COTAÇÃO DE PREÇOS

Brasília/DF, 30 de setembro de 2025.

Senhor Fornecedor,

Solicitamos a gentileza de apresentar proposta de preços para a(s) aquisição(ões) do(s) material(is) e/ou serviço(s) especificado(s) abaixo, **até o dia 14/10/2025.**

ITEM	ESPECIFICAÇÃO
1.	Contratação de soluções de segurança cibernética visando à proteção contínua dos ativos informacionais da Instituição, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação. As orientações estão contidas na Especificação Técnica abaixo. **ATENÇÃO:** Os critérios de seleção do fornecedor serão por técnica e preço e por item. Diante disso, o proponente poderá cotar somente o(s) item(ns) que irá ofertar, individualizando a solução, a implementação e o repasse de conhecimento. Os itens que não cotar ou que não há custo, informar o valor de R$ 0,00. Os valores cotados devem ser em Reais.

I) QUESTINAMENTOS

1. Deverão ser encaminhados para gecoc.eqcbe@poupex.com.br. **O prazo para recebimento de questionamentos é de até 2 dias úteis antes do fim do prazo para recebimento da proposta comercial e da documentação.**

II) A PROPOSTA DEVERÁ CONTER

1. Dados da empresa (CNPJ, Razão Social, endereço e contato);
2. Especificação detalhada do produto/serviço;
3. Garantia do material e do serviço, quando o caso;
4. Valor unitário, valor total e unidade de medida (valores em reais);
5. Incluir no valor dos itens, impostos e demais taxas;
6. Prazo para entrega em dias úteis ou corridos;
7. Validade da proposta (pelo menos 30 dias úteis);
8. Data da proposta atualizada;
9. **Forma de pagamento (liquidado em até 10 dias úteis após o aceite do material ou da conclusão da execução do serviço, mediante a apresentação da correspondente nota fiscal, por meio de transferência bancária ou boleto bancário);**
10. Dados bancários (conta jurídica - vinculada ao CNPJ); e
11. Assinatura do responsável.

III) NORMAS ESPECÍFICAS

2. Incluso no valor do material e/ou serviço todos os custos diretos e indiretos para perfeita execução dos trabalhos, inclusive as despesas com materiais, mão de obra, transportes, custos financeiros, encargos e impostos necessários.
3. A proposta poderá ser enviada por e-mail para: gecoc.eqcbe@poupex.com.br.
4. A entrega e/ou execução de serviço deverá(ão) ser realizada(s) no endereço.: Avenida Duque de Caxias S/N, Parte "A", Setor Militar Urbano - CEP: 70630-902 - Brasília-DF – ALMOXARIFADO.
5. **A CONTRATADA, em conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 2018, está ciente que a POUPEX coletará dados pessoais dos titulares responsáveis pela empresa, no momento da contratação, e que os dados coletados serão objeto de tratamento e estarão sujeitos à publicidade.**

IV) DADOS PARA ENVIO DA PROPOSTA E AMOSTRA FÍSICA (QUANDO FOR O CASO)

ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO – POUPEX
CNPJ: 00.655.522/0001-21

Endereço: Avenida Duque de Caxias S/N, Parte “A”, Setor Militar Urbano - CEP: 70630-902 - Brasília-DF.
Divisão de Gestão de Compras – Equipe de Compras de Bens – DIGEC/EQCBE
Fones: (61) 3314-7633/3314-7635/3314-7780/3314-7880
WhatsApp: (61) 3314-7585

1 – OBJETO

Contratação de soluções de segurança cibernética visando à proteção contínua dos ativos informacionais da Instituição, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação.

2 – JUSTIFICAVA

O cenário digital atual é caracterizado por uma crescente sofisticação e frequência dos ataques cibernéticos. Instituições financeiras, em especial, têm se tornado alvos preferenciais de ameaças que exploram vulnerabilidades técnicas, falhas humanas e lacunas nos processos de segurança.

Diante desse contexto, é imprescindível que a Instituição mantenha sua infraestrutura de segurança cibernética constantemente atualizada, adotando soluções modernas, integradas e capazes de atuar de forma coordenada nas etapas de prevenção, detecção, resposta e recuperação. A incorporação de tecnologias avançadas não representa apenas uma medida de proteção, mas uma estratégia essencial para assegurar a continuidade dos negócios, a confiança dos clientes e a resiliência organizacional.

As abordagens tradicionais, quando operadas de forma isolada, já não são suficientes para enfrentar ameaças que evoluem rapidamente e utilizam múltiplos vetores de ataque simultaneamente. Por isso, torna-se necessário adotar uma postura proativa, baseada em inteligência artificial, automação de respostas e visibilidade em tempo real sobre os ativos e comportamentos da rede.

Considerando que, mesmo com investimentos contínuos, os riscos cibernéticos permanecem como uma ameaça constante, é fundamental implementar uma arquitetura de segurança em camadas, especialmente nos ambientes críticos da Instituição. Essas camadas devem atuar de forma integrada para proteger os recursos tecnológicos e as informações estratégicas, garantindo a integridade, a disponibilidade e a confidencialidade dos dados.

A adoção dessas soluções reforça o compromisso da Instituição com a segurança de suas operações e sua capacidade de enfrentar, com agilidade e eficácia, os desafios impostos pelo atual cenário de ameaças digitais.

3 – DESCRIÇÃO DA SOLUÇÃO

As soluções de segurança deverão ser fornecidas por meio de licenciamento anual, contemplando todos os componentes necessários para sua plena operação, incluindo software, atualizações, suporte técnico e documentação. O modelo de fornecimento será tradicional, com licenças válidas por 12 meses, renováveis conforme a necessidade da Instituição, garantindo o funcionamento integral das funcionalidades contratadas durante todo o período de vigência.

A solução deverá oferecer acesso contínuo a atualizações de segurança, correções de vulnerabilidades, melhorias de desempenho e novas funcionalidades disponibilizadas pelo fabricante, sem custos adicionais durante o período de licenciamento. O suporte técnico deverá ser prestado exclusivamente pelo fabricante da solução, assegurando maior eficiência na resolução de incidentes e alinhamento com as melhores práticas da tecnologia ofertada. O serviço deverá estar disponível em regime 24x7, com atendimento remoto e escalonamento conforme a criticidade dos chamados.

A empresa contratada será responsável por fornecer os meios necessários para ativação, instalação e configuração inicial da solução, além de disponibilizar manuais, guias técnicos e acesso à base de conhecimento. A solução deverá ser compatível com o ambiente tecnológico da POUPEX e permitir integração com outras ferramentas de segurança já existentes, quando aplicável.

A efetividade da solução será avaliada por meio de relatórios técnicos, indicadores de desempenho e evidências de funcionamento, conforme critérios definidos pela área técnica da Instituição. A aquisição tem como objetivo assegurar

a continuidade da proteção dos ativos de informação da Instituição, com foco na prevenção, detecção e resposta a ameaças cibernéticas, alinhando-se às melhores práticas de mercado.

Quantitativo de Bens e/ou Serviços

Nº	Bens e/ou Serviços	Quantidade
1.1	Solução de *Endpoint* com EDR para servidores (A solução deve vir com o suporte técnico do fabricante incluso.)	500
1.2	Implementação da solução de *Endpoint* com EDR para servidores.	1
1.3	Repasse de conhecimento da solução de *Endpoint* com EDR para servidores.	1
2.1	Solução de Gestão de Vulnerabilidades (A solução deve vir com o suporte técnico do fabricante incluso.)	1
2.2	Implementação da solução de Gestão de Vulnerabilidades.	1
2.3	Repasse de conhecimento da solução de Gestão de Vulnerabilidades.	1
3.1	Solução de *Breach and Attack Simulation* – BAS (A solução deve vir com o suporte técnico do fabricante incluso.)	1
3.2	Implementação da solução de *Breach and Attack Simulation* – BAS.	1
3.3	Repasse de conhecimento da solução de *Breach and Attack Simulation* – BAS.	1
4.1	Solução de Conformidade Equipamentos de Terceiro – NAC (A solução deve vir com o suporte técnico do fabricante incluso.)	2200
4.2	Implementação da solução de Conformidade Equipamentos de Terceiro – NAC.	1
4.3	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC.	1
5.1	Solução de Inteligência Cibernética – OSINT (A solução deve vir com o suporte técnico do fabricante incluso.)	1
5.2	Implementação da solução de Inteligência Cibernética – OSINT.	1
5.3	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT.	1
6.1	Solução de Cofre de Senha e Gestão de Altas Credenciais – PAM (A solução deve vir com o suporte técnico do fabricante incluso.)	1
6.2	Implementação da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1
6.3	Repasse de conhecimento da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1

Especificação das Soluções

ITEM 1 – SOLUÇÃO DE ENDPOINT COM EDR PARA SERVIDORES
Solução de segurança centralizada voltada à proteção avançada de servidores contra ameaças digitais como vírus, *worms*, *ransomware*, *trojans* e ataques de dia zero. Monitora continuamente o comportamento dos sistemas, detecta atividades suspeitas em tempo real e responde automaticamente a incidentes, garantindo integridade, disponibilidade e conformidade dos ambientes críticos.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 1.2 e 1.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

ITEM 2 – SOLUÇÃO DE GESTÃO DE VULNERABILIDADES
Ferramenta especializada na identificação proativa de falhas de segurança em sistemas, aplicações e dispositivos de rede. Realiza varreduras automatizadas e abrangentes, detectando vulnerabilidades conhecidas, configurações incorretas e exposições a riscos. Fornece relatórios detalhados e priorização de correções, apoiando a gestão contínua da postura de segurança e a conformidade com normas como PCI-DSS, ISO 27001 e LGPD.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 2.2 e 2.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

ITEM 3 – SOLUÇÃO DE *BREACH AND ATTACK SIMULATION – BAS*
Plataforma que simula ataques cibernéticos reais de forma controlada para avaliar, em tempo real, a eficácia das defesas de segurança da organização. Testa continuamente controles como *firewall*, *EDR*, *AntiSpam* e políticas de resposta, identificando brechas e vulnerabilidades antes que sejam exploradas. Gera *insights* acionáveis para fortalecer a postura de segurança, acelerar a correção de falhas e garantir conformidade com *frameworks* como *MITRE ATT&CK*.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 3.2 e 3.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

ITEM 4 – SOLUÇÃO DE CONFORMIDADE DE EQUIPAMENTOS DE TERCEIROS – NAC
Plataforma que garante o acesso seguro à rede corporativa, identificando, classificando e controlando todos os dispositivos conectados — sejam gerenciados ou não. Avalia a conformidade com políticas de segurança antes de permitir o acesso, isolando ou bloqueando dispositivos não autorizados ou vulneráveis. Suporta ambientes com políticas de *BYOD (Bring Your Own Device)*, oferecendo visibilidade e controle sobre dispositivos pessoais, e integra-se a outras soluções de cibersegurança para fortalecer a proteção contra ameaças internas e externas.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 4.2 e 4.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

ITEM 5 – SOLUÇÃO DE INTELIGÊNCIA CIBERNÉTICA – *OSINT*
Ferramenta voltada à coleta, análise e correlação de informações públicas disponíveis em fontes abertas como redes sociais, fóruns, sites, domínios e repositórios técnicos. Auxilia na identificação de ameaças externas, exposição de dados sensíveis, perfis de atacantes e riscos reputacionais. Essencial para operações de *threat intelligence*, investigação digital e monitoramento preventivo de ativos expostos na internet.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 5.2 e 5.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

ITEM 6 – SOLUÇÃO DE COFRE DE SENHA E GESTÃO DE ALTAS CREDENCIAIS – *PAM*
Plataforma que protege, controla e audita o uso de credenciais privilegiadas em ambientes corporativos. Armazena senhas de forma segura em cofres criptografados, automatiza a rotação de credenciais e aplica políticas de acesso

baseado em risco e necessidade. Reduz a superfície de ataque, evita uso indevido de contas administrativas e garante conformidade com normas como ISO 27001, LGPD e NIST.
Caso seja necessário a contratação dos serviços de implementação e repasse de conhecimento, itens 6.2 e 6.3, estes deverão ser prestados pela mesma empresa que forneceu a solução.
Os requisitos obrigatórios e desejáveis encontram-se detalhados no **Anexo II**.

IMPLEMENTAÇÃO
A contratada será responsável pela instalação, configuração e validação inicial da solução, garantindo sua plena operação conforme os requisitos técnicos definidos pela contratante.
Caso a(s) solução(ões) a ser(em) contratada(s) já esteja(m) em operação na CONTRATANTE, não haverá a contratação deste item.
O valor da implementação deverá ser apresentado individualmente para cada solução ofertada, quando aplicável.

REPASSE DE CONHECIMENTO
Serão realizadas atividades de repasse de conhecimento técnico às equipes da contratante, com foco na solução implementada, visando assegurar o entendimento aprofundado de sua arquitetura, funcionalidades e procedimentos operacionais. Esse processo tem como objetivo promover autonomia na gestão e manutenção da solução. O repasse de conhecimento poderá ser disponibilizado também sob demanda, por meio de acesso a plataformas especializadas oferecidas pelo fabricante, proporcionando maior flexibilidade e continuidade no processo de assimilação técnica.
Caso a(s) solução(ões) a ser(em) contratada(s) já esteja(m) em operação na CONTRATANTE, não haverá a contratação deste item.
O valor do repasse de conhecimento deverá ser apresentado individualmente para cada solução ofertada, quando aplicável.

SUPORTE TÉCNICO
O suporte técnico deverá estar incluso no licenciamento e prestado exclusivamente pelo fabricante da solução, assegurando domínio completo da tecnologia ofertada e maior eficiência na identificação e resolução de incidentes. O serviço deverá estar disponível em regime 24x7, com atendimento remoto e escalonamento conforme a criticidade dos chamados, assegurando a continuidade operacional da solução durante todo o período de vigência do contrato.

4 – DEVERES E RESPONSABILIDADES DA CONTRATANTE

Nº	Descrição
1	A CONTRATANTE deverá fornecer a infraestrutura, os dados e as informações necessárias para o funcionamento e parametrização da solução, além da equipe técnica para acompanhamento das atividades.
2	Disponibilizar os acessos necessários às informações da Instituição, desde que atenda os critérios de segurança estipulados pela CONTRATANTE.
3	Cumprir todas as normas e condições do Instrumento Contratual.
4	Efetuar os pagamentos devidos à CONTRATADA, na forma convencionada, dentro do prazo previsto, desde que atendidas às formalidades necessárias.
5	Aplicar as penalidades previstas para o caso de descumprimento de cláusulas contratuais ou quando não acatada a justificativa apresentada pela CONTRATADA.
6	Nomear o Gestor do Contrato e os Fiscais Técnicos, visando garantir a eficácia na execução dos serviços contratados, devendo estes:

	• Posicionar e repassar as ocorrências aos níveis hierárquicos competentes; • Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos; • Anotar em registro próprio as falhas detectadas e exigir as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato; • Conferir os serviços prestados e atestar os documentos fiscais pertinentes, podendo suspender qualquer procedimento que não esteja em acordo com os termos contratuais; • Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados, adotando todas as providências necessárias e tratando os desvios; e • Notificar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA, bem como quanto as ocorrências relativas ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para a CONTRATANTE.

5 – DEVERES E RESPONSABILIDADES DA CONTRATADA

Nº	Descrição
1	Propiciar todos os meios e facilidades necessárias à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária.
2	Comunicar à CONTRATANTE, por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários e propondo alternativas para mitigação dos impactos.
3	Auxiliar a equipe técnica da CONTRATANTE na implementação do plano de ação, fornecendo orientações e suporte técnico necessário para garantir o funcionamento adequado da solução.
4	A CONTRATADA não poderá realizar alterações nos ambientes computacionais preexistentes da CONTRATANTE, salvo mediante autorização formal e prévia, respeitando os limites definidos pela área técnica.
5	Indicar representante junto à CONTRATANTE, responsável pela fiel execução do contrato, devendo ser substituído prontamente em caso de indisponibilidade.
6	Atender prontamente às orientações e exigências do Gestor ou Fiscal do contrato, observando os prazos e critérios definidos para a execução dos serviços.
7	Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE.
8	Prestar os serviços dentro dos parâmetros e rotinas estabelecidos na especificação técnica, com observância às recomendações aceitas pela boa técnica, normas e legislação.
9	Responsabilizar-se pela conduta e qualificação técnica dos profissionais envolvidos na execução do contrato.

10	Manter a confidencialidade dos dados, informações e documentos acessados aos quais venha a ter acesso em decorrência da prestação dos serviços contratados, sendo esta obrigação extensiva a seus sócios, diretores, mandatários, assim como todos os empregados envolvidos na contratação.
11	Estar em conformidade com a Lei nº 13.709 (LGPD), incluindo a obrigação de reportar à CONTRATANTE qualquer incidente de segurança envolvendo dados pessoais.

6 – GESTÃO CONTRATUAL

Execução Contratual

Prazos

Validação dos requisitos funcionais – Em até 3 (três) dias úteis, após a convocação formal da empresa que apresentar melhor pontuação no quesito técnica e preço.

Assinatura do instrumento contratual – Em até 5 (cinco) dias úteis após aprovação da fase de validação.

Os prazos das etapas serão conforme quadro abaixo e, pelo fato de as soluções serem individualizadas, os prazos estabelecidos de cada etapa para cada solução serão contabilizados de forma simultânea, iniciando-se a partir da assinatura do instrumento contratual, sem execução sequencial por produto:

Nº	ENTREGAS	PRAZO
1.1	Apresentação de plano de implementação e entrega da subscrição da solução *Endpoint* com EDR para servidores.	Em até 7 dias úteis, após a assinatura do contrato.
1.2	Implementação da solução *Endpoint* com EDR para servidores, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
1.3	Repasse de conhecimento da solução *Endpoint* com EDR para servidores, se necessário.	Em até 7 dias úteis, após a implementação da solução.
2.1	Apresentação de plano de implementação e entrega da subscrição da solução de Gestão de Vulnerabilidades.	Em até 7 dias úteis, após a assinatura do contrato.
2.2	Implementação da solução de Gestão de Vulnerabilidades, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
2.3	Repasse de conhecimento da solução de Gestão de Vulnerabilidades, se necessário.	Em até 7 dias úteis, após a implementação da solução.
3.1	Apresentação de plano de implementação e entrega da subscrição da solução *de Breach and Attack Simulation* – BAS.	Em até 7 dias úteis, após a assinatura do contrato.
3.2	Implementação da solução de *Breach and Attack Simulation* – BAS, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
3.3	Repasse de conhecimento da solução de *Breach and Attack Simulation* – BAS, se necessário.	Em até 7 dias úteis, após a implementação da solução.
4.1	Apresentação de plano de implementação e entrega da subscrição da solução de Conformidade Equipamentos de Terceiro – NAC.	Em até 7 dias úteis, após a assinatura do contrato.
4.2	Implementação da solução de Conformidade	Em até 15 dias úteis, após a

	Equipamentos de Terceiro – NAC, se necessário.	apresentação do plano de implementação.
4.3	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC, se necessário.	Em até 7 dias úteis, após a implementação da solução.
5.1	Apresentação de plano de implementação e entrega da subscrição da solução de Inteligência Cibernética – OSINT.	Em até 7 dias úteis, após a assinatura do contrato.
5.2	Implementação da solução de Inteligência Cibernética – OSINT, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
5.3	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT, se necessário.	Em até 7 dias úteis, após a implementação da solução.
6.1	Apresentação de plano de implementação e entrega da subscrição da solução Cofre de Senha e Gestão de Altas Credenciais – PAM.	Em até 7 dias úteis, após a assinatura do contrato.
6.2	Implementação da solução Cofre de Senha e Gestão de Altas Credenciais – PAM, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
6.3	Repasse de conhecimento da solução Cofre de Senha e Gestão de Altas Credenciais – PAM, se necessário.	Em até 7 dias úteis, após a implementação da solução.

Vigência da(s) Solução(ões): Por 12 (doze) meses podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 120 (cento e vinte) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea:

- os serviços tenham sido prestados regularmente;
- a CONTRATADA não tenha sofrido qualquer punição de natureza pecuniária;
- a CONTRATANTE ainda tenha interesse na realização do serviço;
- o valor do instrumento contratual permaneça economicamente vantajoso para a CONTRATANTE; e
- a CONTRATADA concorde com a prorrogação do instrumento contratual.

Horários	Todas as atividades deverão ser realizadas, preferencialmente, no horário comercial, compreendido entre 08h00 e 18h00, de segunda a sexta-feira.
Locais de Entrega	A entrega da(s) solução(ões) será(ão) realizada(s) de forma digital, por meio de disponibilização remota dos softwares e respectivos componentes. A execução dos serviços de implementação e repasse de conhecimento, se necessário, deverá ocorrer de forma remota.

Comunicação entre Contratante e Contratada

A comunicação formal entre a CONTRATANTE e a CONTRATADA deverá ser realizada preferencialmente por meio de sistema de gerenciamento de chamados, envolvendo o preposto da CONTRATADA e o Gestor ou Fiscal designado pela CONTRATANTE. Alternativamente, poderá ser utilizada comunicação por correio eletrônico institucional, desde que haja registro e rastreabilidade das interações. Todas as tratativas relacionadas à execução do contrato deverão ser documentadas, garantindo transparência, controle e histórico das ações.

Forma de Pagamento

O(s) pagamento(s) da(s) solução(ões), será(ão) efetuado(s) pela CONTRATANTE, após a emissão do Termo de Recebimento e Aceitação dos Serviços, via transferência bancária, mediante entrega da(s) Nota(s) Fiscal(is)/fatura(s), após término da prestação dos serviços, em até o 10º (décimo) dia útil, mediante atesto(s) na(s) Nota(s) Fiscal(is)/Fatura(s) a ser(em) apresentada(s) com 10 (dez) dias do vencimento.
O pagamento da implantação e do repasse de conhecimento, se for o caso, será(ão) efetuado(s) pela CONTRATANTE, após a emissão do Termo de Recebimento e Aceitação dos Serviços, via transferência bancária, mediante entrega da(s) Nota(s) Fiscal(is)/fatura(s), após término da prestação dos serviços, em até o 10º (décimo) dia útil, mediante atesto(s) na(s) Nota(s) Fiscal(is)/Fatura(s) a ser(em) apresentada(s) com 10 (dez) dias do vencimento.

A CONTRATADA deverá observar este prazo ao preencher o vencimento da Nota Fiscal e enviá-la para o e-mail pagamento.gecoc@poupex.com.br

O pagamento será efetuado por conta corrente, cadastrada com o mesmo CNPJ constante da Nota Fiscal, sob o risco de devolução da referida Nota.

A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas Notas Fiscais nesse prazo, essas deverão ser emitidas com data do 1º (primeiro) dia do mês subsequente.

Acompanhamento e fiscalização (incluindo a indicação de gestor e fiscais)

No momento da assinatura do instrumento contratual, a CONTRATADA indicará um representante que será responsável por acompanhar a execução do instrumento contratual e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

A existência e a atuação da fiscalização pela CONTRATANTE em nada restringem a responsabilidade, única, integral e exclusiva da CONTRATADA, no que concerne à execução do instrumento contratual.

