

ANEXO II

**ESPECIFICAÇÕES TÉCNICAS
ESPECIFICACIONES TÉCNICAS**

**ADITAMENTO 1
ADITIVO 1**

VERSÃO EM PORTUGUÊS
VERSIÓN EN PORTUGUÉS

1 OBJETO

Aquisição de solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM) - **Beyond Trust**, assim como serviços de implementação, migração, capacitação e suporte técnico especializado.

2 ESCOPO DA SOLUÇÃO

O escopo da solução contempla a aquisição de licenças, produtos e serviços para implantação da solução de Gestão de Acesso Privilegiado **Beyond Trust** na ITAIPU, devendo ser realizado em regime único, incluindo:

- Etapa de planejamento e elaboração de projeto executivo.
- Fornecimento de equipamentos, softwares e licenças.
- Serviços de instalação, configuração e testes em campo.
- Migração de dados da solução atual para a nova solução.
- Acompanhamento do comissionamento e colocação em serviço.
- Serviços de suporte técnico (Banco de Horas sob demanda).
- Documentação.
- Treinamento.
- Integrações com sistemas existentes (sob demanda).
- Garantias e os demais elementos e serviços necessários para o completo e perfeito funcionamento da solução.

3. ESPECIFICAÇÕES DOS PRODUTOS E SERVIÇOS

3.1 A CONTRATADA deverá fornecer produtos e serviços da solução de Gerenciamento de Acesso Privilegiado (PAM) conforme os seguintes requisitos técnicos:

- **Fabricante:** Beyond Trust.
- **Modalidade da Licença:** Subscrição.
- **Tipo:** Appliance Virtual e appliance físico.
- **Período para Licenciamento:** 36 meses.

Item	PRODUTO E SERVIÇOS	Unidade	QUANTIDADE
1	Beyond Trust Password Safe	Ativos	2.100
2	Beyond Trust Privileged Remote Access - PRA	Usuarios	50
3	Beyond Trust Workforce Password	Usuarios	300
4	Beyond Trust Appliance Virtual	Unidades	2
5	Beyond Trust Appliance Físico	Unidades	2
6	Serviço de implantação e migração de dados (inclui integração Service-Now e Splunk)	Unidade	1
7	Treinamento (repassé de conhecimento)	Unidade	1
8	Suporte Técnico Local e Remoto - Banco De Horas	Horas	900

Tabela 1 - Relação de Produtos e Serviços

3.2 As quantidades de licenças especificadas foram dimensionadas para atender às necessidades

de todo o ambiente da ITAIPU conforme detalhado a seguir. É responsabilidade da CONTRATADA entregar as licenças suficientes para atender tal ambiente:

- O licenciamento do produto “**BeyodTrust Password Safe**” deverá ser suficiente para gerenciar o seguinte ambiente:
 - 1000 (um mil) servidores Linux/Unix.
 - 500 (quinhentos) servidores Windows.
 - 100 (cem) instâncias de Banco de Dados.
 - 500 (quinhentos) ativos de rede (switches, roteadores, firewalls, controladores, balanceadores, WAF e outros).
 - 250 (duzentos e cinquenta) aplicações web.
 - 500 (quinhentos) usuários acessando o cofre/gateway (sendo ao menos 50 simultâneos).
- O licenciamento do produto “**BeyodTrust Privileged Remote Access - PRA**” deverá ser suficiente para garantir acesso remoto de ao menos 50 acessos simultâneos.
- O licenciamento do produto “**BeyodTrust Workforce Passwords**”, deverá ser suficiente para garantir a utilização do produto para ao menos 300 usuários.

3.3 A solução ofertada pela CONTRATADA deve ser integrada com o **Splunk SIEM** e o **Service-Now ITSM**, caso essa integração possua custos ou licenças específicas, estas devem ser parte integrante da proposta apresentada pela CONTRATADA.

3.4 A integração com Splunk SIEM e Service-Now ITSM, é de responsabilidade da CONTRATADA, e deve ser executada na fase de implantação da solução.

3.5 A solução ofertada pela CONTRATADA deve funcionar em modo de cluster de alta disponibilidade no modelo Ativo/Passivo utilizando obrigatoriamente Appliances Virtuais em plataforma VMWare vSphere e Appliances Físicos, tanto para o produto **BeyodTrust Password Safe** quanto para **BeyodTrust Privileged Remote Access - PRA**.

