

Banrisul Licitações

De: Banrisul Licitações
Enviado em: terça-feira, 14 de abril de 2026 07:47
Para: LUCAS.RODRIGUESSILVA@claro.com.br
Assunto: ENC: BANRISUL - EDITAL 000037/2026 - Questionamentos - Claro S/A

À CLARO

REF.: Licitação nº 0000037/2026

OBJETO: Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.

Prezados,

Segue respostas aos questionamentos efetuados:

1. CENÁRIO A – CORE DE SEGURANÇA

1.1 Quantidade de firewalls de grande porte e licenciamento

O item **1.3.1.4** estabelece que a solução deve ser composta por pelo menos oito equipamentos físicos de grande porte (“nodos”), sendo quatro por Data Center (ambientes “X” e “Y”), além de um nodo adicional em cada Data Center para **spare part**.

Diante disso, nosso entendimento é de que deverão ser fornecidos **10 (dez) firewalls físicos ao todo**, sendo:

- 8 (oito) firewalls operacionais; e
- 2 (dois) firewalls como *spare part*.

Solicitamos confirmar se:

- Esse entendimento está correto; e
- **Todos os 10 firewalls, inclusive os spare part, deverão possuir licenciamento completo**, conforme as especificações técnicas exigidas.

RESPOSTA: Está parcialmente correto o entendimento tendo em vista que o dimensionamento completo do cenário A não precisa limitar-se a 10 firewalls. A figura de “nodo” está mais detalhadamente definida a partir do item 1.3.2.1.4 e é uma sugestão referencial mínima para ilustrar o nível de redundância. As proponentes podem entregar um número maior de nodos em suas propostas se assim desejarem. Todos os nodos considerados operacionais no design sugerido pela proposta da proponente devem possuir licenciamento completo conforme especificações do edital.

Os equipamentos de SPARE PART devem estar aptos para funcionamento dentro do nível mais crítico de SLA exigido neste edital (2 horas corridas). Nesses termos, a equipe técnica entende que é preferível que estes equipamentos já estejam com licenciamento completo para uso imediato.

1.2 Equipamentos de gestão centralizada e gestão de logs

Ainda com base no CENÁRIO A, entendemos que, além dos firewalls, será necessário disponibilizar:

- **2 (dois) equipamentos de Gestão Centralizada**, sendo 1 por Data Center;
- **2 (dois) equipamentos de Gestão de Logs**, sendo 1 por Data Center.
- Solicitamos confirmar se esse entendimento procede ou se haverá outra arquitetura aceitável.

RESPOSTA: Está parcialmente correto o entendimento. O modo de redação do questionamento pode dar a entender que as demais funcionalidades estão separadas do ecossistema do fabricante dos firewalls quando na verdade o objeto de contratação é uma solução como um todo. Os equipamentos adicionais mencionados no questionamento para as funcionalidades de Gestão Centralizada e Gestão de Logs sugerem essa entrega no formato on-premise, que é um dos formatos válidos para essas funcionalidades, desde que sejam apresentadas como *appliances* que façam parte da solução de firewalls do fabricante ofertado (físicos ou virtualizados).

Também é importante a leitura dos itens do edital como um todo, considerando que trata-se de uma solução por inteiro. Dessa forma, o questionamento também tem relação com itens de caráter geral da solução para os quais vários requisitos são colocados como modelo global para a solução e suas funcionalidades, como por exemplo:

No item da TR, 2.1.3.2, temos a seguinte redação:

“ Esta solução deve permitir, em um universo de dois sites físicos de Data Center, que um equipamento ou conjunto de equipamentos possa assumir as operações de seus pares em caso de falha de algum nodo principal ou até mesmo assumir completamente a operação para garantir a continuidade do negócio com o nível adequado de segurança e disponibilidade, respeitando níveis de redundância equivalentes a um Data Center padrão Tier 4, considerando nível 2N+1, ou seja, dois conjuntos idênticos de equipamentos redundantes (por site físico) mais um componente extra de spare part para maior resiliência (equipamento para atendimento dos níveis críticos de SLA em caso de RMA)”.