No momento da assinatura do instrumento contratual, a CONTRATANTE indicará a equipe de fiscalização da Contratação, composta por:

- **Gestor do Contrato**: Será indicado no momento da assinatura do contrato.
- **Fiscais Técnicos**: Serão indicados no momento da assinatura do contrato.

Acordo de níveis de serviço - ANS

1. **Acordo de Nível de Serviço para Chamados de Suporte Técnico**
   1.1. O suporte técnico será prestado diretamente pelo fabricante da solução mediante abertura de chamado por parte da CONTRATANTE e o Acordo de Nível de Serviço – ANS obedecerá ao descrito na plataforma do fabricante, sendo obrigatoriamente na modalidade de 24 x 7 para resolução de incidentes e demandas.
   1.2. Pelo fato de o ANS ser prestado diretamente pelo fabricante, não será aplicado o Fator de Redução de Chamado – FRC e o Fator de Redução de Disponibilidade – FRD.

Privacidade e Proteção de Dados Pessoais

Endpoint com EDR – servidores
• POUPEX: Controlador (determina proteção dos ativos corporativos).

• Fornecedor: Operador. (executa a análise dos dados em nome da POUPEX)
• Risco: Alto
• Justificativa: há tratamento de dados pessoais nos logs, e classificado como alto por processar alto volume de dados e exercer monitoramento contínuo.

Gestão de Vulnerabilidades e BAS (Breach and Attack Simulation)
• POUPEX: Controlador (define escopo e sistemas a avaliar).
• Fornecedor: Operador (aplica scanners, relatórios e executa simulações).
• Risco: Baixo
• Justificativa: não envolve dados pessoais diretamente.

Conformidade de Equipamentos de Terceiro e NAC
• POUPEX: Controlador (define quem pode ou não acessar a rede).
• Fornecedor: Operador.
• Risco: Alto
• Justificativa: há tratamento de dados pessoais nos logs, e classificado como alto por processar alto volume de dados e exercer monitoramento contínuo.

Inteligência Cibernética (OSINT)
• POUPEX: Controlador (solicita monitoramento de ameaças para proteger sua estrutura).
• Fornecedor: pode atuar como Controlador Independente quando coleta e trata dados em bases próprias para fins de threat intelligence.
• Risco: Baixo
• Justificativa: não envolve dados pessoais diretamente.

Cofre de Senhas e Gestão de Altas Credenciais
• POUPEX: Controlador (define quais credenciais precisam ser geridas).
• Fornecedor: Operador (administra cofres e acessos).
• Risco: Médio
• Justificativa: há tratamento de dados pessoais nos logs, e não atende aos critérios de alto risco.

Critérios de Recebimento do Objeto	
Critério 1	
Indicador de Qualidade	Prazos das entregas previstas no item 6 – GESTÃO CONTRATUAL.
Mínimo aceitável	100% dos prazos previstos no item 6 – GESTÃO CONTRATUAL.
Métrica	Prazo das entregas igual ao previsto no cronograma do item 6 – GESTÃO CONTRATUAL.
Ferramentas	Acompanhamento e validação dos representantes da CONTRATANTE, mediante relatório de acompanhamento apresentado pela CONTRATADA.
Periodicidade Aferição	Conforme cronograma de entregas definido no item 6 – GESTÃO CONTRATUAL.
Critério 2 – Implementação da Solução	
Indicador de Qualidade	Conclusão da implementação conforme escopo técnico e cronograma apresentado pela CONTRATADA.
Mínimo aceitável	100% das funcionalidades implementadas e operacionais.

Métrica	Validação técnica da CONTRATANTE com base em testes de funcionamento e checklist de entrega.
Ferramentas	Relatório técnico de implementação e Termo de Aceite.
Periodicidade Aferição	Ao final da etapa de implementação.
Critério 3 – Repasse de Conhecimento	
Indicador de Qualidade	Realização de repasse de conhecimento e entrega de materiais de apoio.
Mínimo aceitável	100% das ações previstas no plano de repasse de conhecimento.
Métrica	Participação das equipes e entrega de materiais.
Ferramentas	Relatórios de repasse de conhecimento e listas de presença.
Periodicidade Aferição	Ao final da etapa de repasse de conhecimento.

Sanções

- O inadimplemento total ou parcial das obrigações contratuais dá, à CONTRATANTE, o direito de aplicar as seguintes penalidades:

- Advertência, quando der causa à inexecução parcial do contrato, desde que não cause grave dano à CONTRATANTE;

- Multa, que poderá ser aplicada por descumprimento de quaisquer obrigações contratuais, calculada em percentual de 0,5% a 30% incidente sobre o valor total anual do contrato, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, ou descontada das parcelas devidas à CONTRATADA, sem prejuízo de outras sanções previstas contratualmente;

- Rescisão unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais;

- Em caso de atraso nos prazos para implementação, repasse de conhecimento e entrega das subscrições serão enquadrados como inexecução parcial do contrato;

- Será considerado como inexecução total do contrato, podendo incorrer rescisão contratual, as situações a partir de 3 (três) enquadramentos parciais consecutivos;

- Em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico;

- As multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades;

- Não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves;

- Sendo rescindido o presente contrato, o pagamento devido será proporcional aos serviços prestados até a data da resolução;

- Para se ressarcir de eventuais prejuízos causados pela CONTRATADA e do valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar esses valores dos créditos decorrentes deste mesmo contrato ou de outros contratos que a CONTRATADA possua com a CONTRATANTE;

- Caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA; e

- No processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

7 – VÍNCULO ORÇAMENTÁRIO

Itens n.º	Conta Contábil
1.1, 2.1, 3.1, 4.1, 5.1 e 6.1	**DESENVOLVIMENTO, LICENCA DE USO E MANUTENCAO SISTEMAS - 678.817390000010005**
1.2, 2.2, 3.2, 4.2, 5.2 e 6.2	**PESSOAL ESPECIALIZADO PROCESSAMENTO DADOS - 678.817390000010001**
1.3, 2.3, 3.3, 4.3, 5.3 e 6.3	**SERVICOS DE CONSULTORIA DE TI PESSOAS JURIDICAS - 678.817630000000008**

8 – CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

ADJUDICAÇÃO DO OBJETO ☐ Preço global ☐ Por lote ☒ Por item ☒ Técnica e Preço

Habilitação e Proposta Técnica e Comercial

A empresa participante deverá encaminhar a seguinte documentação:

1. **Proposta Técnica Comercial:**
   - 1.1. Proposta de preços, contendo especificação completa de cada solução ofertada, com no mínimo o solicitado neste documento, além do detalhamento do suporte técnico do fabricante que deverá ser entregue conforme modelo, Anexo I, em papel timbrado da empresa, devidamente assinada pelo responsável e deverá ainda contemplar:
     - 1.1.1. Nome da(s) solução(ões), modalidade(s) e fabricante(s) ofertado(s) (se for o caso);
     - 1.1.2. A implementação e repasse de conhecimento deverão ser cotados na forma remota.
     - 1.1.3. Valor unitário, valor total e unidade de medida (valores em reais);
     - 1.1.4. Dados da empresa (CNPJ, razão social e contato do responsável);
     - 1.1.5. Valor e cronograma de implementação e repasse de conhecimento, se houver;
     - 1.1.6. Declarar na Proposta Comercial a concordância com a forma de faturamento estabelecido no item 6 - GESTÃO CONTRATUAL, subitem Forma de Pagamento;
     - 1.1.7. Dados bancários da empresa (conta jurídica);
     - 1.1.8. Data da proposta atualizada, com validade de pelo menos 60 (sessenta) dias corridos.
     - 1.1.9. Incluir nos preços todos os custos e despesas que, direta ou indiretamente, que decorram das obrigações a serem, tais como e sem se limitar a: telefone, transporte, passagens e diárias, hospedagem, deslocamento, alimentação, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, softwares, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

1.2. Encaminhar devidamente preenchido e assinado pelo responsável o questionário, Anexo II, dos requisitos obrigatórios e desejáveis da(s) solução(ões) ofertada(s); e
1.3. Encaminhar o *Datasheet* (documento que contém informações detalhadas sobre as características e especificações técnicas) de cada solução ofertada.

2. Declarações, conforme Anexo III

2.1. **Declaração de menor** – documento que comprove que a empresa não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º da Constituição Federal;
2.2. **Declaração Auditoria e Plano de Continuidade de Negócio** – a CONTRATADA deverá declarar se é acompanhada por auditoria interna ou externa, se responsabilizando pela veracidade das informações prestadas, estando sujeita a sanções na forma da lei e sobre a existência de plano de continuidade de negócios, garantindo a prestação de serviços conforme estabelecido no item 3 - DESCRIÇÃO DA SOLUÇÃO e 4 ESPECIFICAÇÃO DA SOLUÇÃO, se responsabilizando pela veracidade das informações prestadas;
2.3. **Declaração de atendimento quanto à especificação técnica** – documento que comprove que a empresa atende aos requisitos e critérios estabelecidos na Especificação Técnica e aceita a Minuta de Contrato;

3. Atestado de Capacidade Técnica

3.1. Para fins de qualificação técnica a CONTRATADA deverá apresentar atestado(s) de capacidade técnica, em seu nome (incluindo o CNPJ), emitidos por empresas públicas ou privadas que comprovem o fornecimento e a prestação de serviços de implementação e repasse de conhecimento da(s) solução(ões) ofertada(s);

4. Certidão Negativa de Falência ou Recuperação Judicial

5. Demais exigências

5.1. Documentação informando os critérios utilizados na contratação de serviços em nuvem; e
5.2. Documentação informando os controles de segurança adotados referentes aos serviços em nuvem para assegurar a proteção e privacidade dos dados dos clientes.

6. Participação SPE ou de Consórcio

6.1.1. Em caso de participação na modalidade de SPE (Sociedade de Propósito Específico) ou Consórcio deverão ser apresentados os seguintes documentos:
6.1.1.1. comprovação de compromisso público ou particular de constituição de Consórcio, subscrito pelos consorciados; e
6.1.1.2. indicação da empresa líder do Consórcio, que será responsável por sua representação perante a POUPEX.
6.1.2. Será admitida, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado.
6.1.3. Fica impedida de a empresa consorciada participar, no mesmo processo de compra, de mais de um Consórcio ou de forma isolada;
6.1.4. Os integrantes são responsáveis solidariamente pelos atos praticados em Consórcio, tanto na fase de cotação quanto na de execução do contrato.
6.1.5. Deverão ser considerados:
6.1.5.1. o vencedor é obrigado a promover, antes da celebração do contrato, a constituição e o registro do Consórcio.
6.1.5.2. a substituição de consorciado deverá ser expressamente autorizada pela POUPEX e condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do Consórcio no processo de compra que originou o contrato.
6.1.5.3. em caso de apresentação de atestado de desempenho anterior emitido em favor de Consórcio do qual tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica:

6.1.5.3.1. caso o atestado tenha sido emitido em favor de Consórcio homogêneo, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio; e

6.1.5.3.2. caso o atestado tenha sido emitido em favor de Consórcio heterogêneo, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação.

6.1.5.4. para fins de comprovação do percentual de participação do consorciado, caso este não conste expressamente do atestado ou da certidão, deverá ser juntada ao atestado ou à certidão cópia do instrumento de constituição do Consórcio.

7. Prova de validação de requisitos

7.1. Após definição da empresa com maior pontuação, considerando técnica e preço, além de atender aos critérios de seleção - qualificação da empresa, constantes nesta Especificação Técnica, esta será convocada para apresentação da solução como forma de validar requisitos funcionais e não funcionais obrigatórios e/ou desejáveis.

7.2. A realização da validação funcional e não funcional dos requisitos obrigatórios ou desejáveis será somente entre a Equipe Técnica da CONTRATANTE e a Equipe Técnica da empresa convocada, e ao término desta etapa será elaborado relatório técnico.

7.3. Os requisitos funcionais e não funcionais previstos na especificação técnica que o fornecedor confirmar atendimento, comporão o instrumento Contratual, sendo passíveis de aplicação de sanções e penalidades.

Caso a POUPEX considere necessário, poderá solicitar esclarecimentos e/ou documentos adicionais.

Julgamento

Critério

A POUPEX realizará o julgamento conforme a seguinte metodologia:

1. Somente serão aceitas as soluções que atendam a todos os itens obrigatórios.
2. A pontuação da qualificação técnica será calculada conforme fórmula:
   NQT = (NQE / MNQA) * 70, sendo:
   - NQT = Nota da Qualificação Técnica;
   - NQE = Nota do Questionário da Empresa em questão;
   - MNQA = Maior Nota dos Questionários Apresentados.
3. A pontuação da proposta de preço será calculada conforme fórmula:
   NPP = (MPVO / VP) * 30, sendo:
   - NPP = Nota da Proposta de Preço;
   - MPVO = Menor Preço Válido Ofertado;
   - VP = Valor da Proposta em questão.
4. A pontuação final do fornecedor será calculada conforme fórmula:
   NFF = NQT + NPP, sendo:
   - NFF = Nota Final do Fornecedor;
   - NQT = Nota da Qualificação Técnica;
   - NPP = Nota da Proposta de Preço.

Obs.: O arredondamento será feito até a quarta casa decimal após a vírgula.

Justificativa

Buscar a proposta mais vantajosa para a POUPEX, por meio do atendimento dos critérios definidos neste instrumento.

ANEXO I

MODELO DE PROPOSTA COMERCIAL

A _____ (razão social – nome fantasia), sediada no endereço _____, CEP _____, inscrita no CNPJ n.º_____, (IE ou IM ou CF/DF), neste ato, representada por seu _____(sua) (cargo), conforme (documento - contrato social, procuração) _____, Sr.(a) _____(nome completo), CPF n.º _____, da CI n.º _____(número e órgão emissor), _____(nacionalidade), _____(estado civil), _____(profissão), residente e domiciliado (a) _____, vem apresentar sua proposta comercial para fornecimento da(s) solução(ções) de segurança cibernética visando à proteção contínua dos ativos informacionais, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação, conforme abaixo:

Item	Descrição	QTD	Valor Unitário	Valor Anual
1.1	Solução de *Endpoint* com EDR para servidores Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	500		
1.2	Implementação da solução de *Endpoint* com EDR para servidores.	1		
1.3	Repasse de conhecimento da solução de *Endpoint* com EDR para servidores.	1		
2.1	Solução de Gestão de Vulnerabilidades Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	1		
2.2	Implementação da solução de Gestão de Vulnerabilidades.	1		
2.3	Repasse de conhecimento da solução de Gestão de Vulnerabilidades.	1		
3.1	Solução de *Breach and Attack Simulation* – BAS Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	1		
3.2	Implementação da solução de *Breach and Attack Simulation* – BAS.	1		
3.3	Repasse de conhecimento da solução de *Breach and Attack Simulation* – BAS.	1		
4.1	Solução de Conformidade Equipamentos de Terceiro – NAC. Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	2200		
4.2	Implementação da solução de Conformidade Equipamentos de Terceiro – NAC.	1		
4.3	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC.	1		
5.1	Solução de Inteligência Cibernética – OSINT Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	1		
5.2	Implementação da solução de Inteligência Cibernética – OSINT.	1		
5.3	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT.	1		

6.1	Solução de Cofre de Senha e Gestão de Altas Credenciais – PAM. Obs: Informar a solução, a versão (ex.: *basic, standard, premium* etc.) e o fabricante da solução. A solução deve vir com o suporte técnico do fabricante incluso.	1		
6.2	Implementação da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1		
6.3	Repasse de conhecimento da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1		

Observações:

- Estão inclusos nos preços todos os custos e despesas que, direta ou indiretamente, que decorram das obrigações a serem, tais como e sem se limitar a: telefone, transporte, passagens e diárias, hospedagem, deslocamento, alimentação, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, softwares, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.
- Dados Bancários:
  - Nome do Favorecido – Razão Social
  - CNPJ –
  - Número do Banco -
  - Nome do Banco -
  - Número da Agência Bancária –
  - Número da Conta Corrente –
  - Modalidade de Conta – CONTA CORRENTE ou POUPANÇA
  - Chave Pix –
- O prazo de validade desta proposta é de 60 (sessenta) dias corridos.
- Declaro estar de acordo com a forma de faturamento estabelecido no item 6 - Modelo de Execução do Contrato, subitem Forma de Pagamento, constante na Especificação Técnica referente a contratação de soluções de segurança cibernética.

Brasília-DF, ___ de _____ de 2025.

_____

Carimbo, nome e assinatura do Diretor ou representante legal da empresa

Cédula de Identidade (número e órgão expedidor)

CPF/MF (número) e carimbo

ANEXO II
Requisitos obrigatórios e desejáveis da(s) solução(ões) ofertada(s).

ITEM 1 – SOLUÇÃO DE ENDPOINT COM EDR PARA SERVIDORES			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	A solução deverá ser disponibilizada exclusivamente em ambiente de nuvem, operando sob o modelo SaaS (*Software as a Service*), incluindo integralmente seu sistema de gerenciamento.	Obrigatório	
1.2	Não serão aceitas soluções que se baseiem em softwares genéricos, funcionalidades em fase de desenvolvimento beta ou tecnologias de código aberto (*open source*).	Obrigatório	
1.3	O fabricante da solução deve estar integrado ao programa Microsoft *Active Protections Program* (MAPP), destinado a fornecedores de software de segurança.	Obrigatório	
1.4	Todos os componentes da solução, incluindo o sistema de gerenciamento, devem ser fornecidos pelo mesmo fabricante, não sendo permitida a combinação de itens de fabricantes distintos, em conformidade com as diretrizes estabelecidas neste documento.	Obrigatório	
1.5	O fabricante deve utilizar a telemetria coletada para realizar atividades proativas de investigação e detecção de ameaças (*threat hunting*), fornecendo à contratante as seguintes informações:	----------	----------
1.5.1	Resultados de análises de causa raiz dos incidentes identificados;	Obrigatório	
1.5.2	Classificação das ameaças detectadas e avaliação de seus possíveis impactos;	Obrigatório	
1.5.3	Sugestões de planos de resposta e recomendações de ações a serem adotadas.	Obrigatório	
1.6	A solução de XDR deve ser atualizada continuamente e integrar feeds de inteligência de ameaças para identificar e responder a novas ameaças de forma rápida e eficaz.	Obrigatório	
1.7	A solução deve contemplar 500 licenças de XDR destinadas à proteção de servidores com sistemas operacionais Linux e Windows.	Obrigatório	
1.8	A solução deverá ser capaz de realizar integrações por meio de API REST, exposta como serviço Web, utilizando o protocolo HTTPS com mecanismos de autenticação seguros (como *tokens*, certificados ou OAuth), permitindo a automação e orquestração de funcionalidades da plataforma. Entre as atividades que devem ser suportadas via API, destacam-se:	----------	----------
1.8.1	Instalação, atualização e remoção de agentes;	Desejável	
1.8.2	Consulta e extração de alertas e incidentes;	Obrigatório	
1.8.3	Aplicação e alteração de políticas de proteção e resposta;	Obrigatório	
1.8.4	Isolamento de dispositivos suspeitos ou comprometidos;	Obrigatório	
1.8.5	Envio e consulta de indicadores de ameaça (IoCs);	Obrigatório	
1.8.6	Integração com sistemas de SIEM, SOAR, ITSM e plataformas de gerenciamento de ativos;	Desejável	
1.8.7	Geração de relatórios e dashboards personalizados.	Desejável	
1.9	Todas as funcionalidades da solução de XDR descritas neste documento devem ser executadas com agente único instalado nos *endpoints*.	Obrigatório	
2	GERÊNCIA DA SOLUÇÃO	----------	----------

2.1	A gerência da solução deve ser centralizada e única para todas as funcionalidades descritas neste documento.	Obrigatório	
2.2	A solução deve possuir interface gráfica (GUI) em formato web seguro (HTTPS), com navegação intuitiva e filtros avançados.	Obrigatório	
2.3	A interface de gerência deve ser capaz de identificar *endpoints* com agentes desatualizados, ativos ou removidos nos últimos 30 dias.	Obrigatório	
2.4	A solução deverá ser capaz de identificar agentes com falhas de instalação ou operação, que estejam funcionando sem a proteção integral prevista, permitindo a detecção proativa de inconsistências no estado de segurança dos *endpoints*.	Desejável	
2.5	A solução deve permitir a visualização de eventos contextualizados e históricos, viabilizando a investigação completa de incidentes, desde a detecção inicial até a identificação das causas raízes, com suporte a correlação de dados e reconstrução da cadeia de ataque.	Obrigatório	
2.6	Deve exibir o ciclo completo de execução de processos suspeitos nos *endpoints* monitorados, com acesso à telemetria relevante (como criação de arquivos, conexões de rede, alterações de registro, entre outros), e filtros avançados de busca baseados na matriz MITRE ATT&CK.	Obrigatório	
2.7	As atividades consideradas suspeitas devem ser apresentadas em formato de linha do tempo interativa, permitindo a análise sequencial dos eventos e facilitando a compreensão do comportamento malicioso.	Obrigatório	
2.8	A interface de gerenciamento deve permitir a visualização detalhada dos *endpoints* monitorados, incluindo, no mínimo: nome do dispositivo, sistema operacional (nome e versão), usuário ativo, endereço IP, status de proteção, versão do agente e data da última comunicação com o agente.	Obrigatório	
2.9	A solução deverá permitir a criação e gerenciamento de contas de usuários de forma local, bem como oferecer suporte à autenticação e autorização de usuários por meio dos protocolos SAML 2.0, *Active Directory* (AD) e Azure *Active Directory* (Azure AD).	Obrigatório	
2.10	A solução deverá permitir autenticação de usuários locais com Múltiplo Fator de Autenticação (MFA) próprio.	Obrigatório	
2.11	A solução deverá permitir a segregação hierárquica de contas de usuários por meio de controle de acesso baseado em funções (RBAC – *Role-Based Access Control*), com atribuição granular de permissões por funcionalidade, módulo ou escopo de atuação. Não deverá haver restrições quanto à quantidade de acessos simultâneos por usuários autenticados, garantindo escalabilidade e flexibilidade na gestão de perfis.	Obrigatório	
2.12	A solução deve permitir o acesso ao histórico completo de dados e telemetria diretamente por meio da interface de gerenciamento, independentemente de os eventos terem gerado alertas ou não. Esse acesso deve incluir, no mínimo:	----------	----------
2.12.1	Arquivos executáveis;	Obrigatório	
2.12.2	Ataques de *thread injection*;	Obrigatório	
2.12.3	Execuções de processos;	Obrigatório	
2.12.4	Atividades de *script*;	Obrigatório	
2.12.5	Arquivo baixado e o processo responsável;	Obrigatório	
2.12.6	Comandos executados;	Obrigatório	
2.12.7	Solicitações DNS;	Obrigatório	
2.12.8	Conexões de rede;	Obrigatório	
2.12.9	Escrita em arquivos;	Obrigatório	
2.12.10	Execução de processos;	Obrigatório	
2.12.11	Detecções;	Obrigatório	