3.6 A CONTRATADA deverá garantir a atualização de versão dos softwares contratados, durante a vigência do contrato, incluindo versões maiores (major releases), versões menores (minor releases), versões de manutenção (maintenance releases) e atualizações de qualquer natureza (updates e patches) que forem disponibilizadas para todos os softwares especificados na seção 3.1, sem ônus adicionais.

3.7 A ativação das licenças (contagem de prazo de vigência) deve ser apenas a partir do início da implantação do produto, ou seja, o prazo de 36 meses deverá ser contado a partir do início do processo de implantação da solução.

3.8 Os produtos deverão estar certificados para o ambiente tecnológico da ITAIPU descrito no item 10 Ambiente Tecnológico da ITAIPU.

3.9 Todos os itens deste processo de aquisição, deverão ser obrigatoriamente fornecidos pela mesma CONTRATADA.

3.10 Para o objeto do item 5 da Tabela 1 - Relação de Produtos e Serviços, alternativamente ao equipamento integralmente da marca BeyondTrust, será admitido o fornecimento de Appliance Físico implementado sobre servidor de fabricante distinto, conforme marca e modelo indicados na proposta comercial da CONTRATADA (hipótese do 2.4.1.1 do CBC), devidamente dimensionado conforme requisitos técnicos do fabricante BeyondTrust e com a solução pré-instalada e funcional, mantendo-se os demais requisitos definidos nesta especificação técnica.

3.11 Na hipótese do fornecimento do hardware descrito no item 3.10, é de inteira

responsabilidade da CONTRATADA todo o suporte e garantia do hardware fornecido, incluindo, mas não se limitando a atualizações de firmware, atualizações de sistemas operacionais, e substituição de peças ou componentes, pelo período de vigência do contrato, sem ônus adicional para a ITAIPU e sem consumir, para essas atividades, horas do "Suporte Técnico Local e Remoto - Banco De Horas".

3.12 Todos os componentes de software necessários para o correto funcionamento da solução no hardware ofertado para atuar como "appliance físico", conforme o item 3.10, devem ser fornecidos e mantidos pela CONTRATADA ao longo da vigência do contrato.

4 IMPLANTAÇÃO E MIGRAÇÃO DA SOLUÇÃO ATUAL

4.1 A CONTRATADA deverá realizar o planejamento das atividades em conjunto com a Itaipu, esse planejamento deve compreender as várias tarefas que serão realizadas ao longo do período de implantação e migração de dados. Este planejamento deverá ser registrado em um cronograma que orientará a respectiva execução.

4.2 A instalação, customização da solução e a migração de dados são de responsabilidade da CONTRATADA, devendo considerar as boas práticas definidas pelo fabricante. Estas atividades deverão ser realizadas de forma presencial nas dependências da Central Hidrelétrica de ITAIPU segundo cronograma previamente definido.

4.3 A instalação e customização da solução englobam a migração da solução atual para a nova plataforma e a integração completa da solução aos demais elementos da infraestrutura preexistente em ITAIPU. Os custos relacionados a esta atividade deverão estar contemplados na oferta de preços.

4.4 O produto atual a ser migrado para a solução BeyondTrust é o "Password Manager Pro" da empresa "ManageEngine" (PMP) <https://www.manageengine.com/br/passwordmanagerpro/>.

4.5 A migração deve contemplar toda a base de ativos do Password Manager Pro - PMP que inclui sistemas MS Windows, Red Hat Linux e base de dados PostgreSQL, MSSQL e Oracle, bem como as políticas de rotação de senhas para os ativos mencionados. Há também credenciais avulsas (sem integração ou rotação de senha) que devem ser migradas.

4.6 Deve ser migrado Workflow de aprovação para check-out de credencial do sistema SAP, bem como a rotação da senha após o check-in da credencial. Essa integração junto ao SAP pode ser feita de forma nativa, via API ou através de script externo.

4.7 Devem ser migrados (implementados na solução BeyondTrust) no mínimo os seguintes relatórios:

- Relatório de check-out e check-in de credenciais por grupo de ativos.
- Relatório de acesso remoto - PRA - e do gateway de acesso.
- Relatório de Password Out of Sync.