No item da PET, 1.3.2.1.2.1, temos a seguinte redação:

“A principal premissa é o provimento de uma solução de alta disponibilidade, ou seja, ambientes com nível de redundância que contenham um segundo nodo paralelo por site, trabalhando de modo que possa assumir as operações do site por completo em caso de falha de um nodo principal ou, até mesmo, assumir completamente a operação para garantir a continuidade do negócio, com plena visibilidade dos ambientes e todos os recursos de inspeção disponíveis na linha de segurança;”.

Sendo assim, reforçamos adicionalmente que faz-se necessário o uso de alta disponibilidade (HA) para todas as funcionalidades da solução como um todo, assim como para a Gestão Centralizada e Gestão de Logs.

1.3 Equipamentos de menor porte para compliance

O item **1.3.1.5** menciona a necessidade de “uma estrutura secundária de dois equipamentos físicos de menor porte”, um em cada Data Center, para atender requisitos específicos de compliance.

Diante disso, solicitamos esclarecer:

- Esses **2 (dois) equipamentos** são **adicionais** aos 10 firewalls mencionados no item 1.3.1.4 ou correspondem aos *spare parts*?
- Quais são as **especificações técnicas mínimas** desses equipamentos?
- Qual é o conceito de “**menor porte**” adotado pela CONTRATANTE (capacidade, throughput, funcionalidades)?
- Qual a finalidade específica desses equipamentos no contexto de compliance?

RESPOSTA: Em caráter de observação, recomendamos a leitura de todo o edital antes da emissão de questionamentos. O questionamento foi feito em cima de um item de redação introdutória. Indicamos a leitura das especificações a partir do item 1.3.2.2.3 “*Implementar infraestrutura on-premise de administração complementar ao CENÁRIO A - Core de Segurança de Rede, devendo:*” , **estas devem sanar às referidas dúvidas do questionamento.**

1.4 Uso on-premise e em nuvem

O item **1.3.1.6** indica que certas funcionalidades devem estar presentes tanto em ambientes **on-premise** quanto em **nuvem**.

Solicitamos esclarecer:

- O que a CONTRATANTE entende por “estar presente tanto no uso on-premise como em nuvem”;
- Se é exigido que os **mesmos firewalls ofertados em appliance físico** também sejam disponibilizados **como appliances virtuais**; ou
- Se o requisito refere-se apenas à **equivalência funcional**, independentemente do formato (físico, virtual ou cloud).

RESPOSTA: Em caráter de observação, recomendamos a leitura de todo o edital antes da emissão de questionamentos. O edital requisita, para a solução como um todo, funcionalidades que podem ser atendidas de forma on-premise-e/ou em nuvem, e para alguns casos, equivalência funcional. Cabe a cada proponente organizar o portfólio de produtos ofertados para a solução como um todo de modo que todas as especificações do edital sejam atendidas.

2. CENÁRIO B – FIREWALLS EM NUVEM

Os itens **1.3.2.2** e subitens indicam a necessidade de fornecimento de **2 (dois) firewalls virtuais**, adicionais aos firewalls físicos do CENÁRIO A, a serem instalados em ambiente de nuvem disponibilizado pela CONTRATANTE.

Entretanto, identificamos que algumas especificações técnicas fazem referência a características típicas de **appliance físico**, como interfaces físicas, o que não se aplica a ambientes virtuais.

Dessa forma, solicitamos esclarecer:

- Qual o **dimensionamento esperado** para os firewalls virtuais (vCPU, memória, disco, throughput)?
- Quais são as **especificações técnicas corretas e aplicáveis** aos firewalls virtuais?
- Podemos **desconsiderar** as especificações que se referem exclusivamente a appliance físico?
- Confirmar se **toda a infraestrutura de máquinas virtuais (compute, storage, rede)** será disponibilizada pela CONTRATANTE.

RESPOSTA: Em caráter de observação, recomendamos a leitura de todo o edital antes da emissão de questionamentos. O questionamento está inconsistente.