2.12.12	Atividades de *logon*;	Obrigatório	
2.12.13	Detecções relacionadas ao usuário;	Desejável	
2.12.14	Processos executados por usuários.	Desejável	
2.13	A solução deverá disponibilizar funcionalidade de consulta customizável dos alertas e incidentes criados pelo módulo XDR, permitindo, no mínimo, a filtragem e visualização com base nos seguintes parâmetros:	----------	----------
2.13.1	Período (data de início e fim);	Obrigatório	
2.13.2	Nome do processo;	Obrigatório	
2.13.3	Nome da máquina;	Obrigatório	
2.13.4	Endereço IP;	Obrigatório	
2.13.5	Tipo de ataque ou detecção;	Obrigatório	
2.13.6	Ação tomada (bloqueio, quarentena);	Obrigatório	
2.13.7	Usuário associado.	Obrigatório	
2.14	As consultas deverão oferecer opções de apresentação dos resultados em formato gráfico e tabular, com suporte à utilização de operadores lógicos, termos ou frases, e filtros por expressões regulares. A solução também deverá permitir consultas específicas a indicadores de comprometimento (IoCs) e a *endpoints* monitorados.	Obrigatório	
2.15	A solução deverá permitir a exportação dos resultados das consultas realizadas, incluindo dados de telemetria, lista de agentes, registros de detecções e informações sobre vulnerabilidades, em formato CSV, de forma estruturada e compatível com ferramentas de análise externas.	Obrigatório	
3	ANTIMALWARE E XDR	----------	----------
3.1	Deverá possuir mecanismos avançados de prevenção contra *malwares, spywares* e outras ameaças, com proteção em tempo real.	Obrigatório	
3.2	A detecção de ameaças deverá ocorrer exclusivamente por meio de técnicas comportamentais baseadas em aprendizado de máquina (*Machine Learning*), sem uso de assinaturas.	Obrigatório	
3.3	Não serão aceitas soluções que utilizem módulos de assinatura, ainda que desabilitados ou parametrizados.	Obrigatório	
3.4	O agente instalado nos *endpoints* não deverá depender de atualizações recorrentes de vacinas ou assinaturas.	Obrigatório	
3.5	A solução deverá detectar e bloquear por meio de análise comportamental:	----------	----------
3.5.1	Vírus, *trojans, worms, spyware, adwares, malwares fileless* e *backdoors*;	Obrigatório	
3.5.2	Artefatos maliciosos que operem exclusivamente em memória volátil;	Obrigatório	
3.5.3	Artefatos que alterem permissões com privilégios elevados;	Obrigatório	
3.5.4	Ameaças que utilizem técnicas de "*Side Load* DLL";	Obrigatório	
3.5.5	Ataques ROP (*Return-Oriented Programming*);	Obrigatório	
3.5.6	Ataques SEHOP (*Structured Exception Handler Overwrite Protection*);	Obrigatório	
3.5.7	Ameaças nas fases pré-infecção e pós-infecção;	Obrigatório	
3.5.8	Ataques de movimentação lateral entre *endpoints*;	Obrigatório	
3.5.9	Exploração de vulnerabilidades em aplicações, serviços e sistemas operacionais;	Obrigatório	
3.5.10	*Exploits* de acesso remoto, escalonamento de privilégios e execução em memória;	Obrigatório	
3.5.11	Shell reverso e *webshell*;	Obrigatório	
3.5.12	Ameaças avançadas e vulnerabilidades *zero-day*, mesmo sem conexão com a internet ou console;	Desejável	
3.5.13	Atividades suspeitas de *ransomware*, incluindo criptografia de arquivos;	Obrigatório	

3.5.14	Infecções por navegação em sites maliciosos, "*drive-by downloads*", *spear phishing*, documentos maliciosos (PDF, *Office*), e vetores como Java e ActiveX.	Obrigatório	
3.6	A solução deverá permitir a criação de políticas de segurança personalizadas, incluindo a configuração de políticas em modo de detecção apenas, sem execução de ações corretivas por parte do agente, visando cenários de monitoramento, teste ou validação.	Desejável	
3.7	Deverá permitir criação de políticas de segurança distintas por grupo, categoria ou subcategoria.	Obrigatório	
3.8	Deverá permitir o isolamento manual ou automático de *endpoints* contaminados, impedindo seu acesso à rede, mas mantendo o acesso ao *endpoint* via console de gerenciamento.	Obrigatório	
3.9	Deverá bloquear arquivos contaminados, impedindo qualquer ação do usuário ou do sistema operacional, com opção de envio à quarentena.	Obrigatório	
3.10	Deverá permitir verificação manual e em tempo real de ameaças.	Obrigatório	
3.11	Deverá permitir configuração de ações automáticas diante de ameaças: alerta e exclusão.	Obrigatório	
3.12	Deverá realizar remoção automática de ameaças, incluindo limpeza de registros e pontos de carregamento.	Obrigatório	
3.13	Deverá possuir inspeção e proteção de memória, inclusive contra alterações em "*live memory*".	Obrigatório	
3.14	Deverá possuir prevenção de exploração baseada em kernel.	Obrigatório	
3.15	Deverá possuir sistema automatizado de pontuação ou qualificação de incidentes com base em aprendizado de máquina.	Obrigatório	
3.16	A solução deve consumir *feeds* externos de inteligência com IoCs (*hashes* de arquivos, IPs e domínios), permitir a inserção manual desses indicadores, e possibilitar a configuração do nível de severidade e das ações de bloqueio conforme necessário.	Desejável	
3.17	A solução deve permitir a criação de exceções (exclusões) para Indicadores de Comprometimento (IoCs) e Indicadores de Ataque (IOAs) nas políticas de segurança, com controle de escopo para aplicação das regras.	Obrigatório	
3.18	A solução XDR deve oferecer uma funcionalidade de console de resposta que permita a conexão remota com *endpoints* para fins de investigação e remediação. Essa funcionalidade deve incluir:	----------	----------
3.18.1	Conexão segura e autenticada com o *endpoint* via console integrado à plataforma;	Obrigatório	
3.18.2	Execução de comandos em tempo real diretamente no dispositivo;	Obrigatório	
3.18.3	Extração de evidências (arquivos, *logs*, artefatos de memória etc.) para análise forense;	Obrigatório	
3.18.4	Execução de scripts e comandos customizados definidos pelo analista;	Obrigatório	
3.18.5	*Upload* e execução de arquivos;	Obrigatório	
3.18.6	Controle de escopo e permissões para acesso à funcionalidade, conforme perfil de usuário.	Obrigatório	
4	INTELIGÊNCIA E SANDBOX	----------	----------
4.1	A solução deverá disponibilizar, por meio da console de gerenciamento, informações de inteligência atualizadas sobre os principais grupos de Ameaças Persistentes Avançadas (APT) em atividade, contendo, no mínimo:	----------	----------
4.1.1	Técnicas, Táticas e Procedimentos (TTPs) empregados por cada grupo;	Obrigatório	
4.1.2	Mapeamento das TTPs na matriz MITRE ATT&CK;	Desejável	
4.1.3	Vulnerabilidades exploradas associadas às campanhas identificadas.	Obrigatório	
4.2	A solução deverá disponibilizar, por meio da console de gerenciamento, mecanismo de busca global de indicadores de	----------	----------

	comprometimento (IoCs), permitindo consultas com base, no mínimo, nos seguintes parâmetros:		
4.2.1	*Hashes* criptográficos: MD5, SHA-1 e SHA-256;	Obrigatório	
4.2.2	Nome de arquivo;	Obrigatório	
4.2.3	URLs associadas;	Obrigatório	
4.2.4	Endereços IP.	Obrigatório	
4.3	A solução deverá possuir *dashboard* integrado, contendo informações sobre a telemetria coletada e/ou artefatos coletados e analisados de forma proativa pelo serviço gerenciado do fabricante.	Obrigatório	
4.4	A solução deverá possuir funcionalidade de *sandbox*, permitindo a submissão de até 100 artefatos suspeitos por mês sem custo adicional, para análise em ambiente isolado e seguro.	Obrigatório	
4.5	A *sandbox* deverá suportar a execução de artefatos em múltiplas plataformas, incluindo Windows, Linux e macOS.	Obrigatório	
4.6	A funcionalidade *sandbox* deverá permitir a detonação dos seguintes tipos de artefatos:	----------	----------
4.6.1	Arquivos comuns (executáveis, documentos, scripts, etc.);	Obrigatório	
4.6.2	Arquivos comprimidos;	Obrigatório	
4.6.3	Arquivos comprimidos protegidos por senha;	Desejável	
4.6.4	URLs (endereços web).	Obrigatório	
4.7	A *sandbox* deverá permitir a configuração personalizada da data e hora do ambiente de execução, visando simular cenários específicos.	Desejável	
4.8	A solução deverá permitir a interação manual do usuário com o artefato durante a análise, simulando ações reais em tempo de execução.	Obrigatório	
4.9	A *sandbox* deverá gerar relatórios detalhados de análise estática e dinâmica dos artefatos submetidos.	Obrigatório	
4.10	A *sandbox* deverá permitir a exportação dos relatórios de análise em formato CSV.	Obrigatório	
4.11	A *sandbox* deverá possibilitar a exportação dos Indicadores de Comprometimento (IoCs) em formatos estruturados como JSON e STIX 2.1.	Obrigatório	
4.12	A *sandbox* deverá permitir a exportação do tráfego de rede gerado durante a análise em formato PCAP.	Obrigatório	
5	SIEM E SOAR	----------	----------
5.1	A solução deverá possuir funcionalidades de SIEM diretamente na console de gerenciamento, sem necessidade de licenciamento adicional para ingestão, análise e correlação dos dados de telemetria e detecção gerados para o número de agentes contratados, com as seguintes características:	----------	----------
5.1.1	Disponibilizar regras nativas que correlacionem automaticamente os dados de telemetria dos *endpoints* com informações de inteligência de ameaças proprietária (ex: reputação de arquivos, IPs, domínios, TTPs baseados em MITRE ATT&CK);	Desejável	
5.1.2	Permitir a criação de regras personalizadas utilizando linguagem de consulta avançada, com filtros por processo, usuário, rede, comportamento e atributos de detecção;	Desejável	
5.1.3	Suportar ingestão e correlação de dados provenientes de outras soluções de segurança e infraestrutura (ex: firewalls, proxies, AD, EDRs de terceiros), por meio de APIs ou conectores.	Desejável	
5.2	A solução deverá incluir funcionalidades de orquestração e automação de resposta (SOAR) integradas à console, com suporte a criação de fluxos automatizados e interoperabilidade com outras ferramentas, com as seguintes características:	----------	----------

5.2.1	Disponibilizar ambiente visual para construção de *playbooks* automatizados, com lógica condicional, ações encadeadas e suporte a variáveis, sem necessidade de codificação avançada;	Desejável	
5.2.2	Oferecer *templates* prontos para automação de resposta a incidentes (ex: isolamento de *host*, coleta de evidências, bloqueio de IoCs), com possibilidade de edição e adaptação conforme o contexto operacional;	Desejável	
5.2.3	Permitir interação com ferramentas externas de segurança, colaboração e infraestrutura (ex: SIEMs, ITSM, *firewalls*, plataformas de colaboração como Microsoft Teams), por meio de APIs e conectores nativos.	Desejável	
6	AGENTE DA SOLUÇÃO	----------	----------
6.1	O agente da solução XDR deve poder ser instalado em computadores físicos e virtuais, oferecendo suporte, no mínimo, aos seguintes sistemas operacionais:	----------	----------
6.1.1	Windows Server 2012/2012 R2/2016/2019/2022/2025;	Obrigatório	
6.1.2	Windows Server Core 2016/2019/2022/2025;	Obrigatório	
6.1.3	RHEL 7/8/9;	Obrigatório	
6.1.4	Oracle Linux 7/8/9;	Obrigatório	
6.1.5	Ubuntu 24.04;	Obrigatório	
6.1.6	SUSE Enterprise Linux 15;	Obrigatório	
6.1.7	Debian 12.	Obrigatório	
6.2	A solução deve empregar um agente único para a execução de todas as funcionalidades descritas neste documento, evitando a necessidade de múltiplas instalações ou componentes adicionais.	Obrigatório	
6.3	Para novas versões dos sistemas operacionais mencionados anteriormente, a empresa deverá disponibilizar um agente compatível no prazo máximo de seis meses, contado a partir da data de publicação oficial pelo fabricante do sistema operacional.	Obrigatório	
6.4	O agente deve enviar, de forma automatizada e em tempo real, todos os eventos relevantes para atividades de *threat hunting* ao gerenciador central, independentemente da geração de alertas.	Obrigatório	
6.5	Deverá permitir a instalação remota e silenciosa do agente, sem intervenção do usuário, utilizando recursos nativos da solução, scripts de login, diretivas de grupo (*Group Policy* – GPO) ou o Microsoft *Endpoint Configuration Manager* (MECM).	Obrigatório	
6.6	A instalação, aplicação de patches e atualizações do agente devem ocorrer de forma totalmente autônoma e silenciosa, sem necessidade de interação do usuário ou reinicialização do sistema, garantindo a integridade e a continuidade operacional do *endpoint*.	Obrigatório	
6.7	Toda a comunicação entre os agentes e o gerenciador da solução, para envio de incidentes e telemetria, coleta de atualizações e aplicação de configurações, deve ocorrer diretamente pela Internet, sem intermediários, utilizando canal criptografado (HTTPS).	Obrigatório	
6.8	O agente deve possuir mecanismos robustos contra:	----------	----------
6.8.1	Desinstalação não autorizada;	Obrigatório	
6.8.2	Alterações indevidas nos serviços vinculados;	Obrigatório	
6.8.3	Modificações nos processos e registros relacionados ao agente.	Obrigatório	
6.9	A solução deve incluir uma sistemática de atualização contínua que preserve a eficácia do agente frente a novas ameaças, incluindo vulnerabilidades *zero-day*.	Obrigatório	
6.10	Durante o processo de transição tecnológica, o agente deve permitir coexistência com soluções XDR/EDR previamente instaladas, sem causar conflitos ou comprometimento dos ativos.	Obrigatório	
7	CONTROLE DE DISPOSITIVOS	----------	----------

7.1	A solução deve permitir o controle granular de dispositivos USB conectados aos *endpoints* com sistema operacional Windows que possuam o agente instalado, abrangendo, no mínimo, as seguintes categorias:	----------	----------
7.1.1	Dispositivos de armazenamento em massa;	Obrigatório	
7.1.2	Dispositivos Mobile (MTP/PTP);	Obrigatório	
7.1.3	Dispositivos de comunicação sem fio;	Obrigatório	
7.1.4	Impressoras.	Obrigatório	
7.2	Deverá possuir as seguintes opções de controle para dispositivos USB de armazenamento em massa: acesso total, apenas leitura, leitura e escrita e bloqueio total.	Obrigatório	
7.3	Deverá possuir as seguintes opções de controle para dispositivos móveis, dispositivos de comunicação sem fio e impressoras conectados via USB: acesso total e bloqueio total.	Obrigatório	
7.4	As políticas de controle de dispositivos USB poderão ser configuradas nos modos bloqueio ou auditoria (apenas notificação).	Desejável	
7.5	As políticas de controle de dispositivos USB deverão ser aplicáveis a computadores e/ou usuários.	Obrigatório	
7.6	A solução deverá permitir a personalização das mensagens de notificação exibidas aos usuários dos *endpoints* afetados quando houver bloqueio de dispositivos USB.	Desejável	
7.7	A solução deve permitir o cadastro de uma lista de exceções de dispositivos USB para cada categoria protegida, com opção de controle individual para cada dispositivo incluído.	Obrigatório	
7.8	A solução deve permitir o cadastro de exceções de dispositivos USB com caráter temporário, de modo que a exceção seja removida automaticamente após o período definido.	Desejável	
7.9	A console de gerenciamento da solução deve permitir a inclusão de dispositivos bloqueados na lista de exceções de forma automatizada e/ou disponibilizar, na própria console, as informações necessárias para o cadastro manual. Não serão aceitos mecanismos de identificação de dispositivos USB que exijam o uso de software adicional.	Obrigatório	
7.10	A console de gerenciamento da solução deve disponibilizar um painel de visualização com histórico pesquisável de todos os dispositivos USB conectados (bloqueados ou não) aos *endpoints* que possuam o agente instalado, permitindo a identificação, classificação e auditoria dos eventos de conexão.	Obrigatório	
7.11	A console de gerenciamento deve permitir a visualização do histórico de arquivos gravados em dispositivos USB.	Desejável	
8	FIREWALL DE HOST	----------	----------
8.1	A solução deverá conter módulo de *firewall* de *host*, com capacidade de definição de políticas para sistemas operacionais Windows e Linux que possuam o agente instalado.	Obrigatório	
8.2	As políticas de firewall poderão ser configuradas nos modos aplicação (*enforce*) ou monitoramento.	Obrigatório	
8.3	As regras de firewall deverão permitir a configuração dos seguintes parâmetros:	----------	----------
8.3.1	Comportamento padrão para o tráfego de entrada e saída (permitido ou bloqueado);	Obrigatório	
8.3.2	Especificação do host por FQDN ou endereço IP;	Obrigatório	
8.3.3	Protocolos IPv4 e IPv6;	Obrigatório	
8.3.4	Protocolos TCP, UDP, ICMPv4 e ICMPv6;	Obrigatório	
8.3.5	Ação: permitir ou bloquear;	Obrigatório	
8.3.6	Reconhecimento de localização;	Obrigatório	
8.3.7	Direção: entrada, saída ou ambos.	Obrigatório	

8.4	A solução deverá permitir a criação de localizações de rede customizadas a serem utilizadas nas regras de *firewall* (reconhecimento de localização) com, no mínimo, os seguintes parâmetros:	----------	----------
8.4.1	Teste de Ping para FQDN e endereços IP;	Obrigatório	
8.4.2	Tipo da conexão (com ou sem fio);	Obrigatório	
8.4.3	Endereço do gateway da conexão;	Obrigatório	
8.4.4	Endereço IP (absoluto ou range CIDR) do host;	Obrigatório	
8.4.5	Endereço IP do servidor DHCP.	Desejável	
8.5	A solução deve permitir a visualização dos logs de *firewall* dos hosts com agentes instalados localmente, tanto em cada host quanto na console centralizada de gerenciamento SaaS.	Obrigatório	
9	ANÁLISE DE VULNERABILILDADES	----------	----------
9.1	A solução deve incluir um módulo nativo, fornecido pelo mesmo fabricante da plataforma XDR, responsável por realizar varreduras automatizadas nos servidores que possuem o agente instalado. Este módulo deve ser capaz de identificar *softwares* instalados, incluindo o sistema operacional e seus pacotes associados, e correlacioná-los com vulnerabilidades conhecidas, apresentando na console de gerenciamento centralizada informações detalhadas e relevantes para a atuação do administrador, incluindo:	----------	----------
9.1.1	Nome do aplicativo vulnerável identificado no sistema;	Obrigatório	
9.1.2	Versão exata do aplicativo correlacionada à vulnerabilidade detectada;	Obrigatório	
9.1.3	Identificador CVE (*Common Vulnerabilities and Exposures*) associado à vulnerabilidade;	Obrigatório	
9.1.4	Pontuação CVSS (*Common Vulnerability Scoring System*) correspondente, incluindo vetores de ataque e métricas de severidade;	Obrigatório	
9.1.5	Descrição técnica da vulnerabilidade, contendo impacto potencial, vetores de exploração e requisitos de execução;	Desejável	
9.1.6	Quantidade de hosts afetados, discriminando servidores impactados por cada vulnerabilidade;	Obrigatório	
9.1.7	Solução ou recomendação de remediação fornecida pelo fabricante do software vulnerável, incluindo *links* para patches, atualizações ou instruções de mitigação;	Obrigatório	
9.1.8	Categoria ou tipo da vulnerabilidade, como execução de código remoto, escalonamento de privilégios, divulgação de informação etc.;	Obrigatório	
9.1.9	Capacidade de geração de relatórios e exportação de dados, permitindo análise de tendência, rastreabilidade de risco e suporte à auditoria.	Obrigatório	
9.2	A solução deverá incorporar um mecanismo robusto de priorização de vulnerabilidades, capaz de auxiliar o administrador na definição de ordem de mitigação com base em critérios de risco de exploração. Essa priorização deve considerar múltiplos fatores de avaliação, incluindo, mas não se limitando a:	----------	----------
9.2.1	Complexidade de exploração da vulnerabilidade, incluindo a necessidade de interação do usuário e privilégios exigidos;	Obrigatório	
9.2.2	Disponibilidade e maturidade de *exploits* públicos ou ferramentas automatizadas de exploração;	Obrigatório	
9.2.3	Dados de inteligência cibernética atualizados, abrangendo tendências de ataques, atores de ameaças relevantes e campanhas ativas;	Obrigatório	
9.2.4	Impacto potencial na confidencialidade, integridade e disponibilidade dos ativos afetados;	Obrigatório	
9.2.5	Exposição externa do ativo vulnerável, como serviços voltados à internet ou conexões com redes não confiáveis.	Obrigatório	

9.3	O mecanismo de priorização de vulnerabilidades deve ser capaz de integrar-se com feeds de inteligência de ameaças (*Threat Intelligence*) e frameworks de avaliação como CVSS, EPSS ou similares, possibilitando a geração de score de risco dinâmico e contextualizado para apoiar decisões de resposta rápida e eficaz.	Obrigatório	
9.4	A solução deverá oferecer uma interface de programação de aplicações (API) robusta e segura, que permita a consulta, extração e exportação integral dos dados gerados pelo módulo de análise de vulnerabilidades. Essa API deve ser projetada para integração eficiente com ferramentas externas de gestão, SIEM, ITSM, plataformas de orquestração e dashboards analíticos. Os principais requisitos funcionais incluem:	----------	----------
9.4.1	Acesso completo aos dados estruturados do inventário de vulnerabilidades, permitindo a obtenção de informações como: nome e versão dos aplicativos vulneráveis, identificadores CVE, pontuações CVSS, descrição técnica, recomendações de remediação, e número de hosts impactados;	Obrigatório	
9.4.2	Filtros e parâmetros de consulta avançados, como por gravidade (ex: CVSS ≥ 7), tipo de vulnerabilidade, categoria de ativo, faixa de IP, entre outros;	Desejável	
9.4.3	Exportação em formatos interoperáveis, como JSON e CSV, para facilitar integração e análise personalizada;	Obrigatório	
9.4.4	Autenticação segura e controle de acesso, por meio de protocolos como OAuth 2.0, chaves de API ou integração com sistemas de identidade corporativa (ex: LDAP, SAML);	Obrigatório	
9.4.5	Limitação e paginação de requisições, com controle de performance e proteção contra abusos;	Obrigatório	
9.4.6	Documentação técnica completa e interativa (ex: Swagger/OpenAPI), com exemplos de uso, respostas esperadas e códigos de erro;	Obrigatório	
9.4.7	Suporte à automação de tarefas, como geração periódica de relatórios de vulnerabilidade, criação de *tickets* em sistemas de correção ou envio de alertas para times responsáveis.	Desejável	
9.5	A solução deve incluir um mecanismo de supressão de vulnerabilidades, permitindo ocultar determinadas informações da console de gerenciamento e de relatórios — tanto sob demanda quanto agendados — com base em critérios definidos pelo administrador, como:	----------	----------
9.5.1	Identificador CVE específico;	Desejável	
9.5.2	Nome do *endpoint*;	Desejável	
9.5.3	Grupos de *endpoints*;	Desejável	
9.5.4	Nome do produto;	Desejável	
9.5.5	Versão do produto.	Desejável	
9.6	O módulo de gerenciamento de vulnerabilidades deve possuir capacidade técnica comprovada para identificar vulnerabilidades de segurança em sistemas operacionais de arquitetura 64-bit, abrangendo, no mínimo:	----------	----------
9.6.1	Windows Server 2012/2012 R2/2016/2019/2022/2025;	Obrigatório	
9.6.2	Windows Server Core 2016/2019/2022/2025;	Obrigatório	
9.6.3	RHEL 7/8/9;	Obrigatório	
9.6.4	Oracle Linux 7/8/9;	Obrigatório	
9.6.5	Ubuntu 24.04;	Obrigatório	
9.6.6	SUSE Enterprise Linux 15;	Desejável	
9.6.7	Debian 12.	Obrigatório	