4.8 A implantação da solução BeyondTrust não se limita a migração dos itens especificados acima. Na etapa de planejamento a ITAIPU especificará as demais funcionalidades, fluxos e relatórios que deverão contemplar a solução implantada.

4.9 A CONTRATADA deverá fornecer toda a documentação técnica, manuais, diagramas lógicos e físicos, procedimentos de operação dos produtos em meio digital preferencialmente nos idiomas português e espanhol, excepcionalmente em inglês.

5 TREINAMENTO (REPASSE DE CONHECIMENTO)

5.1 A CONTRATADA deverá realizar transferência de conhecimento da solução implantada na ITAIPU e ter uma duração de até 40 horas para no mínimo 12 pessoas.

5.2 É de responsabilidade da contratada a elaboração de material de apoio (apostilas) e audiovisual para a transferência de conhecimento.

5.3 A transferência de conhecimento deve ser realizada de forma presencial nas dependências da ITAIPU, por profissional capacitada da contratada ou da fabricante.

5.4 O planejamento das datas e horários de execução deverá ser combinado entre a CONTRATADA e a ITAIPU.

5.5 A avaliação da capacitação será realizada pela ITAIPU. Caso mais de 50% dos participantes indicarem que não atendeu as expectativas previstas, a capacitação deverá ser repetida.

5.6 Caso a insuficiência da capacitação deva-se a problemas do desempenho do instrutor, se assim for indicado nas avaliações, outra deverá ser realizada, com a mesma carga horária e com outro instrutor, sem custos adicionais para ITAIPU.

6 SERVIÇOS DE SUPORTE TÉCNICO LOCAL E REMOTO - BANCO DE HORAS

6.1 Faz parte do escopo de atuação do suporte técnico (local e remoto) as atividades relacionadas ao planejamento, consultoria, apoio a projetos internos, suporte, configuração, customização, testes e implementação das ferramentas BeyondTrust ora adquiridas ou qualquer outro elemento relacionado a esta plataforma.

6.2 Devem ser fornecidos serviços de suporte corretivo e preventivo, com profissionais capacitados em todas as soluções fornecidas, e aptos a desenvolverem atendimento remoto e local no escritório Central Hidrelétrica de ITAIPU, em ciclos periódicos ou sob demanda, de forma a garantir o perfeito funcionamento do sistema e a manutenção de todos os critérios de desempenho, disponibilidade e segurança.

6.3 A presente contratação deve contemplar um banco de horas, com 900 horas de suporte técnico local e remoto, não sendo de faturamento garantido, pois deverá ser previamente solicitado, agendado e aprovado pela ITAIPU e será utilizado com os seguintes critérios para o cálculo de horas:

Tipo de Serviço	Unid.	Quant.	Equiv.
Suporte técnico remoto (independente do horário)	Hora	1	0,7
Suporte on-site (horário comercial)	Hora	1	1
Suporte on-site (noturno)	Hora	1	1,5
Suporte on-site (finais de semana e feriados)	Hora	1	2

Tabela 2 Equivalência de horas de atendimento

6.4 Para fins de precificação de horas, considerar o valor do suporte on-site (horário comercial), pois os demais possuem uma equivalência em relação a este.

6.5 As solicitações de atendimento on-site serão de no mínimo 24 horas por solicitação, e agendadas com pelo menos 15 dias de antecedência junto a CONTRATADA.

6.6 Os custos de deslocamento, estadia, alimentação e demais despesas de viagem, são de

exclusiva responsabilidade da CONTRATADA.

6.7 Para todas as atividades, tanto de Suporte Técnico como de implantação, a CONTRATADA deverá assinar contrato de confidencialidade, nos termos apresentados por ITAIPU, a respeito das informações que serão obtidas sobre a Infraestrutura da ITAIPU.

6.8 A CONTRATADA deverá garantir a disponibilidade técnica e o atendimento dos serviços de suporte técnico remoto em regime de 24x7, para todo o conjunto de serviços que faz parte desse contrato, sem limite de acionamentos e devendo responder aos requisitos de níveis de serviço especificados na tabela 3.