O edital menciona diferentes cenários para os quais foram agrupadas características específicas, leia-se o subitem logo após o item questionado:

“1.3.2.2.1. O cenário B engloba o ambiente de firewall em nuvem e a infraestrutura on-premise de administração complementar ao CENÁRIO A - Core de Segurança de Rede, devendo:”

O questionamento refere-se ao Cenário B, que solicita a funcionalidade de firewall em nuvem e outra funcionalidade (essa sim on-premise) de administração complementar. São redações diferentes em itens distintos, cada um com sua especificação (itens 1.3.2.2.2 e 1.3.2.2.3).

3. Migração do ambiente existente

O item **7.7.5** atribui à CONTRATADA a responsabilidade de migração do ambiente atual para a nova solução.

Para adequado planejamento, solicitamos informar:

- Qual é o **fabricante e a solução de firewall atualmente em uso** no ambiente do Banrisul;
- Se essas informações poderão ser oficialmente disponibilizadas à licitante vencedora ou já na fase de esclarecimentos.

RESPOSTA: Considerando que os processos de edital são públicos, informamos que o atual fabricante é a FORCEPOINT, além de outros fabricantes para o qual deverão ser avaliadas integrações conforme especificado em edital. Quando da ocasião do planejamento, a licitante vencedora assinará um termo de sigilo e será adequadamente instruída conforme a redação dos itens que seguem, entre outros:

“7.6.9. Na etapa de planejamento, a CONTRATADA será responsável pelo entendimento do ambiente em produção do CONTRATANTE, para que sejam detalhados os passos necessários para a migração do ambiente. O entendimento do ambiente atual deve envolver todos os itens informados pela equipe técnica do CONTRATANTE no PLANO DE PROJETO.

7.6.10. Todas as informações referentes aos ambientes existentes envolvidos neste processo serão repassadas pelo corpo técnico do CONTRATANTE à CONTRATADA.

7.6.11. Será responsabilidade do CONTRATANTE, disponibilizar acesso às configurações dos equipamentos, bem como documentações existentes de topologia.

7.6.12. O CONTRATANTE possui em seu ambiente soluções de outros fabricantes (Cisco, VMWare, Redhat, Aruba, Fortinet, entre outros). Sempre que solicitado pelo CONTRATANTE, a solução deve prever a integração com outras soluções do CONTRATANTE.”

Dessa forma, as referidas informações serão oficialmente disponibilizadas à licitante vencedora no período oportuno.

4. Serviços: horas técnicas, operação assistida e suporte

4.1 500 horas técnicas x operação assistida

Os itens **7.11.31** (500 horas técnicas/ano) e **7.11.33** (2 profissionais dedicados à operação assistida) geram dúvidas quanto à sobreposição ou segregação dos serviços.

Solicitamos esclarecer:

- As **500 horas técnicas anuais** incluem ou não os serviços de **operação assistida**;
- Qual o **período de duração da operação assistida** (em meses ou anos);
- Se as 500 horas técnicas são **totalmente independentes** da operação assistida.

RESPOSTA: As horas técnicas anuais **NÃO** estão inseridas na operação assistida, trata-se de uma reserva de horas para apoio à novas demandas, implementações ou estudos originalmente fora do escopo previsto em edital, conforme redação:

“7.11.31. A CONTRATADA deve alocar 500 (quinhentas) horas técnicas por ano (em caráter limitador máximo, podendo variar de acordo com as necessidades do CONTRATANTE) para a prestação de serviços de suporte ao desenvolvimento, manutenção, implementação, projetos e especificações de segurança da informação com ênfase na solução ofertada, a serem executados nas dependências do CONTRATANTE, envolvendo:

7.11.31.1. Elaboração de novos projetos;

7.11.31.2. Suporte técnico no desenvolvimento e integração, relativos à solução ofertada;

7.11.31.3. Elaboração de material de apoio e documentação de novos projetos;

7.11.31.4. Elaboração de pareceres técnicos;

7.11.31.5. Orientação a analistas, desenvolvedores e programadores sobre aspectos relacionados à segurança da informação e a da solução ofertada;”

As horas técnicas anuais são um item totalmente independente da Operação Assistida.