ITEM 2 – SOLUÇÃO DE GESTÃO DE VULNERABILIDADES			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	A solução deve ser licenciada para realizar varreduras (*scans*) de vulnerabilidades avaliação de configuração e conformidade (*baseline* e *compliance*) e indícios e padrões de códigos maliciosos conhecidos (*malware*).	Desejável	
1.2	A plataforma de gerenciamento deverá ser instalada nas dependências do cliente e deverá ser compatível para instalação nos seguintes sistemas operacionais:	----------	----------
1.2.1	Oracle Linux 7/8/9;	Obrigatório	
1.2.2	Windows Server 2019/2022/2025.	Obrigatório	
1.3	A solução deve possuir recurso de varredura ativa onde o scanner comunica-se com os alvos (ativos) através da rede.	Obrigatório	
1.4	A solução deve ser licenciada para no mínimo 10 scanners ativos.	Desejável	
1.5	A solução deve ser licenciada para o uso de no mínimo 10 sensores passivos de rede para realizar o monitoramento em tempo real.	Desejável	
1.6	A solução de gerenciamento deverá permitir *hardening* via controles SELinux para impedir explorações no servidor.	Desejável	
1.7	Deve ter a possibilidade de armazenar localmente a base de dados de vulnerabilidades.	Desejável	
1.8	Deve ser capaz de identificar no mínimo 55.000 CVE´S.	Desejável	
1.9	Deve permitir a autenticação com certificados SSL *smart cards* PIV (*Personal identity verification*) e *common access cards* (CAC).	Desejável	
1.10	A solução deve fornecer sem configuração adicional e em instalação padrão pelo menos 90 *dashboards* diferentes para análise das informações coletadas em varreduras.	Desejável	
1.11	Deve possibilitar por meio da console central de gerenciamento no mínimo 3 (três) métodos de escaneamento:	----------	----------
1.11.1	*Scan* ativo;	Obrigatório	
1.11.2	*Scan* com uso de agentes;	Obrigatório	
1.11.3	*Scan* passivo.	Desejável	
1.12	Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv2 score.	Obrigatório	
1.13	A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades.	Obrigatório	
1.14	O algoritmo de priorização deve analisar vulnerabilidades presentes na *National Vulnerability Database* (NVD).	Desejável	
1.15	A solução deve ser capaz de aplicar algoritmos de inteligência artificial (*Machine learning*) para analisar mais de 120 características relacionadas a vulnerabilidades.	Desejável	
1.16	Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial.	Desejável	

1.17	Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades incluindo feeds de inteligência de ameaças ao vivo.	Obrigatório	
1.18	O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:	----------	----------
1.18.1	CVSSv3 *Impact Score*;	Obrigatório	
1.18.2	Idade da Vulnerabilidade;	Obrigatório	
1.18.3	Número de produtos afetados pela vulnerabilidade;	Desejável	
1.18.4	Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;	Desejável	
1.18.5	Lista de todas as fontes (canais de mídia social *dark web* etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade.	Desejável	
1.19	A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação).	Desejável	
1.20	Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras.	Obrigatório	
1.21	A solução deve possuir sistema de alertas com ações definidas para cada alerta entre elas:	----------	----------
1.21.1	Criação de *ticket* no sistema de chamados interno da solução;	Desejável	
1.21.2	Envio de e-mail;	Obrigatório	
1.21.3	Envio de mensagem syslog;	Obrigatório	
1.21.4	Iniciar *scan* sob demanda com base em condições definidas;	Desejável	
1.21.5	Gerar relatório sob demanda filtrado nas condições do alerta.	Desejável	
1.22	A solução deve permitir a instalação de agentes em estações de trabalho e servidores para varredura diretamente no sistema operacional.	Desejável	
1.23	A solução deve ser licenciada para no mínimo 2000 agentes instalados em estações de trabalho e servidores para varredura diretamente no sistema operacional.	Desejável	
1.24	Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades.	Desejável	
1.25	Os agentes devem realizar conexões para o sistema centralizado de gerenciamento de agentes e scanners dentro do ambiente da instituição sem a necessidade de acessar a Internet.	Desejável	
1.26	A solução deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas como por exemplo em determinados dias do mês ou determinados horários do dia.	Desejável	
1.27	A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características: Sistema Operacional, Endereço IP, DNS, NetBIOS Host, NetBIOS Workgroup, MAC, SSH Fingerprint, Porta TCP e/ou UDP, Dias desde a descoberta do ativo, *Exploit* disponível, XREF, *Hosts* com Antivírus Desatualizado, *Host* com Browsers específicos (Opera Chrome, Safari, Firefox), *Hosts* com *browser* TOR instalado, *Hosts* com *software* VOIP instados e *Hosts* com clientes SQL instalados.	Desejável	
1.28	A solução deve agrupar as informações encontradas no ambiente para no mínimo:	----------	----------
1.28.1	Sumário de Ativos;	Obrigatório	
1.28.2	Sumário por CVE;	Obrigatório	
1.28.3	Sumário por Vulnerabilidade;	Obrigatório	
1.28.4	Sumário por protocolo;	Obrigatório	
1.28.5	Sumário por Boletins Microsoft;	Desejável	
1.28.6	Sumários por IP;	Obrigatório	
1.28.7	Sumário por nome DNS;	Desejável	
1.28.8	Lista de todos os sistemas operacionais encontrados;	Obrigatório	

1.28.9	Lista com todos os *softwares* encontrados;	Obrigatório	
1.28.10	Lista com todos os serviços;	Obrigatório	
1.28.11	Lista de *Web Clients*;	Obrigatório	
1.28.12	Lista de *Web Servers*.	Obrigatório	
2	RELATÓRIOS	----------	----------
2.1	Deve ser capaz de executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador.	Obrigatório	
2.2	A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML.	Obrigatório	
2.3	A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos.	Obrigatório	
2.4	A solução deve possuir relatórios pré-configurados com as seguintes informações:	----------	----------
2.4.1	*Hosts* verificados sem credenciais;	Obrigatório	
2.4.2	Top 100 vulnerabilidades mais críticas;	Desejável	
2.4.3	Top 10 *hosts* infectados por *malwares*;	Obrigatório	
2.4.4	Total de vulnerabilidades que podem ser exploradas pelo *Metasploit*;	Desejável	
2.4.5	Vulnerabilidades críticas e exploráveis;	Desejável	
2.4.6	Máquinas com vulnerabilidades que podem ser exploradas;	Desejável	
2.4.7	Informações sobre os hosts com maior número de vulnerabilidades contendo no mínimo as seguintes informações: IP, Nome, Netbios, DNS, Sistema Operacional e MAC *Address*;	Obrigatório	
2.4.8	Lista dos principais *hosts* e sistemas operacionais com *patches* de segurança ausentes;	Obrigatório	
2.4.9	Relatório com informações sobre vulnerabilidades críticas e exploráveis que foram detectadas na rede;	Desejável	
2.4.10	Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um *exploit* disponível e informações do ativo.	Desejável	
2.5	Deve permitir a customização de relatórios podendo incluir no mínimo as seguintes opções:	----------	----------
2.5.1	Marca d'agua customizada em cada página do relatório;	Desejável	
2.5.2	Customização de logo;	Desejável	
2.5.3	Header pré-definido.	Desejável	
3	VARREDURAS	----------	----------
3.1	A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e macOS, bem como *appliances* virtuais.	Desejável	
3.2	A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.	Desejável	
3.3	A solução deve ser configurável para permitir a otimização das configurações de varredura.	Obrigatório	
3.4	A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e *Active Directory*) e root para sistemas Linux.	Obrigatório	
4	AUDITORIA DE CONFIGURAÇÃO	----------	----------
4.1	A solução deve fornecer *dashboards* visuais, em formato de placar, contendo as verificações e controles de segurança verificados com indicação de sucesso ou falha, com base nos principais *frameworks* de segurança reconhecidos pela indústria, tais como:	----------	----------
4.1.1	SANS 20 *Critical Security Controls*;	Desejável	
4.1.2	ISO 27000;	Desejável	
4.1.3	NIST *Cybersecurity Framework*;	Desejável	
4.1.4	PCI *Data Security Standard*;	Desejável	
4.1.5	CIS *Benchmark* L1 e L2.	Desejável	

4.2	A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: Microsoft Defender for Endpoint, Crowdstrike Falcon *e Kaspersky*.	Desejável	
4.3	A solução deve fornecer auditorias de configuração com base *benchmarks* em CIS (*Center for Internet Security*) L1 e L2 para ambos os sistemas operacionais Microsoft Windows e Linux.	Desejável	
4.4	Deve suportar os seguintes *Frameworks* de segurança: ISO/IEC 27001/2, NIST *Cybersecurity Framework* (CSF), NIST 800-53, NIST 800-171, NERC CIP e GLBA.	Desejável	
5	VARREDURA DE APLICAÇÕES WEB	----------	----------
5.1	A solução deve realizar varreduras de vulnerabilidades em 10 FQDN em aplicações *Web* simultaneamente, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10.	Obrigatório	
5.2	A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações *Web* como parte dos ativos a serem inspecionados.	Obrigatório	
5.3	A solução deverá capaz de executar varreduras em sistemas *web* através de seus endereços IP ou FQDN (DNS).	Desejável	
5.4	Deverá avaliar no mínimo os padrões de segurança OWASP Top 10.	Desejável	
5.5	Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:	----------	----------
5.5.1	*Cookies, Headers*, Formulários e *Links*;	Obrigatório	
5.5.2	Nomes e valores de parâmetros da aplicação;	Desejável	
5.5.3	Elementos JSON e XML;	Obrigatório	
5.5.4	Elementos DOM.	Obrigatório	
5.6	Deverá também permitir somente a execução da função *crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação.	Obrigatório	
5.7	Deve ser capaz de utilizar scripts customizados de *crawl* com parâmetros definidos pelo usuário.	Obrigatório	
5.8	Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares.	Obrigatório	
5.9	Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões.	Desejável	
5.10	Deve ser capaz de instituir no mínimo os seguintes limites:	----------	----------
5.10.1	Número máximo de URLs para *crawl* e navegação;	Obrigatório	
5.10.2	Número máximo de diretórios para varreduras;	Obrigatório	
5.10.3	Número máximo de elementos DOM;	Desejável	
5.10.4	Tempo máximo para a varredura;	Obrigatório	
5.10.5	Número máximo de conexões HTTP ao servidor hospedando a aplicação *Web*;	Obrigatório	
5.10.6	Número máximo de requisições HTTP por segundo.	Obrigatório	
5.11	Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual.	Obrigatório	
5.12	Deve suportar o envio de notificações por e-mail e SMS.	Obrigatório	
5.13	A solução deve suportar o esquema de Autenticação Básica (Digest).	Obrigatório	
5.14	A solução deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades.	Obrigatório	
5.15	Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações.	Obrigatório	
5.16	Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências.	Obrigatório	

5.17	Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação.	Obrigatório	
5.18	A solução deve ser capaz de realizar varreduras nos seguintes componentes:	----------	----------
5.18.1	WordPress;	Obrigatório	
5.18.2	Blog *Designer Plugin for* Wordpress;	Obrigatório	
5.18.3	*Event Calendar Plugin for* Wordpress;	Obrigatório	
5.18.4	*Convert Plus Plugin for* Wordpress;	Obrigatório	
5.18.5	AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts;	Obrigatório	
5.18.6	Atlassian Confluence, Atlassian Crowd e Atlassian Jira;	Obrigatório	
5.18.7	Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHPThinkPHP, Webmin e YUI.	Obrigatório	

ITEM 3 – SOLUÇÃO DE BREACH AND ATTACK SIMULATION – BAS			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	A solução deve ser capaz de instrumentar e orquestrar simulações automatizadas de ataques em rede.	Desejável	
1.2	A solução deve apresentar interface gráfica (GUI) baseado na web que permite a manipulação da ferramenta.	Obrigatório	
1.3	A solução deve permitir a autenticação via Active Directory (AD).	Desejável	
1.4	Permitir o cadastro de áreas que representem a infraestrutura a ser analisada.	Desejável	
1.5	Permitir o cadastro de novos agentes de forma a acompanhar o crescimento/mudança da infraestrutura.	Obrigatório	
1.6	As simulações ou casos de teste devem ser totalmente seguros para produção, sem carga maliciosa ou execução de código que possam impactar o ambiente de produção.	Obrigatório	
1.7	As simulações devem ser feitas de forma que se possa:	----------	----------
1.7.1	Agendá-las para uma execução única no futuro;	Obrigatório	
1.7.2	Agendá-las para uma execução repetida no futuro;	Obrigatório	
1.7.3	Indicar o tipo de ataque a ser simulado;	Obrigatório	
1.7.4	Indicar a origem e destino dos ataques.	Obrigatório	
1.8	A solução deve detalhar os ataques disponíveis.	Obrigatório	
1.9	A solução deve permitir combinar múltiplos ataques para criar cenários próximos ao real.	Desejável	
1.10	A solução deve gerar gráficos e métricas das simulações executadas.	Desejável	
1.11	Os dados apresentados pelas simulações executadas devem poder ser filtrados por no mínimo:	----------	----------
1.11.1	Tempo do ataque;	Obrigatório	
1.11.2	Agentes;	Obrigatório	
1.11.3	Áreas.	Obrigatório	
1.12	A solução deve ser capaz de reportar individualmente o resultado dos ataques identificando as lacunas de segurança e indicando os ataques que:	----------	----------
1.12.1	Foram bloqueados;	Obrigatório	
1.12.2	Foram permitidos, mas detectados;	Obrigatório	
1.12.3	Foram permitidos, mas não-detectados.	Obrigatório	
1.13	A ferramenta deve ser capaz de integrar com no mínimo os seguintes componentes de segurança:	----------	----------
1.13.1	*Firewall*;	Desejável	
1.13.2	IDS;	Desejável	
1.13.3	DLP;	Desejável	
1.13.4	*Proxy*;	Desejável	
1.13.5	*Endpoints*;	Desejável	
1.13.6	EDR;	Desejável	
1.13.7	DNS Seguro;	Desejável	
1.13.8	SOAR;	Desejável	

1.13.9	SIEM.	Desejável	
1.14	A solução deve ser capaz de adicionar novas simulações de ataque de forma a estar atualizado com novas ameaças.	Desejável	
1.15	A solução deve ser capaz de ser instalada e configurada tanto na rede interna quanto na Internet.	Desejável	
1.16	Os agentes devem ser capazes de serem instalados e configurados tanto na rede interna quanto na Internet.	Obrigatório	
1.17	A ferramenta deve ser capaz de se comunicar com seus agentes quando estes se encontrarem em:	----------	----------
1.17.1	Utilizado NAT;	Desejável	
1.17.2	Através de um *proxy*.	Desejável	
1.18	A solução deve ser capaz de notificar a finalização do ataque via Syslog para integração com ferramentas já existentes.	Obrigatório	
1.19	A solução deve ser capaz de exportar os dados os via CSV.	Obrigatório	
1.20	Ataques em *endpoints* e servidores:	----------	----------
1.20.1	Comando e controle;	Obrigatório	
1.20.2	Consulta maliciosa de DNS;	Obrigatório	
1.20.3	Shell reverso;	Obrigatório	
1.20.4	Ataques LOTL (*Living-off-the-Land*);	Obrigatório	
1.20.5	Varredura e enumeração;	Obrigatório	
1.20.6	*Fingerprint*;	Obrigatório	
1.20.7	Ping Sweeps;	Obrigatório	
1.20.8	Descoberta de políticas;	Obrigatório	
1.20.9	Varredura de portas;	Obrigatório	
1.20.10	Varreduras de vulnerabilidades;	Obrigatório	
1.20.11	Transferência de arquivos maliciosos;	Obrigatório	
1.20.12	*Man-in-the-middle*;	Obrigatório	
1.20.13	Evasão de políticas;	Obrigatório	
1.20.14	Autenticação e autorização (*Dump* de credenciais);	Obrigatório	
1.20.15	Ataques de força bruta;	Obrigatório	
1.20.16	Exfiltração de dados;	Obrigatório	
1.20.17	Escalação de privilégio;	Obrigatório	
1.20.18	Movimento lateral;	Obrigatório	
1.20.19	Enumeração de domínio;	Obrigatório	
1.20.20	Enumeração de rede com SMB.	Obrigatório	
1.21	Ataques em aplicações web:	----------	----------
1.21.1	Injeção de comando;	Obrigatório	
1.21.2	CSRF;	Obrigatório	
1.21.3	SQL *Injection*;	Obrigatório	
1.21.4	XSS;	Obrigatório	
1.21.5	*Path Traversal*;	Obrigatório	
1.21.6	*File inclusion*;	Obrigatório	
1.21.7	XML *injections*.	Obrigatório	
1.22	Deve possuir testes para pelo menos as seguintes plataformas:	----------	----------
1.22.1	Android;	Desejável	
1.22.2	IOS;	Desejável	
1.22.3	Linux;	Obrigatório	
1.22.4	Mac;	Desejável	
1.22.5	Windows.	Obrigatório	
1.23	Deve testar e qualificar pelo menos os seguintes estágios de ataque:	----------	----------
1.23.1	Reconhecimento;	Obrigatório	
1.23.2	Entrega;	Obrigatório	
1.23.3	Exploração;	Obrigatório	
1.23.4	Execução;	Obrigatório	

1.23.5	Comando e Controle;	Obrigatório	
1.23.6	Ação no alvo.	Obrigatório	
1.24	Deve apresentar os resultados seguindo o padrão do Mitre ATT&CK.	Desejável	
1.25	Atualizações de controle automatizadas, integração com controles de segurança envio/inserção de (IOCs).	Obrigatório	
1.26	Feeds diários de ameaças:	----------	----------
1.26.1	Validar os controles contra a ameaças emergentes, campanhas ativas com uma atualização diária.	Obrigatório	
1.27	Validar os controles de segurança:	----------	----------
1.27.1	*Secure Email Gateway* (SEG);	Obrigatório	
1.27.2	*Secure Web Gateway* (SWG);	Obrigatório	
1.27.3	*Web App Firewalls* (WAF);	Obrigatório	
1.27.4	*Endpoint Security* (AV / EDR);	Obrigatório	
1.27.5	*Network Security* (IPS/IDS);	Obrigatório	
1.27.6	*Data Loss Prevention* (DLP);	Obrigatório	
1.27.7	*Cloud Security* (CWPP);	Obrigatório	
1.27.8	Kubernetes/Containers (K8S);	Obrigatório	
1.27.9	SIEM e SOAR.	Obrigatório	
1.28	Validar a exposição do ambiente quanto as ameaças:	----------	----------
1.28.1	APT *Groups*;	Obrigatório	
1.28.2	ATT&CK *Tactics* & *Techniques*;	Obrigatório	
1.28.3	*Ransomware*;	Obrigatório	
1.28.4	*Malware, Worms* e *Trojans*.	Obrigatório	
1.29	Orientação de mitigação e regras de detecção - Insights de remediação, fornecer orientação para ajustes de controles e aprimoramento de medidas contra ameaças.	Obrigatório	

ITEM 4 – SOLUÇÃO DE CONFORMIDADE DE EQUIPAMENTOS DE TERCEIROS – NAC			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	Não serão aceitos sistemas baseados em software de código aberto (*open source*) de uso genérico.	Obrigatório	
1.2	A solução ofertada não deve estar com término de comercialização ou término de suporte (EoL ou EoS) até o final do contrato.	Obrigatório	
1.3	Fornecer *appliances* virtuais, licenciamento e suporte necessário para a implementação e operação da solução para atender um parque de no mínimo 2.200 (dois mil e duzentos) dispositivos conectados à rede; a solução deverá ser compatível com:	----------	----------
1.3.1	VMware ESXi v8.x ou superior;	Obrigatório	
1.3.2	Microsoft Hyper-V 2025 ou superior;	Obrigatório	
1.3.3	KVM em Red Hat *Enterprise* Linux (RHEL) e/ou Oracle Linux 9;	Desejável	
1.3.4	Citrix XenServer;	Desejável	
1.3.5	*OpenStack*.	Desejável	
1.4	As licenças oferecidas devem contemplar as funcionalidades para todos os 2.200 dispositivos contemplados; não serão aceitas funcionalidades habilitadas para um número de dispositivos menor que o total.	Obrigatório	
1.5	A solução deve implementar autenticação, autorização e contabilização para até 2.200 dispositivos simultâneos, abrangendo 1500 usuários corporativos e 200 visitantes, e incluir mecanismos de gestão de convidados, terceiros e dispositivos BYOD por meio de um *captive* portal dedicado.	Obrigatório	
1.6	A solução deve suportar uma arquitetura totalmente centralizada de seus serviços, ou seja, sem a necessidade de implementar *appliances* fora do *Data Center* e suportando todas as funcionalidades desta especificação técnica.	Obrigatório	
1.7	A plataforma de NAC deve funcionar em modo de alta disponibilidade, nos modos ativo-ativo e ativo-passivo (*standby*).	Obrigatório	
1.8	O componente de aplicação de políticas deve funcionar em modo ativo-ativo. A gerência da solução deve funcionar no mínimo em modo ativo-passivo.	Obrigatório	
1.9	Em caso de falha de um dos componentes da solução, o outro deverá assumir automaticamente todas as operações e funcionalidades, sem interrupção dos serviços. Soluções que exijam intervenção manual para garantir alta disponibilidade não serão aceitas.	Obrigatório	
2	INTEGRAÇÃO COM O AMBIENTE EXISTENTE	----------	----------
2.1	A solução deverá integrar-se nativamente com as seguintes bases de usuários:	----------	----------
2.1.1	OpenLDAP;	Desejável	
2.1.2	Microsoft *Active Directory*;	Obrigatório	
2.1.3	RADIUS;	Obrigatório	
2.1.4	TACACS.	Obrigatório	