SEVERIDADE	DESCRIÇÃO	INÍCIO DO ATENDIMENTO	ENCERRAMENTO DO ATENDIMENTO
0	Ambiente Parado	Imediato	4 h
1	Funcionamento Precário	6 h	12 h
2	Dúvidas, consultas ou demandas específicas	12 h	24 h
3	Atividade Planejada	Negociado	Negociado

Tabela 3: Acordo de Níveis de Serviços (SLAs) do Suporte Técnico Remoto

6.9 O início da prestação de Suporte Técnico Remoto não poderá ultrapassar o tempo máximo (em horas corridas) estabelecido na coluna INÍCIO DO ATENDIMENTO, desde a abertura do chamado pela ITAIPU, tendo a CONTRATADA até o tempo máximo (em horas corridas) estabelecido na coluna ENCERRAMENTO DO ATENDIMENTO para concluir as atividades de suporte, informando a efetiva solução do problema ou solução de contorno.

6.10 Os níveis de severidade serão definidos por ITAIPU na abertura do chamado e poderão sofrer alterações ao longo do atendimento.

6.11 Quanto se tratar de “Atividade Planejada”, com tempos de início e encerramento do atendimento negociado, antes do início da atividade a CONTRATADA deverá apresentar a quantidade de horas estimadas para a execução da atividade, e esta deverá ser aprovada por ITAIPU antes do início efetivo.

6.12 A qualquer momento, caso a CONTRATADA observe que não será possível cumprir com os prazos estabelecidos para início e/ou encerramento do atendimento, esta deverá comunicar formalmente a ITAIPU, apresentando as devidas justificativas para o não cumprimento dos prazos, e caberá exclusivamente a ITAIPU o aceite ou não das justificativas apresentadas.

6.13 Quando a solução e/ou resposta passar a depender do FABRICANTE, passa a vigorar os tempos de atendimento e solução descritos pelo FABRICANTE considerando sempre o programa de suporte contratado por ITAIPU junto ao FABRICANTE.

6.14 O encerramento do atendimento e fechamento do chamado, somente poderá ser realizado após validado e atestado pela ITAIPU.

6.15 Apenas serão faturadas horas do banco de horas efetivamente utilizadas, devendo ser previamente solicitadas, agendadas e aprovadas pela ITAIPU.

6.16 O atendimento do chamado de suporte técnico caracterizado como SEVERIDADE 0, devem ser iniciados imediatamente após o acionamento e registro do chamado, utilizando recursos de acesso remoto se necessário.

6.17 Para atividades de Suporte Técnico Local, somente deverão fazer parte deste computo as horas consumidas nas atividades designados pela ITAIPU ou em local previamente aprovado pela área gestora. Não deverá fazer parte deste cálculo as horas consumidas desde o deslocamento do técnico até a apresentação na ITAIPU.

6.18 Para os casos de serviços de suporte técnico local deverá ser realizado um relatório técnico das atividades desenvolvidas.

6.19 A CONTRATADA deverá dispor de no mínimo DOIS meios para aberturas de chamados, sendo um obrigatoriamente o canal telefônico, e o outro podendo ser e-mail ou sistema web de tickets.

6.20 Em até 10 dias após a data indicada na OIS, a CONTRATADA deverá realizar uma reunião de planejamento com a ITAIPU para definir os cronogramas das atividades a serem realizadas.

7 REQUISITOS FUNCIONAIS MÍNIMOS DA SOLUÇÃO

7.1 A solução **BeyondTrust Password Safe** deve garantir o atendimento do seguinte conjunto de requisitos ao longo da vigência do contrato:

7.1.1 Manter a oferta e suporte de Appliance Físico para a solução.

7.1.2 Garantir o funcionamento da solução on-primises, nas dependências da ITAIPU, sem a necessidade de recursos em nuvem.

7.1.3 Manter solução de disaster recovery nativa no produto.

7.1.4 Manter simplicidade da infraestrutura através do conceito de appliances all-in-one, onde todos os recursos necessários para o funcionamento da solução estão presentes no appliance.

7.1.5 Manter suporte oficial, ofertado pelo fabricante, através do Brasil ou do Paraguai.

7.1.6 Manter compatibilidade plena e nativa com clientes Windows, Linux (GUI) e MacOS.

7.1.7 Manter compatibilidade plena e agentless com ativos gerenciados Windows Server, Linux Server, SGBDs.

7.1.8 Manter suporte para a integração com os componentes Splunk SIEM e Service-Now ITSM utilizados na ITAIPU Binacional.

