dados e relatórios detalhados, garantindo total transparência e a certeza de que o ambiente está sendo continuamente gerido e acompanhado pela equipe **SONDA**.

Além disso, o serviço conta com integração entre nosso ITSM e o Monitoramento por meio da ferramenta de Enterprise Application Integration (EAI), permitindo a abertura automática de chamados sempre que uma anomalia for detectada. Isso reduz significativamente o tempo de resposta a qualquer irregularidade no ambiente.

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

9. Premissas e Requisitos

Abaixo são listadas as premissas e restrições do serviço:

- 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 (*Client Access Licenses*) de acesso para conexão a estes servidores.

- Todo software Microsoft instalado na Cloud **SONDA**, deve ter as suas licenças adquiridas junto a **SONDA**, exceto as licenças que permitem BYOL.
- 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 pode reiniciar automaticamente a máquina virtual;
- A reserva de recurso computacional (vCPU/vGB RAM) por servidor virtual não é permitida;
- Caso o **CLIENTE** exclua a instância 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;
- 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**.
- 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** necessite utilizar algum Sistema Operacional ou Banco de dados que não tenha mais suporte pelo o fabricante, a **SONDA** não garante a completude e funcionamento correto dos serviços ofertados, além dos riscos operacionais de disponibilidade do ambiente em caso de bugs da ferramenta, vulnerabilidades que podem expor o ambiente a cyber ataques, visto que o fabricante não disponibiliza patches de correções para as falhas de segurança. Será necessária aprovação da **SONDA** e se aprovado, será emitida uma Carta de risco ao **CLIENTE** com validade de seis meses;
- O volume mínimo do disco virtual para o disco de Sistema Operacional é de 100 GB por servidor Windows, e 50 GB por servidor Linux e não poderá ser segregado;
- Caso ocorra uma interrupção do servidor físico da Cloud **SONDA**, onde os servidores virtuais estão implementados, ocorrerá um downtime até que os servidores virtuais migrem de Host automaticamente. Consequentemente poderá existir uma interrupção nos serviços providos por estes servidores até que termine o processo de migração das máquinas virtuais;
- Baseado na premissa anterior, em caso de utilização de servidores de Banco de Dados na estrutura de servidor Virtual, poderá ocorrer perda de dados na base. Diante disso, a interrupção inesperada nos serviços e possível corrupção das informações, será necessária a restauração dos dados através do último backup realizado;
- Os profissionais da **SONDA** não realizarão atendimento a softwares e sistemas que fazem parte do negócio do **CLIENTE** e/ou não relacionados na Matriz de Responsabilidades. Portanto, o **CLIENTE** deverá possuir equipe de TI de administração e suporte para seus serviços/aplicações;
- Para um maior controle do ambiente, aprovisionamentos superiores a 25% da capacidade atual do ambiente do **CLIENTE**, será necessária a abertura de chamado e análise de viabilidade de capacidade técnica;

- Por padrão, os logs do sistema operacional são armazenados por categorias de eventos e, ao atingirem o limite de tamanho configurado, os registros mais antigos são automaticamente eliminados, o que impossibilita consultas ou recuperações retroativas. As principais categorias e seus respectivos limites são: System, Application e Security, com 20 MB cada, e Setup, com 1 MB.

10. 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

10.1. Matriz de Responsabilidade Cloud SONDA

No quadro abaixo está listado as responsabilidades do Produto Cloud **SONDA**.

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 Sistema Operacional	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

No quadro 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**.

10.2. Matriz de Responsabilidades – Serviços Gerenciados

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

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 SONDA Hybrid	R	S
Não	Análise de desempenho e performance da infraestrutura da plataforma	R	S
Não	Backup da Plataforma	R	

Nota: Requisições e Matriz de Responsabilidade de serviços relacionados à infraestrutura do **CLIENTE** se encontram no descritivo do produto específico.

No quadro 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**.

11.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 na Cloud SONDA	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

12.Níveis de Serviço

Serviço	Nome	Descrição	Meta
CLOUD SONDA	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.	99,90 %

A large, bold, blue stylized letter 'N' that fills most of the frame. The letter has a rounded top and a curved bottom right. In the bottom right corner, there is a small blue rectangular box containing the brand name and slogan.

SONDA[®]
make it easy