2.2	A solução deve oferecer suporte à identificação passiva de usuários por meio de métodos como MS-Eventing API ou o protocolo Microsoft *Remote Procedure Call* (MSRPC), sem a necessidade de instalação de agentes nos dispositivos finais.	Desejável	
2.3	A solução deve ser capaz de realizar a identificação passiva de usuários por meio da obtenção de informações de sistemas externos, utilizando protocolos ou especificações compatíveis, como Syslog e API REST.	Obrigatório	
2.4	A solução deve ser capaz de sincronizar automaticamente seu relógio interno com servidores de tempo confiáveis, utilizando o protocolo NTP (*Network Time Protocol*).	Obrigatório	
2.5	A solução deve possuir uma API RESTful com as seguintes características:	----------	----------
2.5.1	Permitir operações de consulta, criação, atualização e exclusão (GET, POST, PUT, DELETE) sobre objetos como *endpoints*, políticas, perfis de dispositivo, certificados e sessões;	Obrigatório	
2.5.2	Permitir a consulta e atualização de atributos de perfil, incluindo endereço MAC, tipo de dispositivo e status de conformidade, bem como a associação de dispositivos a grupos de identidade e a aplicação de políticas de acesso;	Obrigatório	
2.5.3	Suportar mecanismos de autenticação como OAuth 2.0, autenticação básica (*Basic Auth*) ou integração com diretórios corporativos (ex: *Active Directory*);	Obrigatório	
2.5.4	Possibilitar integração bidirecional com plataformas de gerenciamento de vulnerabilidades (ex: *Tenable, Qualys*) e sistemas ITSM *open source* ou proprietários, sem restringir a tecnologia utilizada;	Desejável	
2.5.5	Permitir a execução de ações automatizadas, tais como quarentena de dispositivos, reautenticação e alteração de perfil, com base em eventos provenientes de sistemas externos.	Obrigatório	
2.6	Todos os registros de log gerados pela solução devem estar em conformidade com o padrão Syslog e ser encaminhados, de forma simultânea, para no mínimo dois servidores distintos de armazenamento de *logs*.	Obrigatório	
2.7	A solução deve permitir configurar os níveis de gravação Syslog, definindo quais eventos serão registrados e em quais níveis de gravidade (informações, avisos, erros, críticos). Também deve possibilitar a personalização do formato dos logs, incluindo campos adicionais, dados de identificação de dispositivos ou outras informações específicas conforme os requisitos da organização.	Obrigatório	
2.8	A solução deve ser capaz de integrar-se, por meio dos protocolos RADIUS, IEEE 802.1X e SNMP, com plataformas de switches de mercado que ofereçam suporte a esses protocolos, incluindo, mas não se limitando a equipamentos de fabricantes como Cisco, Huawei, Dell, entre outros.	Obrigatório	
2.9	A solução deve permitir integração com plataformas de switches por meio de protocolos como SNMP, Telnet ou SSH, sem obrigatoriedade de utilização exclusiva de RADIUS ou 802.1X.	Desejável	
2.10	A solução deve ser capaz de integrar-se, por meio dos protocolos RADIUS, IEEE 802.1X e SNMP com plataformas wireless de mercado, incluindo Cisco, Aruba, Aerohive (Extreme), entre outras.	Obrigatório	
2.11	A solução deve permitir integração com plataformas wireless por meio de protocolos como SNMP, Telnet ou SSH, sem obrigatoriedade de utilização exclusiva de RADIUS ou 802.1X.	Desejável	
2.12	A solução deverá suportar o protocolo RADIUS, conforme os padrões definidos nas RFCs 2865, 2866 e 3576, incluindo:	----------	----------

2.12.1	Atributos padrão;	Obrigatório	
2.12.2	Atributos específicos de fornecedor (*Vendor-Specific Attributes* – VSAs), como VLAN dinâmica, ACLs, roles e perfis de acesso.	Obrigatório	
2.13	A solução deve permitir a configuração remota e centralizada de *switches*, incluindo alteração de VLAN e ACL conforme políticas definidas, com ou sem uso de autenticação via 802.1X.	Obrigatório	
2.14	Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-TLS, EAP-TTLS, EAP-MSCHAPv2 e *Protected* EAP (PEAP).	Obrigatório	
2.15	A solução deve suportar notificações SNMPv3, incluindo alertas sobre status dos equipamentos e eventos de segurança, como violações de políticas ou falhas de autenticação.	Obrigatório	
2.16	A solução deve ser capaz de capturar e processar tráfego espelhado, proveniente de uma ou mais interfaces TAP, para fins de identificação de dispositivos conectados (*fingerprinting*) e análise detalhada de tráfego.	Desejável	
2.17	Deve também coletar e processar fluxos de dados nos formatos NetFlow v9 e/ou sFlow, oriundos de múltiplos dispositivos de rede, com o objetivo de realizar *fingerprinting* e caracterização dos ativos.	Desejável	
2.18	A solução deve operar tanto em modo *Proxy* quanto em modo Servidor, conforme necessidade de arquitetura.	Obrigatório	
2.19	A solução deve permitir a integração com o Microsoft *Endpoint Configuration Manager* (SCCM) para validação de conformidade e controle de acesso baseado em status de atualização de registro.	Obrigatório	
2.20	A solução deve permitir a integração com o Microsoft *Intune* para validação de conformidade de dispositivos móveis e desktops gerenciados.	Obrigatório	
2.21	A solução deve permitir a verificação de conformidade de dispositivos Windows com base em atualizações gerenciadas pelo WSUS.	Obrigatório	
2.22	A solução deve permitir o envio de mensagens Syslog personalizadas para destinos específicos, baseadas na avaliação das políticas aplicadas, incluindo no mínimo informações como o usuário autenticado e o endereço IP do dispositivo.	Obrigatório	
3	AGENTE DA SOLUÇÃO	----------	----------
3.1	A solução deverá realizar, de forma contínua, a detecção e categorização de dispositivos conectados à rede, permitindo o controle automático de equipamentos não reconhecidos ou não autorizados, sem a necessidade de instalação de agentes.	Desejável	
3.2	Deverá dispor de agente para instalação em dispositivos clientes que não possam ser gerenciados por mecanismos sem agente (*agentless*). O agente deverá receber configurações, aplicar políticas de segurança da plataforma NAC e executar as ações correspondentes localmente.	Obrigatório	
3.3	Deverá possibilitar a instalação remota e silenciosa do agente, sem intervenção do usuário, por meio de recursos nativos da solução, *login-scripts* e diretivas de grupo (*Group Policy* – GPO).	Obrigatório	
3.4	Deverá permitir a atualização remota e silenciosa do agente, sem necessidade de interação por parte do usuário.	Obrigatório	
3.5	A comunicação entre a plataforma NAC e os agentes instalados deverá ocorrer de forma criptografada, assegurando a confidencialidade e integridade das informações trafegadas.	Obrigatório	
3.6	Deverá oferecer mecanismo para utilização de agente temporário, aplicável em casos nos quais não seja possível realizar a instalação definitiva. Este agente deverá permitir desinstalação automática após o término de sua utilização.	Obrigatório	

3.7	A solução deverá restringir ações do usuário que permitam a desativação, remoção ou alteração das configurações do agente instalado.	Desejável	
3.8	A solução deve ser capaz de verificar e validar a postura dos dispositivos da rede sem agente.	Desejável	
3.9	Deverá permitir a verificação e validação da postura de segurança de dispositivos conectados à rede, tanto nos casos em que não haja agente instalado quanto com agentes permanentes ou temporários.	Obrigatório	
3.10	O agente deverá ser compatível, no mínimo, com os seguintes sistemas operacionais:	----------	----------
3.10.1	*Windows 10 Home/Pro/Enterprise 21H1 ou superior;*	Obrigatório	
3.10.2	*Windows 10 Enterprise LTSC 2021 ou superior;*	Obrigatório	
3.10.3	*Windows 11 Home/Pro/Enterprise 22H2 ou superior;*	Obrigatório	
3.10.4	*Windows 11 Enterprise LTSC 2024 ou superior;*	Obrigatório	
3.10.5	*RHEL 7.x, 8.x e 9.x;*	Obrigatório	
3.10.6	*Ubuntu 24.04;*	Obrigatório	
3.10.7	*Apple macOS 13.x, 14.x, 15.x ou superior.*	Obrigatório	
4	IDENTIFICAÇÃO DE DISPOSITIVOS	----------	----------
4.1	A solução deverá ser capaz de identificar, de forma precisa, o ponto de conexão de cada dispositivo à rede, contemplando, no mínimo, as seguintes informações:	----------	----------
4.1.1	Controladora wireless utilizada;	Desejável	
4.1.2	*Access point* (AP) conectado;	Obrigatório	
4.1.3	SSID empregado na conexão;	Obrigatório	
4.1.4	Porta física do switch utilizada;	Obrigatório	
4.1.5	Fabricante e modelo do *switch*;	Obrigatório	
4.1.6	Identificação (nome e alias) da porta do *switch*;	Desejável	
4.1.7	Números das VLANs de dados e de voz;	Desejável	
4.1.8	Configurações aplicadas à porta do *switch*.	Desejável	
4.2	Para fins de identificação da entrada de novos dispositivos na rede, a solução deverá ser compatível com os seguintes métodos:	----------	----------
4.2.1	Detecção de pacotes DHCP originados pelo dispositivo;	Desejável	
4.2.2	Recebimento de pacotes DHCP via encaminhamento por IP *Helper*;	Obrigatório	
4.2.3	Consulta a tabelas de endereços dos *switches* ou do *gateway* padrão;	Desejável	
4.2.4	Recebimento de traps SNMP gerados pelas controladoras *wireless* ou *switches*;	Desejável	
4.2.5	Processamento de pacotes 802.1X de autenticação, quando atuando como servidor 802.1X;	Obrigatório	
4.2.6	Processamento de pacotes 802.1X de *accounting*, mesmo quando não atuando como servidor 802.1X.	Desejável	
5	CLASSIFICAÇÃO DE DISPOSITIVOS	----------	----------
5.1	A solução deverá ser capaz de detectar e classificar automaticamente os dispositivos conectados à rede, com base em atributos como função, sistema operacional, fabricante, *tags* e demais características relevantes. Essa classificação não deverá se restringir a parâmetros predefinidos, devendo permitir a inclusão de novos critérios conforme necessidade administrativa ou técnica.	Obrigatório	
5.2	A classificação de dispositivos deverá contemplar, no mínimo, as seguintes categorias:	----------	----------
5.2.1	Dispositivos de rede: *access points wireless*, roteadores, *switches*, telefones IP;	Obrigatório	
5.2.2	Dispositivos Apple: iPhone, iPad, equipamentos com macOS;	Obrigatório	
5.2.3	Dispositivos Android: *smartphones* e *tablets*;	Obrigatório	
5.2.4	Impressoras: modelos de fabricantes como HP, Brother, Ricoh;	Obrigatório	
5.2.5	Estações de trabalho: Windows, macOS, Linux;	Obrigatório	

5.2.6	Dispositivos IoT: televisores, câmeras IP, projetores, sensores e equipamentos inteligentes.	Obrigatório	
5.3	Para construção de perfis de dispositivos, a solução deverá implementar, no mínimo, os seguintes mecanismos de coleta de informações:	----------	----------
5.3.1	Informações de pacote DHCP;	Obrigatório	
5.3.2	Detecção de portas TCP abertas;	Obrigatório	
5.3.3	Banner de identificação via NMAP;	Desejável	
5.3.4	Cabeçalhos HTTP obtidos ao acessar o *captive* portal;	Obrigatório	
5.3.5	Atributos RADIUS da sessão 802.1X;	Obrigatório	
5.3.6	Tráfego *Netflow*;	Obrigatório	
5.3.7	Tráfego LLDP;	Desejável	
5.3.8	Consulta SNMP a equipamentos de rede (*switches* e controladoras *wireless*);	Obrigatório	
5.3.9	Dados provenientes de serviços como *Active Directory*;	Obrigatório	
5.3.10	Consultas DNS para resolução de nomes;	Obrigatório	
5.3.11	Endereços IPv4 e IPv6;	Obrigatório	
5.3.12	Detecção da presença ou ausência do agente da solução;	Obrigatório	
5.3.13	Consulta SNMPv1, SNMPv2 ou SNMPv3 ao próprio dispositivo.	Desejável	
5.4	A solução deverá dispor de interface para definição de regras personalizadas de classificação, com capacidade de atribuir pesos e níveis de confiança aos critérios utilizados. Deverá permitir:	----------	----------
5.4.1	Criação de novas regras e categorias personalizadas;	Obrigatório	
5.4.2	Utilização de base de regras e categorias pré-configuradas;	Obrigatório	
5.4.3	Atualização da base de regras e categorias pré-configuradas por meio de mecanismos específicos;	Obrigatório	
5.4.4	Uso da classificação de dispositivos como parâmetro de autorização nas políticas de controle de acesso;	Obrigatório	
5.4.5	Registro manual de dispositivos em categorias específicas pelo administrador da solução.	Obrigatório	
6	ANÁLISE E REMEDIAÇÃO DE POSTURA	----------	----------
6.1	A solução deverá ser capaz de realizar a análise e a remediação de postura de segurança em estações com sistemas operacionais Linux (RHEL e Ubuntu), macOS e Windows (10 e 11), com e/ou sem agente instalado no dispositivo.	Obrigatório	
6.2	A solução deverá ser capaz de identificar e reportar a versão do sistema operacional instalado em cada endpoint gerenciado, utilizando mecanismos de sondagem passiva, ativa ou agentes locais.	Obrigatório	
6.3	A solução deverá ser capaz de identificar o nome do usuário autenticado no sistema operacional do dispositivo gerenciado, utilizando o agente instalado ou, no mínimo, mecanismos como integração com ferramenta de EDR ou recebimento de eventos via Syslog.	Desejável	
6.4	A solução deverá permitir a consulta de chaves e valores de registro do sistema operacional Microsoft Windows, incluindo áreas específicas como HKLM, HKCU, entre outras.	Desejável	
6.5	A solução deverá permitir a execução local de scripts (ex: PowerShell, Bash, Python) no dispositivo gerenciado, como parte de uma ação de correção ou conformidade.	Desejável	
6.6	A solução deverá ser capaz de identificar os dispositivos periféricos conectados via USB em dispositivos Microsoft Windows.	Desejável	
6.7	A solução deverá ser capaz de inventariar aplicativos instalados em endpoints Windows, Linux e macOS.	Desejável	
6.8	A solução deverá ser capaz de verificar a existência de um arquivo em endpoints Windows, Linux e macOS.	Desejável	

6.9	Identificação de Usuário:	----------	----------
6.9.1	Determinar o nome do usuário conectado ao dispositivo;	Obrigatório	
6.9.2	Cruzar os dados do usuário com serviço de diretório para obtenção de informações como nome completo, e-mail e grupos de pertencimento.	Obrigatório	
6.10	Verificação de antivírus:	----------	----------
6.10.1	Verificar se há antivírus instalado e em execução;	Obrigatório	
6.10.2	Verificar a data da última atualização do antivírus;	Obrigatório	
6.10.3	Forçar a atualização da base de vírus (ação de remediação);	Desejável	
6.10.4	Forçar a execução do antivírus quando este estiver inativo (ação de remediação).	Desejável	
6.11	Antivírus suportados nativamente:	----------	----------
6.11.1	Linux: ClamAV, Crowdstrike, Microsoft Defender, SentinelOne;	Desejável	
6.11.2	macOS: Crowdstrike, Microsoft Defender, SentinelOne;	Desejável	
6.11.3	Windows: Crowdstrike, Microsoft Defender, SentinelOne.	Obrigatório	
6.12	A solução deverá executar a verificação do estado de atualização dos pacotes instalados, habilitar o gerenciamento de patches caso esteja desabilitado e realizar a aplicação automatizada das atualizações necessárias nos seguintes sistemas operacionais e ferramentas de gerenciamento:	----------	----------
6.12.1	Red Hat Enterprise Linux: Dandified Yum (DNF);	Desejável	
6.12.2	macOS: Apple Software Update;	Desejável	
6.12.3	Windows: Windows Server Update Services (WSUS) e/ou System Center Configuration Manager (SCCM) / Microsoft Endpoint Configuration Manager.	Obrigatório	
7	CAPTIVE PORTAL	----------	----------
7.1	Deve implementar um portal web seguro (HTTPS) que será automaticamente apresentado aos usuários temporários (visitantes) durante sua conexão com a rede (*hotspot*).	Obrigatório	
7.2	O portal web deverá ser suportado pelos principais navegadores de Internet tais como Microsoft Edge, Mozilla Firefox, Safari e Google Chrome.	Obrigatório	
7.3	Deve implementar um portal HTTPS para a criação de contas temporárias dos tipos visitante, com a autenticação de autorizadores baseados em *Active Directory*, LDAP e atribuição de privilégios para o autorizador de acordo com seu perfil.	Obrigatório	
7.4	Deve ser capaz de implementar a opção "*self-service*" que permite que o usuário visitante crie sua própria conta temporária diretamente. através do portal do *hotspot* seguro, sem a necessidade de um autorizador.	Obrigatório	
7.5	O *captive* portal deve permitir o registro de dispositivos pessoais no modelo *Bring Your Own Device* (BYOD) e a plataforma deve possibilitar a atribuição de diferentes perfis de acesso à rede (cabeada e sem fio).	Obrigatório	
7.6	Permitir a customização do portal, com a inclusão de imagens, textos e campos de texto.	Desejável	
7.7	Para usuários visitantes, a solução deve permitir limitar o tempo de validade do acesso.	Desejável	
7.8	Deve permitir a personalização do formulário de criação de conta temporária que será completado pelo autorizador, especificando campos obrigatórios e opcionais. A criação de novos campos personalizados também deve ser permitida. No entanto, o formulário a ser preenchido deve permitir ao menos os seguintes campos: Nome, Sobrenome, E-mail, Empresa, Telefone e Campos personalizados.	Obrigatório	

7.9	Deve permitir a personalização do nível de segurança da senha temporária que será atribuída ao visitante, especificando o número mínimo de caracteres, o número de caracteres especiais e quantos números serão usados para compor a senha temporária.	Desejável	
7.10	O *captive* portal deve ter suporte nativo para inglês, espanhol e português.	Desejável	
7.11	Deve ter uma API REST para poder fazer inscrições, alterações e exclusões de contas de convidados a partir de sistemas externos à solução.	Desejável	
7.12	Deverá possuir uma Autoridade Certificadora interna para o aprovisionamento e gerenciamento de certificados digitais para dispositivos BYOD.	Desejável	
7.13	O auto-registro de dispositivos dos usuários deve suportar o aprovisionamento de um certificado digital que identifique o dispositivo BYOD e sirva como um método de autenticação para a rede com fio e sem fio.	Desejável	
7.14	O administrador deverá ter a capacidade de suspender/reativar dispositivos e revogar certificados a partir da interface de gerência da solução.	Desejável	
7.15	Deve permitir a integração com sistemas MDM (*Mobile Device Management*).	Desejável	
8	AÇÕES DE CONTROLE	----------	----------
8.1	Alterar dinamicamente a VLAN da porta de switches por meio de protocolos como 802.1X (modo Proxy ou Server) e/ou SNMP.	Obrigatório	
8.2	Executar comando de *shutdown* remoto na porta dos switches via 802.1X ou SNMP.	Obrigatório	
8.3	Configurar dinamicamente parâmetros de porta com base no tipo de dispositivo identificado (ex: estação, telefone IP, impressora).	Obrigatório	
8.4	Atribuição dinâmica de ACLs de acesso (dACL) com base em políticas definidas.	Obrigatório	
8.5	Suporte à ACL do tipo "*filter-id*" compatíveis com controladoras wireless existentes.	Desejável	
8.6	Redirecionamento de tráfego web por meio de ACLs específicas ou políticas de acesso.	Obrigatório	
8.7	Configuração e atribuição de parâmetros de reautenticação via 802.1X.	Obrigatório	
8.8	Implementação do padrão RADIUS *Change of Authorization* (CoA).	Obrigatório	
8.9	Desconexão ou alteração do perfil de conectividade de usuários wireless via 802.1X ou SNMP.	Obrigatório	
8.10	Mapeamento automático do domínio de voz (*Voice Domain*) para dispositivos como telefones IP.	Desejável	
8.11	Personalização e agrupamento de atributos de autorização para compor políticas dinâmicas.	Desejável	
8.12	Criação de perfis de usuários com base em identidade, tipo de dispositivo e comportamento de acesso.	Obrigatório	
8.13	Autorização condicional fundamentada em múltiplos critérios, como:	----------	----------
8.13.1	Atributos LDAP e grupos do *Active Directory*;	Obrigatório	
8.13.2	Campos do certificado digital (CN, OU);	Obrigatório	
8.13.3	Horário de conexão, meio de acesso e localização geográfica;	Desejável	
8.13.4	Tipo de dispositivo (ex: Windows, macOS, Android, iOS);	Desejável	
8.13.5	Conformidade com políticas de segurança por sistema operacional, inclusive via MDM.	Obrigatório	
8.14	Capacidade de combinar livremente os fatores de autorização condicional, mencionados acima, na construção de políticas de autorização.	Obrigatório	
9	GESTÃO DA PLATAFORMA	----------	----------

9.1	A gestão da solução de NAC deverá ser realizada por meio de interface gráfica única e centralizada, instalável e/ou acessível via navegador web.	Obrigatório	
9.2	A console deverá permitir a visualização, administração e configuração de todos os componentes da plataforma, incluindo dispositivos, políticas, inventário e relatórios.	Obrigatório	
9.3	A comunicação entre a console e os *appliances* virtuais deverá ser totalmente criptografada, com suporte a protocolos seguros (TLS/HTTPS).	Obrigatório	
9.4	A console deverá apresentar todos os dispositivos conectados, com suas respectivas características detectadas (como IP, MAC, nome do dispositivo, tipo, sistema operacional, entre outros), sendo as colunas de exibição customizáveis pelo administrador.	Obrigatório	
9.5	A console deverá identificar quais dispositivos estão enquadrados em cada regra de política aplicada, com apresentação clara e detalhada na interface.	Obrigatório	
9.6	Os dispositivos deverão ser organizados em grupos dinâmicos, baseados em qualquer característica disponível, como função, tipo, sistema operacional ou perfil de usuário.	Obrigatório	
9.7	Deverá haver funcionalidade de inventário integrado, com categorização dos dispositivos por tipo, função, usuário associado e sistema operacional.	Desejável	
9.8	O sistema deverá permitir importação e exportação de credenciais temporárias por meio de arquivos em formato .txt ou .csv.	Obrigatório	
9.9	As credenciais de acesso à console deverão ser locais ou integradas a diretórios corporativos, como *Active Directory* (AD) ou LDAP.	Obrigatório	
9.10	Deverá ser implementado controle de acesso baseado em função (RBAC), com perfis customizáveis por usuário ou por grupo do AD/LDAP, permitindo atribuições granulares de permissões.	Obrigatório	
9.11	A console deverá disponibilizar dashboard gráfico interativo e personalizável, com visualização das seguintes informações:	----------	----------
9.11.1	Métricas operacionais das últimas 24 horas;	Obrigatório	
9.11.2	Porcentagem de dispositivos por classificação (tipo/função);	Obrigatório	
9.11.3	Nível de conformidade dos dispositivos por perfil de segurança;	Desejável	
9.11.4	Número de dispositivos conectados via rede cabeada e sem fio;	Desejável	
9.11.5	Proporção entre usuários corporativos e convidados;	Obrigatório	
9.11.6	Número total de dispositivos classificados (*profiling*);	Desejável	
9.11.7	Total de falhas de autenticação nas últimas 24 horas, com indicação dos motivos;	Desejável	
9.11.8	Funcionalidade de *drill-down* para detalhamento de eventos de autenticação e autorização.	Desejável	
9.12	A plataforma deverá contar com mecanismos de auditoria, permitindo o registro e rastreio de ações administrativas realizadas na console.	Obrigatório	
9.13	A arquitetura da console deverá prever alta disponibilidade (HA) e recuperação em caso de falhas, garantindo operação contínua e resiliente.	Obrigatório	