7.1.9 Prover mecanismo automatizado de gravação de sessão e registro de log dos acessos remotos realizados através da ferramenta.

7.1.10 Permitir gerenciamento de acesso privilegiado por meio da configuração de grupos de acesso.

7.1.11 O fornecedor ou usuário final não deve conhecer a credencial do sistema específico que precisa acessar.

7.1.12 A solução deve funcionar com equipamentos, sistemas ou dispositivos finais que se encontrem em mais de um Domínio ou AD Microsoft.

7.1.13 Possibilitar a configuração do acesso remoto a sistemas com base nos seguintes critérios:

- perfil de acesso (consulta, administração, etc).
- ativo e/ou sistema (conjunto de ativos) a serem acessados.
- usuário e/ou grupo de usuários (ex: área/setor responsável).
- workflow de aprovação.
- controle de acesso baseado em função (RBAC).

7.1.14 Prover múltiplo fator de autenticação.

7.1.15 Possibilitar elaboração de fluxos para aprovação das solicitações de acesso realizadas por usuários com autorização.

7.1.16 Permitir acompanhamento em tempo real da sessão remota realizada (funcionalidade "over the shoulder"), bem como permitir a gravação desta em vídeo e/ou texto (teclas pressionadas) de forma automática e transparente, visando garantir mecanismos de auditoria para os acessos.

7.1.17 Em caso de necessidade ou emergência, deve ser permitido ao gerenciador terminar a sessão remota.

7.1.18 Prover fluxos independentes de concessão de acesso para sistemas ou ativos que são de responsabilidade de áreas diferentes.

7.1.19 Permitir a configuração de permissões de acesso remoto vinculadas a intervenções específicas, com prazos definidos (ex: datas de início e término previstos) através de fluxos de aprovação configuráveis.

7.1.20 Dispor de uma interface de programação (API) que permita integração dos fluxos de aprovação de acesso remoto a ferramentas externas para gestão de tickets.

7.1.21 Permitir configuração de acesso via API.

7.1.22 Prover controles que viabilizem auditoria e que gerem alertas quando o acesso for realizado.

7.1.23 Permitir a supervisão de acessos remotos em curso, trazendo informações como:

- Ativo que está sendo acessado.
- Usuário logado.
- Horário de conexão.
- Integração para envio de eventos para outros sistemas por meio de APIs/Protocolos.

7.1.24 Finalização automática de sessões baseadas na inatividade da sessão.

7.1.25 Permitir identificar alteração nos padrões de comportamento de acesso dos usuários e atuar para mitigar violações.

7.1.26 Possibilitar mapeamento e identificação dos ativos conectados ao ambiente e suas respectivas credenciais e certificados digitais.

7.1.27 Possibilitar troca de senha automática de forma periódica e/ou após acesso a credencial do cofre.

7.1.28 Possibilitar o compartilhamento de senhas de forma segura, permitindo o acesso segmentado a credenciais específicas com base em grupos de acesso.

7.1.29 Dispor de mecanismo para armazenamento centralizado e seguro das credenciais de sistemas visando uso em caso de "disaster recovery".

7.1.30 Permitir o armazenamento seguro de tokens e usuários/senhas de usuários de serviço utilizados para integração de sistemas.

7.1.31 Permitir a elevação de privilégio de usuários de forma gerenciada para acesso e execução de aplicações ou serviços específicos restritos a perfis de administração.

7.2 A solução **BeyondTrust Privileged Remote Access** deve garantir o atendimento do seguinte conjunto de requisitos ao longo da vigência do contrato:

7.2.1 Permitir acesso remoto seguro sem a necessidade de VPN, reduzindo riscos de exposição.

7.2.2 Permitir acesso "just-in time" garantindo que os usuários tenham permissão apenas quando necessário, minimizando o risco de acesso não autorizado.