A Operação Assistida deve ocorrer conforme o cronograma de atividades/entregas referido no item 7.13 de modo que: “7.13.1.6.2. **PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA:** Em até 60 (sessenta) dias corridos a partir do início da **MIGRAÇÃO PARA O NOVO AMBIENTE** para a

apresentação e início das atividades dos profissionais dedicados à operação assistida, de forma que estes participem da fase de **IMPLEMENTAÇÃO INICIAL DO PROJETO;**” estando previsto inicialmente na planilha de orçamentos o prazo de 54 meses (descontados os meses de implementação).

4.2 Suporte 24x7 e precificação dos serviços

O item **7.11.34** exige suporte técnico **24x7x365**, em regime presencial e remoto.

Para fins de dimensionamento e precificação, solicitamos esclarecer:

- A CONTRATADA deverá prover **simultaneamente**:
 - Suporte 24x7x365;
 - 500 horas técnicas anuais; e
 - Operação assistida com profissionais dedicados?
- Caso contrário, qual é a **composição correta** e como deve ser estruturada a **precificação** desses serviços.

RESPOSTA: O entendimento está parcialmente correto, porém, retratado de forma muito simplista no pedido de esclarecimento. O questionamento refere-se à apenas um subitem do item “7.11. MANUTENÇÃO, SUPORTE TÉCNICO E OPERAÇÃO ASSISTIDA DOS AMBIENTES” que corresponde a aproximadamente quatro páginas do edital. A Contratada deverá atender ao Suporte 24x7x365 e à Operação assistida nos termos do item 7.11 do edital bem como a minuta contratual e, da mesma forma, também deverá atender às 500 horas técnicas conforme explicado no questionamento anterior, respeitando os termos e vigência do contrato.

5. Gestão de Vulnerabilidades

Identificamos, nos itens **7.9.3 a 7.9.17**, exigências que caracterizam atividades típicas de **Gestão de Vulnerabilidades**, as quais normalmente requerem ferramentas específicas (ex.: Tenable, Ecotrust, similares), com custos e licenciamento próprios.

Dessa forma, solicitamos esclarecer:

- A CONTRATANTE realmente exige a prestação de **serviços de Gestão de Vulnerabilidades** como parte do escopo?
- Em caso positivo:
 - Qual o **tipo de teste** esperado (DAST, outro)?
 - Qual a **quantidade e tipo de ativos** a serem licenciados?
 - Qual a **periodicidade** esperada dos scans (mensal, trimestral, anual)?
 - Qual é a **expectativa da CONTRATANTE** quanto a entregáveis e resultados desse serviço?

RESPOSTA: O questionamento se refere aos seguintes itens, que versam sobre as responsabilidades da CONTRATADA:

“7.9.3. A CONTRATADA tem a responsabilidade de aplicar os controles necessários para corrigir quaisquer vulnerabilidades ligadas à solução que possam afetar a confidencialidade, integridade e disponibilidade dos serviços prestados ao CONTRATANTE;

7.9.17. Caso a CONTRATADA tenha conhecimento de vulnerabilidades na solução ou na infraestrutura que trafega, processa ou armazena dados do CONTRATANTE, ou vulnerabilidades em outros ativos que possam afetar dados do CONTRATANTE, deve comunicar imediatamente o CONTRATANTE;”

Não há item no edital sobre a contratação específica de serviços de Gestão de Vulnerabilidades no formato indicado pelo questionamento. Dessa forma não fazem sentido as questões

referentes aos tipos de teste, quantidade e tipo de ativos e periodicidade esperada dos scans nesse formato.

O Item 7.9.1 traz “A CONTRATADA deve *viabilizar* a execução de testes da solução, visando a identificação de vulnerabilidades no ambiente de TI que possam afetar o CONTRATANTE;” no sentido de que deve apoiar os procedimentos de auditoria, internos e externos, de modo a tornar viável os testes para auditoria e compliance realizados periodicamente nos ambientes, e não propriamente executar tais testes.