ITEM 5 – SOLUÇÃO DE INTELIGÊNCIA CIBERNÉTICA – OSINT			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	A proponente deverá disponibilizar console de gerenciamento centralizado do sistema.	Obrigatório	
1.2	O funcionamento do produto deverá ser em nuvem com acesso realizado via web pela CONTRATANTE.	Obrigatório	
1.3	O sistema deverá possuir mecanismo de captura automatizado de informações em sites, chats e mídias sociais.	Obrigatório	
1.4	Pesquisar informações em mídias sociais, *deep* web e *dark* web de forma nativa em pelo menos os seguintes tipos de fonte:	----------	----------
1.4.1	Fóruns, Twitter, Facebook, Telegram, Pastebin, RSS feeds, IRC, *Discord*, Sites. Onion, Zone-h, Shodan, *Certificate Transparency*;	Obrigatório	
1.4.2	WhatsApp, Mercado Livre, OLX, lojas de aplicativos.	Desejável	
1.5	Deve realizar monitoramento de marcas na web.	Obrigatório	
1.6	Deve fazer transcrição de áudio captado em grupos de mensageria (pelo menos Telegram e Whatsapp).	Desejável	
1.7	Deve fazer OCR de imagens capturadas em grupos de mensageria (pelo menos Telegram e Whatsapp).	Desejável	
1.8	Deve possuir fontes relevantes pré-configuradas na plataforma em fontes Whatsapp e Telegram relacionada à grupos de fraudadores brasileiros.	Desejável	
1.9	Deve indexar base de vulnerabilidades (CVE) relacionadas a dispositivos e ferramentas de rede e segurança.	Obrigatório	
1.10	Deve monitorar links patrocinados no Google, Bing, Yahoo e redes Sociais.	Obrigatório	
1.11	Deve permitir a configuração dos robôs de coleta da plataforma de forma independente pela CONTRATANTE de forma a não depender da CONTRATADA para direcionar os assuntos de interesse a serem monitorados.	Desejável	
1.12	Deve permitir configurar os *BOTs* com usuários distintos para a mesma fonte de dados.	Desejável	
1.13	Deve oferecer API para integração com outras ferramentas, permitindo o consumo das informações de forma estruturada, além de possibilitar a definição de acessos e perfis distintos conforme a origem da requisição.	Obrigatório	
1.14	Permitir por meio da interface web, o acesso aos logs de falhas e erros dos BOTs.	Desejável	
1.15	Deve permitir a identificação de *defacement* de páginas.	Obrigatório	
1.16	Deve identificar a emissão de certificados de domínios monitorados.	Obrigatório	
1.17	Deve identificar a criação de domínios de recursos monitorados.	Obrigatório	
1.18	Deve permitir a notificação de eventos relevantes em forma de ocorrências para outros usuários em times dentro da organização.	Desejável	
1.19	Deve permitir a associação de múltiplos eventos a uma mesma ocorrência.	Desejável	
1.20	Deve ser possível visualizar diretamente nos eventos a(s) ocorrência(s) em que o dado evento foi associado.	Obrigatório	

1.21	As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.	Desejável	
1.22	Deve ser possível notificar via e-mail a criação e modificação de ocorrências aos times envolvidos.	Desejável	
1.23	Deve realizar técnicas de machine learning para a classificação de imagens na plataforma.	Desejável	
1.24	O Acesso a interface de gerenciamento WEB deve possuir duplo fator de autenticação.	Obrigatório	
1.25	Deve possuir boletins elaborados por Analistas do fabricante com acesso via plataforma com pelo menos os seguintes assuntos: hacktivismo, *malwares*, falhas e vulnerabilidades críticas, fraudes no segmento financeiro, vazamentos de informação, vazamentos de credenciais, ameaças cibernéticas, engenharia social, monitoramento de atores ou grupos de *hackers* ou fraudadores e ataques em larga escala.	Desejável	
1.26	Realização de *Threat Hunting* por meio da plataforma contratada em busca dos assuntos de interesse dentro do contexto de inteligência cibernética e de potenciais ameaças direcionadas a CONTRATANTE; Configuração e parametrização da plataforma para coleta dos assuntos de interesse da CONTRATANTE dentro do contexto de inteligência cibernética de forma a direcionar as informações coletadas na plataforma; Criação de buscas pré-configuradas na plataforma direcionadas para contextos distintos em busca de potenciais ameaças à contratante; Criação de alertas automáticos da plataforma nos assuntos de interesse da contratante no contexto de inteligência cibernética; Elaboração de relatórios de inteligência sobre ameaças de interesse da contratante; Interação com *Threat Actors* no intuito de adquirir informações pertinentes às ameaças em estudo; Interação com o time da CONTRATANTE; Interação com o time interno do fabricante para configuração de monitoramento de fontes de interesse para a CONTRATANTE; Realização de serviços de suporte técnico pelo fabricante; Elaboração de relatório mensal consolidado com todos os *tickets* abertos no mês e informações importantes sobre a CONTRATANTE e setor financeiro.	Obrigatório	
2	GERENCIAMENTO	----------	----------
2.1	Para efetuar o gerenciamento da solução, o sistema deverá:	----------	----------
2.1.1	Possuir interface de gerenciamento no idioma português do Brasil;	Desejável	
2.1.2	Disponibilizar interface web acessível por meio de *cloud* pública;	Obrigatório	
2.1.3	Ser compatível com os navegadores web, nas versões mais recentes e atualizadas, como Google Chrome, Mozilla Firefox e Microsoft Edge;	Obrigatório	
2.1.4	Disponibilizar módulo de administração e gerenciamento de perfis de acesso e grupos de trabalho;	Desejável	
2.1.5	Permitir a configuração de alertas diretamente via interface de gerenciamento;	Obrigatório	
2.1.6	Permitir, no mínimo, configurar, habilitar e desabilitar múltiplos logins de usuários, complexidade de senhas, troca de senha no primeiro *login*, troca de senha periodicamente, ativação e desativação de usuários, definição de grupos e times, duplo fator de autenticação;	Desejável	
2.1.7	Permitir a criação de projetos para cada time, possibilitando que o usuário salve os resultados das pesquisas, individualmente por projeto;	Desejável	
2.1.8	Disponibilizar perfil de administrador para acesso aos recursos da ferramenta, bem como acesso aos dados e alertas de outros usuários;	Obrigatório	
2.1.9	Permitir a criação de grupos de usuários por perfil de acesso e visualização;	Desejável	

2.1.10	Permitir que dentro dos grupos, sejam criados projetos onde todos os usuários participantes tenham acesso aos projetos relacionados ao grupo.	Desejável	
2.2	A solução deverá permitir que, dentro do projeto, o usuário:	----------	----------
2.2.1	Salve consultas para disponibilizar para outros usuários;	Desejável	
2.2.2	Crie, gerencie e exclua alertas;	Desejável	
2.2.3	Salve tabelas de dicionários para o uso em pesquisas.	Desejável	
2.3	Possuir análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades:	----------	----------
2.3.1	Visualização de perfis relacionados a palavras-chaves;	Desejável	
2.3.2	Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;	Desejável	
2.3.3	Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas;	Desejável	
2.3.4	Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;	Desejável	
2.3.5	Exportar as informações identificadas em relatórios via XLS ou CSV, DOCX e PDF.	Desejável	
3	COLETA DE DADOS EM FÓRUNS	----------	----------
3.1	Para efetuar coleta de dados em fóruns, o sistema deverá:	----------	----------
3.1.1	Suportar, minimamente, os seguintes fóruns: PHPBB, PHPNUKE e *vbulletin;*	Obrigatório	
3.1.2	Coletar os dados que foram criados e modificados desde a última coleta;	Obrigatório	
3.1.3	Manter sincronia com a estrutura do fórum analisado. Caso sejam criadas novas estruturas, como novos fóruns ou subfóruns, tópicos ou mensagens, o sistema deverá catalogá-los e iniciar a coleta das informações imediatamente após adição da nova fonte;	Obrigatório	
3.1.4	Manter em sua base de dados informações sobre a última coleta, incluindo data, horário e fuso horário da última coleta realizada em cada fórum;	Desejável	
3.1.5	Deverá extrair, no mínimo, os seguintes metadados de cada mensagem: data, hora e minuto do momento do envio e do momento da coleta;	Desejável	
3.1.6	No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação;	Obrigatório	
3.1.7	Manter todos os metadados da coleta realizada (fonte, grupo, hash da coleta).	Desejável	
4	COLETA DE DADOS EM REDES SOCIAIS	----------	----------
4.1	Para efetuar a coleta de dados de contas em redes sociais, o sistema deverá:	----------	----------
4.1.1	Suportar minimamente as redes sociais Linkedin, X, Instagram e Facebook;	Obrigatório	
4.1.2	Permitir o cadastramento de novas contas de redes sociais;	Desejável	
4.1.3	Coletar publicações já realizadas na conta em questão, mesmo que estas sejam anteriores à data de cadastramento no sistema;	Desejável	
4.1.4	Coletar as novas publicações feitas pela conta desde a última coleta;	Obrigatório	
4.1.5	Extrair, no mínimo, os seguintes metadados de cada mensagem: data, hora e minuto do momento do envio e do momento da coleta;	Desejável	
4.1.6	Possuir mecanismo que busque automaticamente novas publicações das contas cadastradas conforme um agendamento pré-configurado;	Desejável	
4.1.7	Monitorar pelo menos 2000 perfis brasileiros relacionados a fraudes ou segurança cibernética em redes sociais monitoradas;	Desejável	

4.1.8	Coletar apenas as publicações que ainda não constam em sua base de dados. Alterações também deverão ser catalogadas e armazenadas. No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação.	Obrigatório	
5	COLETA DE DADOS EM REDES DE COMPARTILHAMENTO DE TEXTOS	----------	----------
5.1	Para efetuar a coleta de dados em redes de compartilhamentos de texto, a solução deverá:	----------	----------
5.1.1	Suportar automaticamente a rede de compartilhamento de textos *pastebin;*	Obrigatório	
5.1.2	Permitir o cadastramento de novas contas de redes de compartilhamento de textos;	Desejável	
5.1.3	Realizar a coleta de publicações já existentes na conta cadastrada, inclusive aquelas anteriores à data de inclusão no sistema;	Obrigatório	
5.1.4	Coletar novas publicações realizadas pela conta desde a última coleta efetuada;	Obrigatório	
5.1.5	Extrair, no mínimo, os seguintes metadados de cada publicação: data, hora e minuto do envio e da coleta;	Desejável	
5.1.6	Possuir mecanismo de busca automática por novas publicações nas contas cadastradas, conforme agendamento pré-configurado;	Desejável	
5.1.7	Coletar apenas publicações ainda não registradas na base de dados. Alterações em publicações já coletadas devem ser identificadas, catalogadas e armazenadas. Em caso de exclusão na origem, as publicações não deverão ser removidas da aplicação.	Desejável	
6	COLETA DE DADOS EM APLICATIVOS DE TROCA DE MENSAGENS	----------	----------
6.1	Para efetuar a coleta de dados em aplicativos de troca de mensagens, a solução deverá:	----------	----------
6.1.1	Suportar, no mínimo, de forma automática, os seguintes aplicativos de troca de mensagens: WhatsApp, Telegram, Discord e IRC;	Obrigatório	
6.1.2	Possuir foco no Brasil, com monitoramento de grupos relacionados a fraudes em língua portuguesa, ao menos nos aplicativos WhatsApp, Telegram, IRC e Discord;	Desejável	
6.1.3	Monitorar grupos brasileiros relacionados a fraudes ou problemas cibernéticos no WhatsApp;	Desejável	
6.1.4	Monitorar grupos brasileiros relacionados a fraudes ou problemas cibernéticos no Telegram;	Desejável	
6.1.5	Monitorar servidores brasileiros no Discord;	Desejável	
6.1.6	Monitorar servidores com usuários brasileiros em seus canais no IRC;	Desejável	
6.1.7	Permitir a criação de robôs específicos, com a adição de novas contas e números de telefone nas soluções de aplicativos de troca de mensagens (WhatsApp, Telegram, *Discord* e IRC);	Desejável	
6.1.8	Permitir a inclusão e o monitoramento de novos grupos dos aplicativos de troca de mensagens;	Obrigatório	
6.1.9	Coletar publicações já realizadas nos grupos monitorados, mesmo que anteriores à data de cadastramento no sistema, desde que disponibilizadas pelo aplicativo;	Obrigatório	
6.1.10	Coletar novas publicações realizadas pelas contas monitoradas desde a última coleta;	Obrigatório	
6.1.11	Extrair, no mínimo, os seguintes metadados de cada mensagem: data, hora e minuto da coleta, ambas com precisão de segundos, coletar dados públicos dos usuários participantes dos grupos;	Desejável	
6.1.12	Possuir mecanismo que realize buscas automáticas por novas publicações das contas cadastradas, conforme agendamento pré-configurado;	Desejável	

6.1.13	Coletar apenas publicações que ainda não constem na base de dados. Alterações nas publicações também deverão ser catalogadas e armazenadas. Em caso de exclusão na origem, as publicações não deverão ser removidas da aplicação;	Obrigatório	
6.1.14	Ser capaz de identificar e registrar mensagens com anexos (imagens, áudios, vídeos, documentos), incluindo metadados como tipo de mídia, tamanho e nome do arquivo;	Desejável	
6.1.15	Identificar mensagens que foram editadas ou encaminhadas, registrando essa informação nos metadados.	Desejável	
7	BUSCA DO CONTEÚDO	----------	----------
7.1	Para efetuar a busca de conteúdo, a solução deverá:	----------	----------
7.1.1	Disponibilizar mecanismo para busca de informações, permitindo: busca por intervalo de datas, por metadados e por base de dados;	Obrigatório	
7.1.2	Disponibilizar, por meio de *interface web*, a busca utilizando mecanismos como: proximidade, fuzzy (difusa), lógica binária, expressões regulares, operadores lógicos (“AND”, “OR” e “NOT”) e caracteres *wildcard*;	Desejável	
7.1.3	Permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga;	Desejável	
7.1.4	Permitir a definição da quantidade de resultados exibidos por página;	Desejável	
7.1.5	Realizar a busca de conteúdo dentro dos arquivos indexados;	Desejável	
7.1.6	Permitir integração com API REST, com suporte ao retorno de informações nos formatos XML ou JSON;	Obrigatório	
7.1.7	Permitir salvar o resultado da pesquisa.	Desejável	
8	ALERTAS	----------	----------
8.1	Para efetuar a geração de alertas, a solução deverá:	----------	----------
8.1.1	Disponibilizar ambiente para criação e gerenciamento de alertas, com as mesmas funcionalidades oferecidas pelo ambiente de busca, exibindo os alertas já configurados, respeitando as permissões de acesso dos usuários e grupos aos quais pertencem;	Desejável	
8.1.2	Permitir a criação de alertas com configuração de periodicidade, expressão de busca e definição de endereços eletrônicos para envio;	Obrigatório	
8.1.3	Possibilitar a ativação, desativação, edição e exclusão de alertas existentes, conforme as permissões de acesso;	Desejável	
8.1.4	Executar alertas ativos, conforme o agendamento previamente configurado;	Desejável	
8.1.5	Enviar e-mails contendo os alertas, incluindo os resultados encontrados, separados por base de dados, a quantidade de ocorrências identificadas e o *timestamp* do momento da geração do alerta;	Desejável	
8.1.6	Possibilitar o envio de e-mails criptografados;	Desejável	
8.1.7	Possibilitar o envio de e-mails autenticados;	Obrigatório	
8.1.8	Disponibilizar opção para teste dos alertas existentes.	Desejável	
8.2	Para a geração de testes de alerta, o sistema deverá consultar a base de dados existente e enviar e-mail com os resultados obtidos.	Desejável	
8.3	A interface de acesso e consulta deverá ser instalada em ambiente de nuvem da CONTRATADA.	Obrigatório	
8.4	A ferramenta deverá ser licenciada no mínimo para 05 usuários com acesso a todas as funcionalidades disponíveis.	Obrigatório	

ITEM 6 – SOLUÇÃO DE COFRE DE SENHA E GESTÃO DE ALTAS CREDENCIAIS – PAM			
Nº	**CARACTERÍSTICAS TÉCNICAS**	**REQUISITO**	**RESPOSTA DO FORNECEDOR (S/N)**
1	CARACTERÍSTICAS GERAIS	----------	----------
1.1	Suportar, no mínimo, 3.000 sessões simultâneas.	Obrigatório	
1.2	Suportar, no mínimo, 650.000 horas de armazenamento de gravação de sessões.	Obrigatório	
1.3	Os usuários geridos pela solução poderão estar conectados simultaneamente.	Obrigatório	
1.4	Solução para armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux/Unix, Windows, Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede, totalizando 75 usuários ou 5.400 dispositivos. Deve permitir que até 30 usuários estejam conectados simultaneamente.	Obrigatório	
1.5	Prover autenticação transparente no sistema-alvo ou dispositivo de rede. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um *proxy* para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso.	Obrigatório	
1.6	Eliminar credenciais inseridas em códigos-fonte, *scripts* e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e invisíveis aos desenvolvedores e equipe de suporte de TI.	Desejável	
1.7	Banco de dados de uso exclusivo para evitar que informações sejam armazenadas em bancos de dados compartilhados.	Obrigatório	
1.8	Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências.	Obrigatório	
1.9	Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer *software* nos sistemas-alvos ou dispositivos de rede.	Obrigatório	
1.10	Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa.	Obrigatório	
1.11	Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.	Obrigatório	
1.12	Possibilidade de manter senhas privilegiadas em aplicações e integração com sistemas legado.	Obrigatório	
1.13	Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução.	Obrigatório	
1.14	Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo.	Obrigatório	
1.15	Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata.	Obrigatório	
1.16	Provisionamento de usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede.	Desejável	

1.17	Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais.	Obrigatório	
1.18	Permitir o monitoramento on-line do uso das contas e desligamento da sessão.	Obrigatório	
1.19	Apresentar o recurso "*break glass*" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade.	Obrigatório	
1.20	Armazenamento de certificados digitais.	Desejável	
1.21	Publicação de certificados digitais em servidores de aplicação (Tais como: Apache, IIS, *Weblogic, WebSphere*, entre outras).	Desejável	
1.22	Oferecer a funcionalidade de "*Discovery*" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos.	Obrigatório	
1.23	Oferecer a funcionalidade de "*Discovery*" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente os certificados.	Desejável	
1.24	Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido.	Obrigatório	
1.25	Monitorar e avaliar as atividades de contas ou grupos privilegiados que não são administrados pela solução.	Desejável	
1.26	Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.	Obrigatório	
1.27	Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado.	Obrigatório	
1.28	Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato ".csv".	Obrigatório	
1.29	A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH, API REST HTTP/HTTPS.	Obrigatório	
1.30	Caso seja necessária alguma integração com aplicações legadas e/ou integrações com o ambiente interno, o mesmo deverá ser customizado e desenvolvido pelo fabricante.	Desejável	
1.31	Extrair informações do servidor localizado nos *Data Centers* remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas.	Obrigatório	
1.32	A solução deve possuir função de monitoramento e análise de comportamento para os sistemas e/ou dispositivos que contemplem, no mínimo, as especificações técnicas do parque computacional da CONTRATANTE.	Obrigatório	
1.33	A solução deve possuir ferramenta de monitoração própria para que seja possível especificar limiares (*threasholds*) referente ao uso de memória, CPU, disco e banco de dados, por exemplo.	Obrigatório	
1.34	Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução.	Desejável	
1.35	No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades.	Obrigatório	

1.36	Alterações realizadas no *cluster* de cofre de senhas de alta disponibilidade local devem ser automaticamente replicadas para os outros servidores de redundância.	Obrigatório	
1.37	Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (*Hash)* e endereço IP do host ou conjunto de hosts a serem acessados pela solução.	Obrigatório	
1.38	Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS.	Obrigatório	
1.39	Possibilidade de implementação SNMP sobre IPv6.	Desejável	
1.40	Implementar a especificação IETF RFC 2460, referente ao protocolo IPv6.	Desejável	
1.41	A solução deve realizar agendamento automático para descoberta de ativos na rede trazendo, no mínimo, as seguintes informações dos ativos descobertos: sistema operacional, hardware instalado, software instalado, serviços rodando, portas abertas e processos em execução.	Desejável	
1.42	Possuir funcionalidade de "AD Bridge" para integração de servidores Linux/Unix no *Active Directory*, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD.	Desejável	
1.43	Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local.	Obrigatório	
1.44	Caso seja separado em componentes, nenhum deles deve conter senhas em texto claro para autenticação.	Obrigatório	
1.45	Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA ou ECC.	Obrigatório	
1.46	Liberação de acesso para execução de tarefas específicas em plataforma SSH.	Obrigatório	
1.47	Liberação de acesso para execução de tarefas específicas em plataforma TELNET.	Desejável	
1.48	Tanto appliances quanto sistemas operacionais devem ser "hardenizados" e protegidos com firewall interno e detecção de intrusão.	Obrigatório	
2	GESTÃO DE USUÁRIOS E PERFIS	----------	----------
2.1	Cadastro de usuários com informações de nome e e-mail.	Obrigatório	
2.2	Cadastro de perfis de usuários.	Obrigatório	
2.3	Segregação de funções por perfis de acesso.	Obrigatório	
2.4	Flexibilidade para criação de quaisquer perfis novos, com diversas combinações de telas e funcionalidades de acordo com a necessidade do negócio sem intervenção do fornecedor.	Obrigatório	
2.5	Importação automática de contas de usuários do AD.	Obrigatório	
2.6	Importação automática de contas de usuários do LDAP.	Obrigatório	
2.7	Gerenciamento de Grupos e Perfis de acesso integrados aos grupos de AD.	Obrigatório	
2.8	Permitir que o administrador solicite para um usuário justificativa de ações executadas em uma sessão.	Desejável	
3	AUTENTICAÇÃO DE USUÁRIOS	----------	----------
3.1	Autenticação local através de usuários e senha.	Obrigatório	
3.2	Autenticação centralizada integrada com LDAP, LDAPS para MS AD com múltiplos DCS.	Obrigatório	
3.3	Autenticação centralizada integrada com RADIUS.	Desejável	
3.4	Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores.	Obrigatório	
3.5	Duplo fator de autenticação nativo para acesso web ou através de cliente.	Desejável	