7.2.3 Oferecer controle granular e detalhado sobre todas as sessões privilegiadas, com auditoria e conformidade.

7.2.4 Garantir a integração nativa com a solução BeyondTrust Password Safe evitando duplicidade de dados.

7.3 A solução **BeyondTrust Workforce Password** deve garantir o atendimento do seguinte conjunto de requisitos ao longo da vigência do contrato:

7.3.1 Suportar pastas de segurança personalizadas, onde cada usuário tenha pastas individuais para suas senhas diárias, permitindo que os funcionários mantenham suas credenciais de forma segura diretamente do navegador.

7.3.2 Suporte para extensões de navegador, garantindo a integração aos fluxos de trabalho existentes dos usuários, simplificando a recuperação e preenchimento automático de senhas. Deverão ser suportados no mínimo os seguintes navegadores Mozilla Firefox, Google Chrome e Microsoft Edge.

7.3.3 Possuir capacidades abrangentes de auditoria com foco em ambiente empresarial, permitindo rastrear, analisar e revisar as ações do usuário.

7.3.4. Permitir detectar atividades suspeitas relacionadas ao acesso de aplicativos de negócios dos funcionários e oferecer uma visão holística da saúde das senhas em toda a organização.

7.3.5 Permitir a aplicação de políticas de senhas, garantindo que as senhas estejam em conformidade com as políticas de segurança, abrangendo todas as aplicações, não apenas as privilegiadas.

8. QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS

8.1 A CONTRATADA deverá comprovar a qualificação técnica dos profissionais que atuarão na implantação, migração, treinamento e suporte técnico através de documentação apropriada, apresentando em até 30 dias após a data indicada na Ordem de Início de Serviço (OIS), os certificados de especialização dos profissionais envolvidos nas atividades.

8.2 Os profissionais envolvidos nas atividades implantação, migração, treinamento e suporte técnico deverão comprovadamente pertencer ao quadro próprio da CONTRATADA ou do FABRICANTE, devendo ser comprovado tal vínculo através de documentação apropriada em até 30 dias após a data indicada na Ordem de Início de Serviço (OIS):

8.3 A CONTRATADA deverá comprovar que possui em seu quadro funcional, no mínimo, 01 (um) profissional com ao menos 01 (uma) certificação oficial dos produtos BeyondTrust relacionados com a presente contratação. Para comprovar a certificação, a CONTRATADA deverá apresentar os certificados de formação oficial do fabricante, bem como documentação que comprove o vínculo do profissional certificado com a CONTRATADA.

8.4 A ITAIPU se reserva o direito de não aceitar atendimento por profissionais não qualificados, devendo a CONTRATADA substituir imediatamente o profissional de forma a não comprometer o atendimento final.

9. CONDIÇÕES DE FORNECIMENTO E ACEITE

9.1 A ITAIPU somente emitirá o aceite da solução após o devido recebimento, avaliação Técnica de todos os itens constantes deste processo e constatação de que estão em concordância com o especificado.

9.2 A CONTRATADA deverá emitir junto ao faturamento mensal, um relatório de qualidade dos serviços, informando a quantidade de chamados ao suporte remoto e seus respectivos tempos de atendimento no período, confrontando-os com o SLA especificado no item 6.8 (Tabela 3).

9.3 A CONTRATADA deverá apresentar a comprovação de registro dos softwares junto ao fabricante, evidenciando o devido licenciamento e demais garantias.

9.4 A CONTRATADA deverá apresentar a comprovação de que o suporte registrado junto a BeyondTrust para os produtos contratados se encaixa em modalidade adequada para as exigências desta especificação.

9.5 A CONTRATADA é responsável pelo correto comportamento e eficiência do seu pessoal, comprometendo-se a prestar os serviços com pessoal técnico especializado nas atividades a serem desenvolvidas a fim de concluir eficientemente as solicitações de serviço abertas.

10. AMBIENTE TECNOLÓGICO DA ITAIPU

10.1 Servidores Microsoft Windows Server 2003 e superiores (32-bits e 64-bits).

10.2 Servidores Red Hat Enterprise Linux 6 e superiores (64-bit).

10.3 Plataforma de virtualização Vmware ESXi 5.5 e superiores.

10.4 Desktops: Windows 7 e superiores (32-bits e 64-bits).

10.5 Microsoft 365 E3, E5, F3.

10.6 Splunk SIEM.

10.7 Service-Now ITSM.