Já o item 7.9.3., mencionado no questionamento, indica que, uma vez identificadas vulnerabilidades, a CONTRATADA deve atuar junto ao fabricante para providenciar a correção da mesma forma que, no item 7.9.17, a CONTRATADA deve comunicar imediatamente ao CONTRATANTE quando da identificação de alguma vulnerabilidade.

Atenciosamente,



Gerencia de Licitações
Unidade de Contratações e Pagadoria
☎ (51) 3215-4503 | E-mail: banrisul_licitacoes@banrisul.com.br

De: LUCAS RODRIGUES DA SILVA <LUCAS.RODRIGUESSILVA@claro.com.br>

Enviada em: quarta-feira, 8 de abril de 2026 14:00

Para: Banrisul Licitacoes <BANRISUL_LICITACOES@banrisul.com.br>

Assunto: BANRISUL - EDITAL 000037/2026 - Questionamentos - Claro S/A

PEDIDO DE ESCLARECIMENTOS

Licitação Eletrônica nº 000037/2026

Objeto: Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida
À Gerência de Licitações – BANRISUL

Prezados,

Após análise detalhada do Edital da Licitação Eletrônica nº 000037/2026 e de seus anexos, especialmente do Termo de Referência e das Especificações Técnicas, Claro S/A, solicita, respeitosamente, os esclarecimentos abaixo, com o objetivo de assegurar o correto entendimento do escopo, o adequado dimensionamento técnico e a correta formação de preços da proposta.

1. CENÁRIO A – CORE DE SEGURANÇA

1.1 Quantidade de firewalls de grande porte e licenciamento

O item 1.3.1.4 estabelece que a solução deve ser composta por pelo menos oito equipamentos físicos de grande porte (“nodos”), sendo quatro por Data Center (ambientes “X” e “Y”), além de um nodo adicional em cada Data Center para **spare part**.

Diante disso, nosso entendimento é de que deverão ser fornecidos **10 (dez) firewalls físicos ao todo**, sendo:

- 8 (oito) firewalls operacionais; e
- 2 (dois) firewalls como *spare part*.

Solicitamos confirmar se:

- Esse entendimento está correto; e
- **Todos os 10 firewalls, inclusive os spare part, deverão possuir licenciamento completo**, conforme as especificações técnicas exigidas.

1.2 Equipamentos de gestão centralizada e gestão de logs

Ainda com base no CENÁRIO A, entendemos que, além dos firewalls, será necessário disponibilizar:

- **2 (dois) equipamentos de Gestão Centralizada**, sendo 1 por Data Center;
 - **2 (dois) equipamentos de Gestão de Logs**, sendo 1 por Data Center.
- Solicitamos confirmar se esse entendimento procede ou se haverá outra arquitetura aceitável.

1.3 Equipamentos de menor porte para compliance

O item **1.3.1.5** menciona a necessidade de “uma estrutura secundária de dois equipamentos físicos de menor porte”, um em cada Data Center, para atender requisitos específicos de compliance.

Diante disso, solicitamos esclarecer:

- Esses **2 (dois) equipamentos** são **adicionais** aos 10 firewalls mencionados no item 1.3.1.4 ou correspondem aos *spare parts*?
- Quais são as **especificações técnicas mínimas** desses equipamentos?
- Qual é o conceito de “**menor porte**” adotado pela CONTRATANTE (capacidade, throughput, funcionalidades)?
- Qual a finalidade específica desses equipamentos no contexto de compliance?

1.4 Uso on-premise e em nuvem

O item **1.3.1.6** indica que certas funcionalidades devem estar presentes tanto em ambientes **on-premise** quanto em **nuvem**.