3.6	Gestão de autenticação com múltiplos autenticadores simultaneamente.	Obrigatório	
4	CADASTRO DE ATIVOS	----------	----------
4.1	Cadastro de equipamentos parametrizado manualmente.	Obrigatório	
4.2	Atributos como Marca, Modelo, Fabricante, Localidade, Grupo abertos para configuração do administrador da ferramenta independente do fabricante.	Obrigatório	
4.3	Discovery automatizado de credencias em servidores e bancos de dados.	Desejável	
4.4	*Scan* e *Discovery* automatizado de certificados digitais.	Desejável	
4.5	Cofre de Credenciais.	Obrigatório	
4.6	Sistema seguro de armazenamento de credenciais e senhas.	Obrigatório	
4.7	Armazenamento de senhas criptografadas com padrões de criptografias fortes como AES 256 ou superior.	Obrigatório	
4.8	Consolidação periódica de senhas para identificar senhas que foram alterados em sistema gerenciados.	Obrigatório	
4.9	Envio de alerta por SIEM de senhas que não estejam iguais ao cofre.	Obrigatório	
5	COFRE DE INFORMAÇÕES PRIVILEGIADAS	----------	----------
5.1	Armazenamento de certificados digitais.	Desejável	
5.2	Armazenamento de senhas pessoais.	Obrigatório	
5.3	Alerta de vencimento de informações armazenadas.	Obrigatório	
5.4	Logs de alteração de informações privilegiadas.	Obrigatório	
5.5	Disponibilização de vídeo sem *download* com fluxo dentro da ferramenta.	Desejável	
5.6	Permissão para compartilhamento de informações com outros usuários.	Obrigatório	
6	GRAVAÇÃO DE LOGS (VÍDEOS E COMANDOS)	----------	----------
6.1	Gravação de Vídeo das sessões realizadas através de *webproxy* ou *proxy* transparente em formato otimizado.	Obrigatório	
6.2	Gravação de comandos digitados em ambientes SSH.	Obrigatório	
6.3	Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download.	Desejável	
6.4	Proxy Transparente com gravação de *logs* e vídeos ao sistema alvo sem revelar aos usuários as credenciais utilizadas através de cliente local utilizado pelo usuário como *Putty*, ou RDP *Client* sem necessidade de abrir interface web ou baixar nenhum cliente adicional na máquina do usuário.	Desejável	
6.5	Exportação de sessão em formato vídeo.	Desejável	
6.6	Gravação de comandos digitados em ambientes RDP.	Desejável	
6.7	Busca de registro de sessão por usuário, sistema alvo, ip alvo, data e hora.	Obrigatório	
6.8	Busca por comandos e entradas de teclado digitados em plataforma Linux.	Obrigatório	
6.9	Busca de comandos e entradas de teclado em plataforma Windows.	Obrigatório	
6.10	Gravação de *Logs* de *Input* e *Output* de comandos.	Obrigatório	
6.11	Sem necessidade de agentes locais para gravação de sessão.	Obrigatório	
6.12	Marcação de pontuação de comandos de acordo com nível de risco de cada comando.	Desejável	
6.13	Armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:	----------	----------
6.13.1	Identificação do usuário que realizou determinado acesso a um dispositivo;	Obrigatório	
6.13.2	Identificação de quem aprovou o acesso do usuário;	Obrigatório	

6.13.3	Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto.	Obrigatório	
6.14	Prover, ao menos, os seguintes filtros para a recuperação de logs: Usuário; Dispositivo acessado, Tipo de conexão, Intervalo de tempo (data/hora/minuto inicial e final).	Obrigatório	
6.15	Permitir o acompanhamento on-line de sessões remotas pelo administrador e desligamento da sessão remotamente.	Obrigatório	
7	BLOQUEIO DE COMANDOS E CONTROLE DE PRIVILÉGIOS	----------	----------
7.1	Bloqueio e/ou alerta de comandos, interrupção de sessão ou apenas o registro de execução.	Desejável	
7.2	Possibilidade de bloqueio e auditoria de comandos específicos.	Obrigatório	
7.3	Interface para acesso via RDP a aplicações locais com gravação de sessão.	Desejável	
7.4	No caso de acesso a aplicação remota (*Remote App*) ao fechar a aplicação a sessão do usuário deve ser encerrada.	Desejável	
7.5	Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.	Obrigatório	
7.6	Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado.	Obrigatório	
7.7	Marcação de pontuação de comandos de acordo com nível de risco de cada comando.	Desejável	
8	ROTAÇÃO DE SENHAS	----------	----------
8.1	Troca automática de senhas para servidores (Unix, Linux, Windows), bancos de dados (MS SQL, ORACLE, MYSQL, PostgreSQL), dispositivos de rede, *mainframe*.	Obrigatório	
8.2	Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da Instituição.	Obrigatório	
8.3	Flexibilidade para configuração de força de senha gerada.	Obrigatório	
8.4	Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.	Obrigatório	
8.5	Possibilidade de manter senhas privilegiadas em aplicações e integração com sistemas legado.	Obrigatório	
8.6	*Templates* com linguagem acessível e fácil interpretação.	Desejável	
8.7	Gatilhos de transferência de arquivo - Permitir colocar plugins para avaliar ou notificar sobre um arquivo que está sendo transferido para um servidor.	Desejável	
8.8	Armazenamento de histórico de senhas por equipamento.	Obrigatório	
8.9	Registro de troca de senha executadas.	Obrigatório	
8.10	Relatório de acompanhamento de trocas de senha.	Obrigatório	
8.11	Relatório de erros de trocas de senha.	Obrigatório	
8.12	Alertas de falha ou sucesso de trocas de senha.	Obrigatório	
8.13	*Templates* abertos e configuráveis para criação de *booking* para execução de comandos específicos, conforme perfil do usuário ou grupo de usuários.	Desejável	
8.14	Cadastrar automaticamente chaves públicas das chaves SSH em servidores autorizados.	Desejável	
8.15	Possibilidade de reconfiguração de scripts de troca de senha por configuração.	Obrigatório	
8.16	Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca.	Obrigatório	
8.17	Disponibilizar os *templates* de troca de senha de forma que possam ser abertos, editáveis e auditáveis.	Desejável	
8.18	*Templates* com linguagem acessível e fácil interpretação.	Desejável	
8.19	Fluxo de aprovação de alteração de *template* para evitar fraudes.	Obrigatório	

8.20	Rastreabilidade de alteração de *template*.	Desejável	
8.21	Troca de senhas em aplicações HTTP/HTTPS com *templates*.	Desejável	
9	ANÁLISE DE COMPORTAMENTO	----------	----------
9.1	Análise de sessão de usuário baseado em histórico de comportamento. Análise mínima das variáveis de estações origem, estações destino, credenciais, horários, duração de sessão.	Obrigatório	
9.2	Identificação de comportamentos diferenciados com alertas de anormalidades em relatórios em tela ou alertas para SIEM/SYSLOG.	Obrigatório	
9.3	Análise de sessão de usuários com pontuação de comando críticos com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG.	Obrigatório	
9.4	*Dashboards* gráficos com informações sobre riscos e ameaças.	Obrigatório	
10	DASHBOARDS E RELATÓRIOS	----------	----------
10.1	Relatórios de operação com lista e usuários cadastrados, equipamentos cadastros, credenciais cadastradas.	Obrigatório	
10.2	Relatórios PCI.	Desejável	
10.3	Relatórios de Gestão de Evidências.	Obrigatório	
10.4	Relatórios de Auditoria.	Obrigatório	
10.5	Relatórios de Alertas.	Obrigatório	
10.6	Exportação para Excel (.csv).	Obrigatório	
10.7	Dashboard de utilização.	Obrigatório	
10.8	Dashboard de conexões.	Obrigatório	
10.9	Dashboard de utilização de sessões.	Obrigatório	
10.10	Dashboard de sessão.	Obrigatório	
10.11	Dashboard de usuário.	Obrigatório	
10.12	Dashboard de servidor.	Obrigatório	
11	CENTRAL DE GERENCIAMENTO	----------	----------
11.1	Console central de gerenciamento de aplicação com capacidade para:	----------	----------
11.1.1	Suporte à utilização de certificados digitais válidos pela ICP-Brasil e certificados auto-assinados gerados pela própria solução;	Desejável	
11.1.2	Criação de usuários;	Obrigatório	
11.1.3	Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;	Obrigatório	
11.1.4	Busca de sessão gravada;	Obrigatório	
11.1.5	Possibilidade de sessão remota através de programa clientes instalados na estação de trabalho do usuário sem a necessidade de passar por aplicação web ou baixar nenhum cliente adicional na máquina do usuário;	Desejável	
11.1.6	Busca de Consulta de senhas;	Obrigatório	
11.1.7	Gestão de políticas de acesso centralizadas;	Obrigatório	
11.1.8	Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;	Desejável	
11.1.9	Cadastro de dispositivos centralizados.	Obrigatório	
12	AMBIENTE DE INSTALAÇÃO	----------	----------
12.1	Tanto *appliances* quanto sistemas operacionais devem ser "hardenizados" e protegidos com firewall interno e detecção de intrusão.	Desejável	
12.2	A solução deve ser baseada em *appliance* virtual ou físico, atendendo as seguintes especificações:	----------	----------
12.2.1	Caso o banco de dados e/ou Sistema Operacional utilizado seja de terceiros (exemplo: ORACLE/SQL ou Windows), a solução deverá ser entregue com licenças de software e garantia que a compatibilize com a solução;	Obrigatório	

12.2.2	Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação, sem custos adicionais para a CONTRATANTE;	Obrigatório	
12.2.3	Não haver necessidade de utilização de ferramentas de terceiros para completar a solução, ou seja, um fabricante único que atenda todas as necessidades;	Obrigatório	
12.2.4	Possibilidade de configuração em cluster de contingência, alta disponibilidade (HA) e recuperação de desastres (DR).	Desejável	
13	ARQUITETURA DE IMPLANTAÇÃO DA SOLUÇÃO	----------	----------
13.1	Para as soluções ofertadas em virtual *appliance* ou máquina virtual, os recursos de hardware serão fornecidos pela CONTRATANTE.	Obrigatório	
13.2	Para que a solução continue funcionando localmente mesmo com a falha de um nó de cada elemento, no mínimo os seguintes elementos devem ser instalados em regime de alta disponibilidade:	----------	----------
13.2.1	A solução deve replicar as configurações, de modo que, no evento de falha de um dos *appliances*, a solução continue disponível.	Obrigatório	
13.3	O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é:	----------	----------
13.3.1	Appliance principal: Ativo;	Obrigatório	
13.3.2	Appliance secundário: Ativo.	Obrigatório	
13.4	Caso a solução fornecida seja do tipo appliance (*hardware*), devem ser fornecidos pela CONTRATADA, no quantitativo necessário para atender aos requisitos de arquitetura e alta disponibilidade apresentados, com todas as licenças válidas, com garantia igual ao do objeto desta contratação e sem custos adicionais para a CONTRATANTE.	Obrigatório	

ANEXO III

(TIMBRE DA EMPRESA)
DECLARAÇÕES PARA PARTICIPAÇÃO DO PROCESSO

À
ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO POUPEX
GERÊNCIA DE COMPRAS E CONTRATOS (GECOC)
Avenida Duque de Caxias s/nº, Setor Militar Urbano, Parte A
70630-902 – Brasília/DF

A empresa ....., inscrita no CNPJ sob o nº ....., por intermédio de seu representante legal o(a) Sr(a) ....., portador(a) da Cédula de Identidade no..... e do CPF/MF no ....., referente ao processo de fornecimento de solução(ões) de segurança cibernética para proteção contínua dos ativos informacionais da POUPEX, atendendo boas práticas de segurança cibernética e em conformidade com órgãos reguladores, **DECLARA**, sob as penalidades da lei, para fins de participação deste processo de contratação, que:

( ) atende a especificação técnica em sua totalidade, bem como ACEITA a minuta de contrato anexa à referida especificação técnica.

( ) não permite a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal na execução de suas atividades, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

( ) não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos. Ressalva: emprega ..... (INFORMAR NÚMERO DE MENORES) menor(es), a partir de quatorze anos, na condição de aprendiz;

( ) busca prevenir e erradicar práticas danosas ao meio ambiente, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos à produção, consumo e destinação dos resíduos sólidos de maneira sustentável, implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

( ) é acompanhada por auditoria interna ou externa e responsabiliza pela veracidade das informações prestadas, onde está sujeita a sanções na forma da lei e sobre. Garante a existência de plano de continuidade de negócios, mantendo a prestação de serviços conforme estabelecido no item 3 - DESCRIÇÃO DA SOLUÇÃO e 4 ESPECIFICAÇÃO DA SOLUÇÃO.

(Nome da cidade), ---------- de ---------- de 2025.

Nome e assinatura do representante legal
Cédula de Identidade (número e órgão expedidor)

OBSERVAÇÃO: caso o representante que estiver subscrevendo o presente documento não seja o sócio administrador ou diretor, declarado no contrato social ou na ata de constituição, será necessário comprovar os poderes para assinatura.

ANEXO III
MINUTAS DE CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ____/2025 - POUPEX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE SOLUÇÕES DE SEGURANÇA CIBERNÉTICA FIRMADO ENTRE A POUPEX E A _____.

A **ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO - POUPEX**, sediada na Av. Duque de Caxias s/n.º, Parte A, Setor Militar Urbano - SMU, Brasília/DF, CEP 70630-902, inscrita no CNPJ nº 00.655.522/0001-21, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) (cargo) _____, na forma autorizada por (documento) _____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado(a) em _____, doravante denominada **CONTRATANTE**, e a **(razão social – nome fantasia)** _____, sediada no endereço _____, CEP _____, inscrita no CNPJ nº _____, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) _____ (cargo), conforme (documento - contrato social, procuração)_____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado (a) em _____, doravante denominada **CONTRATADA**, têm justo e avençado o presente contrato de prestação de serviços, conforme Proposta Técnica e Comercial de Preço de ____/____/_____ e Especificação Técnica, de ___/____/____, partes integrantes deste instrumento, regido pelas cláusulas seguintes e pelas normas de Direito Privado:

1. OBJETO

1.1. O objeto do presente contrato consiste na contratação de empresa especializada para soluções de segurança cibernética visando à proteção contínua dos ativos informacionais da CONTRATANTE, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação, contendo os seguintes itens:

Tabela 1

Item	Descrição	Quant.
1.	Solução de Gestão de Vulnerabilidades (deve vir com o suporte técnico do fabricante incluso)	1
1.1	Implementação da solução de Gestão de Vulnerabilidades.	1
1.2	Repasse de conhecimento da solução de Gestão de Vulnerabilidades.	1
2.	Solução de *Breach and Attack Simulation* – BAS (deve vir com o suporte técnico do fabricante incluso)	1
2.1	Implementação da solução de *Breach and Attack Simulation* – BAS.	1
2.2	Repasse de conhecimento da solução de *Breach and Attack Simulation* – BAS.	1
3.	Solução de Inteligência Cibernética – OSINT (deve vir com o suporte técnico do fabricante incluso)	1
3.1	Implementação da solução de Inteligência Cibernética – OSINT.	1
3.2	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT.	1

2. CONDIÇÕES PARA EXECUÇÃO DOS SERVIÇOS

2.1. A CONTRATADA realizará todas as atividades, preferencialmente, no horário comercial, de segunda a sexta-feira exceto feriados, das 8h às 18h.

2.2. A entrega da(s) solução(ões) será(ão) realizada(s) de forma digital, por meio de disponibilização remota dos *softwares* e respectivos componentes.

2.3. A execução dos serviços de implementação e repasse de conhecimento, se necessário, deverá ocorrer de forma remota.

2.4. As soluções de segurança deverão ser fornecidas por meio de licenciamento anual, contemplando todos os componentes necessários para sua plena operação, incluindo *software*, atualizações, suporte técnico e documentação. O modelo de fornecimento será tradicional, com licenças válidas por 12 meses, renováveis conforme a necessidade da CONTRATANTE, garantindo o funcionamento integral das funcionalidades contratadas durante todo o período de vigência.

2.5. A solução deverá oferecer acesso contínuo a atualizações de segurança, correções de vulnerabilidades, melhorias de desempenho e novas funcionalidades disponibilizadas pelo fabricante, sem custos adicionais durante o período de licenciamento.

2.6. A CONTRATADA será responsável por fornecer os meios necessários para ativação, instalação e configuração inicial da solução, além de disponibilizar manuais, guias técnicos e acesso à base de conhecimento. A solução deverá ser compatível com o ambiente tecnológico da CONTRATANTE e permitir integração com outras ferramentas de segurança já existentes, quando aplicável.

2.7. A efetividade da solução será avaliada por meio de relatórios técnicos, indicadores de desempenho e evidências de funcionamento, conforme critérios definidos pela área técnica da CONTRATANTE.

2.8. Descrição da solução:

2.8.1. **Solução de Gestão de Vulnerabilidades:** ferramenta especializada na identificação proativa de falhas de segurança em sistemas, aplicações e dispositivos de rede. Realiza varreduras automatizadas e abrangentes, detectando vulnerabilidades conhecidas, configurações incorretas e exposições a riscos. Fornece relatórios detalhados e priorização de correções, apoiando a gestão contínua da postura de segurança e a conformidade com normas como PCI-DSS, ISO 27001 e LGPD.

2.8.2. **Solução de *Breach And Attack Simulation* (BAS):** plataforma que simula ataques cibernéticos reais de forma controlada para avaliar, em tempo real, a eficácia das defesas de segurança da organização. Testa continuamente controles como firewall, EDR, AntiSpam e políticas de resposta, identificando brechas e vulnerabilidades antes que sejam exploradas. Gera insights acionáveis para fortalecer a postura de segurança, acelerar a correção de falhas e garantir conformidade com frameworks como *MITRE ATT&CK*.

2.8.3. **Solução de inteligência cibernética (OSINT):** ferramenta voltada à coleta, análise e correlação de informações públicas disponíveis em fontes abertas como redes sociais, fóruns, sites, domínios e repositórios técnicos. Auxilia na identificação de ameaças externas, exposição de dados sensíveis, perfis de atacantes e riscos reputacionais. Essencial para operações de *threat intelligence*, investigação digital e monitoramento preventivo de ativos expostos na internet.

2.9. Serviços de implementação: a CONTRATADA será responsável pela instalação, configuração e validação inicial da solução, garantindo sua plena operação conforme os requisitos técnicos definidos pela CONTRATANTE.

2.10. Repasse de Conhecimento: serão realizadas atividades de repasse de conhecimento técnico às equipes da CONTRATANTE, com foco na solução implementada, visando assegurar o entendimento aprofundado de sua arquitetura, funcionalidades e procedimentos operacionais. Esse processo tem como objetivo promover autonomia na gestão e manutenção da solução. O repasse de conhecimento poderá ser disponibilizado também sob demanda, por meio de acesso a plataformas especializadas oferecidas pelo fabricante, proporcionando maior flexibilidade e continuidade no processo de assimilação técnica.

2.11. Suporte Técnico: o suporte técnico deverá estar incluso no licenciamento e prestado exclusivamente pelo fabricante da solução, assegurando domínio completo da tecnologia ofertada e maior eficiência na identificação e resolução de incidentes. O serviço deverá estar disponível em regime 24x7, com atendimento remoto e escalonamento conforme a criticidade dos chamados, assegurando a continuidade operacional da solução durante todo o período de vigência do contrato.

2.12. Acordo de Nível de Serviço para Chamados de Suporte Técnico: o suporte técnico será prestado diretamente pelo fabricante da solução mediante abertura de chamado por parte da CONTRATANTE e o Acordo de Nível de Serviço – ANS obedecerá ao descrito na plataforma do fabricante, sendo obrigatoriamente na modalidade de 24 x 7 para resolução de incidentes e demandas.

2.12.1. será dado início a abertura do chamado para o suporte técnico através dos canais: e-mail (_____) ou telefone (_____) para a centralização dos chamados e controles de SLA.

2.13. A CONTRATANTE e a CONTRATADA são pessoas jurídicas totalmente distintas e independentes, não configurando este contrato nenhuma forma de sociedade, pelo que os profissionais terceirizados, designados pela CONTRATADA para a prestação dos serviços objeto deste contrato, atuarão sem qualquer subordinação laboral à CONTRATANTE e, portanto, inexistente vínculo ou relação de trabalho com a CONTRATANTE.

3. PREÇO

3.1. O valor total deste contrato é de R$ _____ (_____).

3.2. As despesas decorrentes deste contrato correrão por conta dos recursos próprios da POUPEX, consignados na conta orçamentária. Centro de custo: _____. Conta contábil/orçamentaria _____.

3.3. Nos preços fixados nesta cláusula estão compreendidos todos os custos e despesas que, direta ou indiretamente, decorram do cumprimento pleno e integral do objeto deste contrato, tais como e sem se limitar a: telefone, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, softwares, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

4. FORMA E CONDIÇÕES DE PAGAMENTO

4.1. A CONTRATANTE pagará à CONTRATADA, conforme quadro abaixo, pela prestação dos serviços objeto deste contrato, após a conclusão dos serviços, mediante a emissão do Termo de Recebimento, Aceitação dos Serviços e atesto na nota fiscal a ser apresentada com 10 (dez) dias de antecedência do vencimento:

Item	Descrição	Qtd	Valor Unitário (R$)	Valor Total (R$)
1.	Solução de Gestão de Vulnerabilidades	1		
1.1	Implementação da solução de Gestão de Vulnerabilidades.	1		
1.2	Repasse de conhecimento da solução de Gestão de Vulnerabilidades.	1		
2.	Solução de *Breach and Attack Simulation* – BAS	1		
2.1	Implementação da solução de *Breach and Attack Simulation* – BAS.	1		
2.2	Repasse de conhecimento da solução de Breach and Attack Simulation – BAS.	1		
3.	Solução de Inteligência Cibernética – OSINT	1		
3.1	Implementação da solução de Inteligência Cibernética – OSINT.	1		
3.2	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT.	1		

4.2. As notas fiscais (NFe/DANFE) deverão ser preenchidas com os dados da CONTRATANTE informados a seguir:

Razão Social: ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO – POUPEX

CNPJ: 00.655.522/0001-21

Inscrição municipal ou CF/DF: 07.451.631/001-57

End.: Avenida Duque de Caxias, s/n.º, Parte A, Setor Militar Urbano – SMU

Cidade: Brasília/DF

CEP: 70630-902

4.3. A CONTRATANTE obriga-se a efetuar as retenções tributárias incidentes nos percentuais e alíquotas determinados por Leis e Decretos, para as quais a CONTRATADA deverá destacar na Nota Fiscal os respectivos valores das retenções cabíveis.

4.4. Não serão efetuados os recolhimentos referentes ao IRPJ, CSLL, PIS e COFINS, quando a Declaração de Optante pelo SIMPLES Nacional for apresentada junto com a Nota Fiscal. Neste caso, o documento original da Declaração deverá ser enviado pelos Correios para o endereço do item 4.2.

4.5. Para que o pagamento seja realizado por meio de depósito bancário, as informações abaixo devem estar atualizadas, vinculadas ao CNPJ da CONTRATADA, ou de alguma de suas filiais, desde que devidamente registrado na nota fiscal.