Solicitamos esclarecer:

- O que a CONTRATANTE entende por “estar presente tanto no uso on-premise como em nuvem”;
- Se é exigido que os **mesmos firewalls ofertados em appliance físico** também sejam disponibilizados **como appliances virtuais**; ou
- Se o requisito refere-se apenas à **equivalência funcional**, independentemente do formato (físico, virtual ou cloud).

2. CENÁRIO B – FIREWALLS EM NUVEM

Os itens **1.3.2.2** e subitens indicam a necessidade de fornecimento de **2 (dois) firewalls virtuais**, adicionais aos firewalls físicos do CENÁRIO A, a serem instalados em ambiente de nuvem disponibilizado pela CONTRATANTE.

Entretanto, identificamos que algumas especificações técnicas fazem referência a características típicas de **appliance físico**, como interfaces físicas, o que não se aplica a ambientes virtuais.

Dessa forma, solicitamos esclarecer:

- Qual o **dimensionamento esperado** para os firewalls virtuais (vCPU, memória, disco, throughput)?
- Quais são as **especificações técnicas corretas e aplicáveis** aos firewalls virtuais?
- Podemos **desconsiderar** as especificações que se referem exclusivamente a appliance físico?

- Confirmar se **toda a infraestrutura de máquinas virtuais (compute, storage, rede)** será disponibilizada pela CONTRATANTE.

3. Migração do ambiente existente

O item **7.7.5** atribui à CONTRATADA a responsabilidade de migração do ambiente atual para a nova solução. Para adequado planejamento, solicitamos informar:

- Qual é o **fabricante e a solução de firewall atualmente em uso** no ambiente do Barrisul;
- Se essas informações poderão ser oficialmente disponibilizadas à licitante vencedora ou já na fase de esclarecimentos.

4. Serviços: horas técnicas, operação assistida e suporte

4.1 500 horas técnicas × operação assistida

Os itens **7.11.31** (500 horas técnicas/ano) e **7.11.33** (2 profissionais dedicados à operação assistida) geram dúvidas quanto à sobreposição ou segregação dos serviços.

Solicitamos esclarecer:

- As **500 horas técnicas anuais** incluem ou não os serviços de **operação assistida**;
- Qual o **período de duração da operação assistida** (em meses ou anos);
- Se as 500 horas técnicas são **totalmente independentes** da operação assistida.

4.2 Suporte 24x7 e precificação dos serviços

O item **7.11.34** exige suporte técnico **24x7x365**, em regime presencial e remoto.

Para fins de dimensionamento e precificação, solicitamos esclarecer:

- A CONTRATADA deverá prover **simultaneamente**:
 - Suporte 24x7x365;
 - 500 horas técnicas anuais; e
 - Operação assistida com profissionais dedicados?
- Caso contrário, qual é a **composição correta** e como deve ser estruturada a **precificação** desses serviços.

5. Gestão de Vulnerabilidades

Identificamos, nos itens **7.9.3 a 7.9.17**, exigências que caracterizam atividades típicas de **Gestão de Vulnerabilidades**, as quais normalmente requerem ferramentas específicas (ex.: Tenable, Ecotrust, similares), com custos e licenciamento próprios.

Dessa forma, solicitamos esclarecer:

- A CONTRATANTE realmente exige a prestação de **serviços de Gestão de Vulnerabilidades** como parte do escopo?
- Em caso positivo:
 - Qual o **tipo de teste** esperado (DAST, outro)?
 - Qual a **quantidade e tipo de ativos** a serem licenciados?
 - Qual a **periodicidade** esperada dos scans (mensal, trimestral, anual)?
 - Qual é a **expectativa da CONTRATANTE** quanto a entregáveis e resultados desse serviço?

Certos de sua atenção, permanecemos no aguardo dos esclarecimentos para adequada elaboração da proposta, em estrita conformidade com o edital.

Atenciosamente,

LUCAS RODRIGUES DA SILVA
GRANDES EMPRESAS E GOVERNO
Diretoria de Vendas | Mercado Financeiro
Fone: +55 51 9.9188-5194
lucas.rodriuessilva@claro.com.br

Siga nossas redes @claroempresasbra

Claro[!]-empresas