Nome do Favorecido – (RAZÃO SOCIAL DA CONTRATADA)

CNPJ – 00.000.000/0000-00

Número do Banco - 000

Nome do Banco - BANCO FULANO S/A

Número da Agência Bancária – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Número da Conta Corrente – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Modalidade de Conta – CONTA CORRENTE/CONTA POUPANÇA

Chave PIX – (INFORMAR)

4.6. Na impossibilidade de o pagamento ser realizado em conta corrente, poderá ser emitido Boleto Bancário pela CONTRATADA, fazendo-se referência à nota fiscal emitida.

4.7. O pagamento será liquidado em até 10 (dez) dias úteis após a entrada da nota fiscal na Gerência de Compras e Contratos (GECOC), desde que o serviço esteja devidamente prestado.

4.7.1. A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas Notas Fiscais nesse prazo, essas deverão ser emitidas com data do 1º (primeiro) dia do mês subsequente.

4.7.2. Todos os campos da nota fiscal deverão ser corretamente preenchidos, sem exceção, sob pena de devolução da Nota. A nota fiscal emitida com irregularidades (rasuras, dados incompletos, vencimento em desacordo, etc.) será devolvida com as informações que motivaram a rejeição para nova emissão, e será iniciada a contagem de novo prazo para pagamento após as correções pertinentes.

4.8. O custo das tarifas bancárias deverá ser suportado pela CONTRATADA nos casos em que os dados bancários informados estejam em desacordo com o CNPJ da CONTRATADA, ou que apresentem alguma inconsistência que motivaram a rejeição do pagamento.

4.9. Será considerada inválida qualquer forma de cobrança realizada em desacordo com o previsto nesta cláusula.

4.10. O não pagamento de quaisquer valores devidos pela CONTRATANTE no prazo acima mencionado implicará a incidência dos seguintes encargos moratórios, até a data do efetivo pagamento:

4.10.1. Juros de mora de 1% (um por cento) ao mês, calculados “pro rata die”; e

4.10.2. Multa de 2% (dois por cento) sobre o parcelamento em atraso.

5. PRAZO

5.1. O prazo para a execução dos serviços será de 12 (doze) meses, contados a partir da data de assinatura deste contrato, podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 120 (cento e vinte) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea:

5.1.1. que os serviços tenham sido prestados regularmente e satisfatoriamente;

5.1.2. a CONTRATADA não tenha sofrido qualquer punição de natureza pecuniária;

5.1.3. a CONTRATANTE ainda tenha interesse na realização do serviço;

5.1.4. o valor do contrato permaneça economicamente vantajoso para a CONTRATANTE; e

5.1.5. a CONTRATADA concorde com a prorrogação do contrato.

5.2. A CONTRATADA deverá, ainda, cumprir os seguintes prazos:

Item	Descrição	Prazo
1.	Assinatura do instrumento contratual	Em até 5 (cinco) dias úteis após aprovação da fase de validação
2.	Apresentação de plano de implementação e entrega da subscrição da solução de Gestão de Vulnerabilidades.	Em até 7 dias úteis, após a assinatura do contrato.
2.1	Implementação da solução de Gestão de Vulnerabilidades, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
2.2	Repasse de conhecimento da solução de Gestão de Vulnerabilidades, se necessário.	Em até 7 dias úteis, após a implementação da solução.
3.	Apresentação de plano de implementação e entrega da subscrição da solução de *Breach and Attack Simulation* –BAS.	Em até 7 dias úteis, após a assinatura do contrato.
3.1	Implementação da solução de *Breach and Attack Simulation* – BAS, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
3.2	Repasse de conhecimento da solução de *Breach and Attack Simulation* – BAS, se necessário.	Em até 7 dias úteis, após a implementação da solução.
4.	Apresentação de plano de implementação e entrega da subscrição da solução de Inteligência Cibernética – OSINT.	Em até 7 dias úteis, após a assinatura do contrato.
4.1	Implementação da solução de Inteligência Cibernética – OSINT, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
4.2	Repasse de conhecimento da solução de Inteligência Cibernética – OSINT, se necessário.	Em até 7 dias úteis, após a implementação da solução.

6. RECEBIMENTO DOS SERVIÇOS E EMISSÃO DO TERMO DE ACEITAÇÃO DOS SERVIÇOS

6.1. O recebimento dos serviços com a consequente emissão do Termo de Aceitação dos Serviços está condicionado ao atendimento, quando for o caso:

6.1.1. dos prazos de entrega previstos no item 5.2.;

6.1.2. da implementação com todas as soluções operacionais. A validação técnica pela CONTRATANTE se dará com base em testes de funcionamento e checklist de entrega, e

6.1.3. do repasse de conhecimento à equipe da CONTRATANTE, com a execução de 100% das ações previstas no plano e entrega dos materiais de apoio.

6.2. A aferição ocorrerá com base no acompanhamento e validação realizados pela CONTRATANTE, mediante relatórios de acompanhamento apresentados pela CONTRATADA.

7. REAJUSTE

7.1. O valor pactuado da cláusula 4ª poderá ser reajustado após 12 (doze) meses da assinatura deste contrato, após solicitação da CONTRATADA, mediante negociação entre as partes, tendo como limite máximo a variação do Índice Nacional de Preços ao Consumidor Amplo (IPCA/IBGE) ocorrida nos últimos 12 (doze) meses, a contar da data da apresentação da proposta ou do último reajuste.

7.2. No caso da extinção ou não divulgação do índice IPCA/IBGE, o valor será reajustado com outro índice equivalente, que melhor se ajuste ao objeto do contrato, ou ainda, por acordo entre as partes.

7.3. A CONTRATADA, ao realizar a solicitação de reajuste, deverá encaminhar a memória de cálculo, com base no índice utilizado no item 7.1

7.4. O reajuste deverá ser solicitado antes do término da atual vigência do contrato, sob pena de preclusão.

8. OBRIGAÇÕES DA CONTRATADA

8.1. São obrigações da CONTRATADA:

8.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

8.1.2. auxiliar a equipe técnica da CONTRATANTE na implementação do plano de ação, fornecendo orientações e suporte técnico necessário para garantir o funcionamento adequado da solução;

8.1.3. a CONTRATADA não poderá realizar alterações nos ambientes computacionais preexistentes da CONTRATANTE, salvo mediante autorização formal e prévia, respeitando os limites definidos pela área técnica.

8.1.4. realizar todos os procedimentos e as demais atividades relativas ao objeto contratado por meio de equipe técnica especializada e devidamente qualificada, necessária à completa e perfeita execução do objeto contratado, em conformidade com a especificação técnica e melhores práticas;

8.1.5. manter a confidencialidade e a segurança dos documentos durante todo o processo;

8.1.6. comunicar por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários;

8.1.7. alertar seus prepostos, empregados e/ou prestadores de serviços acerca da boa conduta, principalmente, no tocante à disciplina e discrição quando da execução de suas tarefas;

8.1.8. garantir o ambiente de segurança necessário em atendimento à Lei Geral de Proteção de Dados (LGPD);

8.1.9. prestar os serviços com zelo e desempenho necessário à execução dos serviços;

8.1.10. comunicar imediatamente a CONTRANTANTE qualquer irregularidade na prestação dos serviços;

8.1.11. propiciar os meios e facilidades necessárias à fiscalização dos serviços, observando as penalidades cabíveis;

8.1.12. refazer, sem ônus para a CONTRATANTE, os serviços executados em desacordo com as características e especificações exigidas neste contrato e constantes da Proposta Comercial da CONTRATADA;

8.1.13. atender as exigências previstas na Circular BACEN n.º 3.978 – (PLD/FT), que dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016;

8.1.14. não designar, para a prestação dos serviços objeto deste contrato, familiar de dirigente ou de empregado da CONTRATANTE ou da Fundação Habitacional do Exército – FHE;

8.1.14.1. considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

8.1.15. não transferir, por qualquer forma, os direitos e obrigações que o presente contrato lhe atribui, salvo com a expressa anuência da CONTRATANTE, manifestada por escrito e por quem detenha poderes para tanto;

8.1.16. não se pronunciar em nome da CONTRATANTE, inclusive junto a órgãos de imprensa, sobre nenhum assunto relativo à sua atividade, guardar sigilo absoluto quanto a toda informação obtida da CONTRATANTE em decorrência do presente contrato, bem como não divulgar ou reproduzir nenhum documento, instrumentos normativos e materiais encaminhados pela CONTRATANTE;

8.1.17. não utilizar o nome da CONTRATANTE, ou sua qualidade de prestadora de serviços, em qualquer forma de divulgação de suas atividades, tais como cartões de visita, anúncios, impressos ou qualquer outro tipo de propaganda;

8.1.18. ressarcir toda e qualquer quantia que for efetivamente paga pela CONTRATANTE, em decorrência do ato ou fato culposo e/ou doloso dos empregados, prestadores de serviços e/ou prepostos da CONTRATADA;

8.1.19. pagar todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços objeto do contrato. Fica, desde logo, convencionado que a CONTRATANTE poderá descontar, de qualquer

crédito da CONTRATADA, a importância correspondente a eventuais pagamentos dessa natureza, que venha a efetuar por imposição legal;

8.1.20. apresentar, quando solicitado pela CONTRATANTE cópia de todo e qualquer documento que ateste a regularidade da CONTRATADA;

8.1.21. cumprir todas as leis e instrumentos normativos reguladores da sua atividade empresarial, bem como satisfazer, às suas próprias expensas, todas e quaisquer exigências legais decorrentes da execução do presente contrato; e

8.1.22. assumir responsabilidade pelos danos diretos provocados à CONTRATANTE, decorrente de atos comissivos e omissivos, praticados por seus sócios, associados, integrantes não sócios, empregados, representantes, prestadores de serviços e prepostos, durante a execução do contrato. Os danos causados à CONTRATANTE serão suportados pela CONTRATADA, até o limite equivalente a 50% (cinquenta por cento) dos últimos 6 (seis) pagamentos realizados pela CONTRATANTE à CONTRATADA. Nenhuma das partes responderá por lucros cessantes, danos morais ou quaisquer danos indiretos.

8.2. A CONTRATADA é, para todos os fins e efeitos jurídicos, única e exclusiva responsável por seus empregados, prepostos e/ou prestadores de serviços, afastando a CONTRATANTE, em todas as hipóteses, de qualquer responsabilidade fiscal, trabalhista, comercial, civil, penal, administrativa e previdenciária pelos contratos firmados pela CONTRATADA. Desde já, a CONTRATADA e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se a excluir a CONTRATANTE de toda demanda judicial promovida por seu empregado, preposto e/ou seu contratado para prestação de serviços objeto deste contrato, isentando a CONTRATANTE de todo e qualquer ônus, responsabilidade e/ou vínculo para com esses.

8.2.1. Caso seja mantida a presença da CONTRATANTE em eventuais reclamações trabalhistas ou quaisquer outras ações, administrativas ou judiciais, que tenham como fundamento matérias reguladas na legislação já referida, a CONTRATADA, seus sócios e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se, desde logo e sem qualquer discussão, a ressarcir a CONTRATANTE de todos os valores despendidos e de adiantar pagamentos a serem efetuados em razão de eventuais condenações, no prazo de 24 (vinte e quatro) horas, contados da solicitação nesse sentido, sob pena de multa de 10% (dez por cento) sobre o valor da condenação ou do valor efetivamente pago, em conformidade com o art. 408 do Código Civil.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. São obrigações da CONTRATANTE:

9.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

9.1.2. acompanhar e fiscalizar a execução do serviço contratado;

9.1.3. fornecer a infraestrutura, os dados e as informações necessárias para o funcionamento e parametrização da solução, além da equipe técnica para acompanhamento das atividades;

9.1.4. disponibilizar os acessos necessários às informações da CONTRATANTE, desde que atenda os critérios de segurança estipulados pela CONTRATANTE;

9.1.5. permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, caso necessário, o acesso remoto da CONTRATANTE, respeitadas as normas de segurança vigentes;

9.1.6. receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita;

9.1.7. notificar a CONTRATADA, por escrito, sobre ou a respeito de quaisquer irregularidades encontradas nas execuções de serviços fixando-lhe prazos para as correções;

9.1.8. proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços dentro das condições estabelecidas neste contrato;

9.1.9. efetuar os pagamentos de sua responsabilidade nas datas previstas, desde que cumpridos todos os procedimentos administrativos de responsabilidade da CONTRATADA.

10. DA RESPONSABILIDADE SOCIAL E AMBIENTAL

10.1. Em cumprimento às diretrizes da Política de Responsabilidade Socioambiental da CONTRATANTE, a CONTRATADA se compromete a:

10.1.1. não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal na execução de suas atividades, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

10.1.2. não empregar menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre, e nem menores de 16 (dezesseis) anos, salvo na condição de jovem aprendiz;

10.1.3. não permitir a prática ou a manutenção de atos discriminatórios que limitem o acesso a relação de emprego, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.4. buscar prevenir e erradicar práticas danosas ao meio ambiente, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos à produção, consumo e destinação dos resíduos sólidos de maneira sustentável, implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.5. comprovada a não observância dos preceitos acima, a CONTRATANTE notificará a CONTRATADA para a respectiva regularização. O não atendimento da notificação sujeitará a CONTRATADA às penalidades previstas contratualmente e, até mesmo, impossibilitar a renovação do pacto sem prejuízo das cominações legais.

11. DA PROTEÇÃO DOS DADOS E DAS INFORMAÇÕES DA CONTRATANTE E DE TERCEIROS

11.1. As partes se comprometem a tratar os dados pessoais a que tiveram acesso em decorrência do presente contrato, exclusivamente para cumprir com a finalidade a que se destina seu tratamento e em respeito a toda a legislação aplicável sobre segurança da informação, privacidade e proteção de dados pessoais, inclusive, a Lei Federal nº. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais ("LGPD"), sem exclusão das demais normas setoriais ou gerais sobre os temas, sob pena de incorrer na obrigação de indenizar a parte inocente e terceiros porventura impactados, pelas perdas e danos, nos termos da lei, suportando as consequências do referido descumprimento.

11.2. Na suspeita ou ocorrência de qualquer acesso não autorizado, divulgação indevida, exposição indesejada e/ou situação acidental ou intencional de destruição, deleção, perda, alteração ("Incidente") que envolva os Dados Pessoais tratados em razão deste Contrato, a Parte que tomou ciência do evento deverá comunicar a outra Parte dentro do prazo de 48 (quarenta e oito) horas, trazendo no mínimo as informações exigidas no art. 48, § 1º da LGPD, além de outras que porventura forem solicitadas e que possibilitem a condução de investigação e perícia forense relacionada ao Incidente.

12. CONFIDENCIALIDADE

12.1. A CONTRATADA obriga-se a manter o sigilo sobre as informações fornecidas ou obtidas junto à CONTRATANTE, sejam estas classificadas como "informações confidenciais", ou não, abrangendo inclusive informações cadastrais, comerciais ou outras obtidas em decorrência da presente contratação, que são de propriedade exclusiva da CONTRATANTE, respondendo a CONTRATADA pelo pagamento das perdas e danos apurados em processo próprio, quando ocorrer a violação ou a divulgação das mesmas, inclusive por atos de seus empregados, prepostos, prestadores de serviços ou terceiros que as obtiverem junto à CONTRATADA.

12.1.1. O referido sigilo se estende mesmo após o término do compromisso contratual, por tempo indeterminado.

12.1.2. A CONTRATANTE tornará disponível à CONTRATADA as informações públicas e não-públicas sobre suas contas, bens, propriedades, direitos, obrigações, negócios e operações, além de outras, doravante referidas, em conjunto, como as "INFORMAÇÕES".

12.1.3. Serão consideradas como informações públicas aquelas de caráter oficial que forem publicamente divulgadas pela CONTRATANTE.

12.2. As Partes se obrigam, por si, suas controladas, coligadas, seus empregados, administradores, prepostos, terceiros de sua confiança e por seus representantes legais a:

12.2.1. manter confidencialidade sobre todas as INFORMAÇÕES e a não as transmitir nem as revelar a terceiros;

12.2.2. não discutir, perante terceiros, nem usar, divulgar, revelar ou dispor das INFORMAÇÕES para outra finalidade que não aquelas relacionadas à avaliação de seus interesses recíprocos em negociar com a outra parte, cumprindo-lhes adotar cautelas e precauções adequadas no sentido de impedir o uso indevido das INFORMAÇÕES por qualquer pessoa que a estas venha a ter acesso; e

12.2.3. guardar e manter confidencialidade sobre todas as cópias, reproduções, sumários, análises ou comunicados referentes às INFORMAÇÕES ou nestas baseadas, devendo devolvê-los à CONTRATANTE, quando solicitado.

12.3. A parte que estiver recebendo as INFORMAÇÕES ou qualquer outro dado referente às atividades desenvolvidas pela outra parte se obriga e se compromete a protegê-los, a fim de que não sejam revelados a terceiros não autorizados. Todavia, essa obrigação não se aplica às INFORMAÇÕES e/ou dados que:

12.3.1. já forem do domínio público à época em que tiverem sido revelados;

12.3.2. passarem a ser de domínio público, após sua revelação, sem que a divulgação seja efetuada em violação ao disposto neste Acordo;

12.3.3. já forem notoriamente do conhecimento da parte recipiente antes de lhe terem sido revelados; ou

12.3.4. forem legalmente revelados à parte recipiente por terceiros que não os tiverem recebido sob a vigência de uma obrigação de confidencialidade.

13. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

13.1. Em cumprimento às diretrizes contidas na ISO/IEC 27001, ISO/IEC 27035 e LGPD, a CONTRATADA compromete-se em estabelecer, implementar, manter e aprimorar continuamente um sistema de gestão de segurança da informação (SGSI), mas não se limitando à:

13.1.1. apresentar Plano de Gestão de Incidentes de Segurança da Informação para conhecimento e análise da CONTRATANTE;

13.1.2. possuir e manter processo estruturado de Gestão de Incidentes de Segurança da Informação, conforme ISO/IEC 27001 e ISO/IEC 27035;

13.1.3. permitir auditoria ou verificação de conformidade durante a vigência do contrato pela CONTRATANTE;

13.1.4. definir prazos e formas de comunicação de incidentes, incluindo:

a) canal de comunicação;

b) notificação imediata (até 1h após a detecção);

c) comunicação de incidentes com impacto relevante (ex.: vazamento de dados); e

d) obrigatoriedade de investigação e relatório de lições aprendidas.

13.2. Sanções contratuais em caso de falhas graves ou reincidentes na gestão de incidentes.

14. FISCALIZAÇÃO E GESTÃO DO CONTRATO

14.1. A execução do contrato será acompanhada e fiscalizada pelos seguintes representantes, abaixo CREDENCIADOS:

CONTRATANTE
Gestor do contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
Fiscal do Contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
CONTRATADA
Preposto:
Nome: XXXXXXX –Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX
Responsável Técnico:
Nome: XXXXXXX –Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX

14.2. As alterações dos representantes acima nomeados como Gestor, Fiscais, Preposto e Responsável Técnico, poderão ser realizadas por meio de simples APOSTILAMENTO, sendo estabelecido novo CREDENCIAMENTO.

14.3. O representante da CONTRATANTE denominado Gestor do Contrato, atuará com o apoio dos Fiscais do Contrato, credenciados neste instrumento.

14.4. O Gestor, juntamente com os Fiscais, deverá acompanhar a prestação dos serviços, registrar as ocorrências e determinar as medidas necessárias ao fiel cumprimento do contrato, bem como atestar, no todo ou em parte, a realização dos serviços objeto deste contrato.

14.5. O atesto dos serviços prestados pela CONTRATANTE para pagamento da nota fiscal não exime a plena responsabilidade da CONTRATADA em garantir o cumprimento total e satisfatório do contrato em conformidade com as especificações estabelecidas quando da contratação.

14.6. O descumprimento total ou parcial das responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste contrato.

15. ALTERAÇÕES CONTRATUAIS

15.1. As alterações das obrigações estabelecidas neste contrato deverão ser formalizadas por meio da lavratura de Termo Aditivo, mediante acordo entre as partes, e em conformidade com os preços e condições vigentes.

15.2. Na hipótese de alteração das condições econômicas fundamentais prevalecentes na assinatura deste contrato, as partes ajustarão as cláusulas que assegurarão a recuperação dos valores ora contratados, objetivando a manutenção do equilíbrio econômico-financeiro do contrato.

15.3. A CONTRATADA deverá comunicar à CONTRATANTE quaisquer alterações em seu Contrato Social, razão ou denominação social, objeto, CNPJ e outros e ainda seus dados bancários, endereços, telefones, fax, e demais dados que, porventura, venham interferir na alteração da habilitação e qualificação exigidas para a execução das obrigações contratuais.

16. DO REEQUILÍBRIO CONTRATUAL

16.1. Na hipótese de ocorrência de fatos supervenientes que alterem substancialmente os encargos pactuados, inclusive em decorrência de modificações na legislação tributária que impactem direta ou indiretamente os custos da execução contratual, será assegurado o direito à revisão contratual, mediante requerimento fundamentado e comprovação do desequilíbrio.

16.2. O pedido de revisão deverá ser formalizado durante a vigência do contrato e será decidido pela FHE no prazo de até 90 (noventa) dias, prorrogável por igual período, conforme previsto na legislação aplicável, acompanhados de toda a documentação comprobatória pertinente, que demonstrem de forma clara e inequívoca, incluindo:

16.2.1. O fundamento legal que deu origem ao pleito;

16.2.2. O demonstrativo econômico-financeiro do impacto direto e quantificável das alterações fáticas e/ou normativas na estrutura de custos e/ou receitas do Contrato;

16.2.3. Apresentação de valores e percentuais que justifiquem a necessidade de revisão contratual;

16.2.4. O período em que o impacto se torna mensurável e efetivo.

16.3. Qualquer alteração no Contrato decorrente do reequilíbrio econômico-financeiro deverá ser formalizada por meio de Termo Aditivo, devidamente assinado pelas Partes.

16.4. O pleito de reequilíbrio e as negociações subsequentes não suspenderão a execução do Contrato, que deverá prosseguir em seus termos originais até que o Termo Aditivo de reequilíbrio seja formalizado ou a controvérsia seja definitivamente resolvida.

16.5. A FHE poderá, de ofício, promover a revisão contratual nos casos em que se verificar redução da carga tributária, desde que garantido o contraditório e a ampla defesa.

16.6. A revisão poderá resultar em: a) Reajuste dos valores contratados; b) Alteração de prazos ou condições de execução; c) Outras medidas compensatórias que restabeleçam o equilíbrio econômico-financeiro.

17. RESILIÇÃO DO CONTRATO

17.1. Independentemente de justificativa e sem que caiba qualquer indenização à outra parte, este contrato poderá ser denunciado a qualquer tempo, pela CONTRATANTE ou pela CONTRATADA, mediante comunicação feita por escrito e com antecedência mínima de 30 (trinta) dias.

18. PENALIDADES

18.1. O inadimplemento total ou parcial das obrigações contratuais dá, à CONTRATANTE, o direito de aplicar as seguintes penalidades:

18.1.1. advertência, quando constatadas pequenas irregularidades que não cause grave dano à CONTRATANTE;

18.1.2. multa, que poderá ser aplicada por descumprimento de quaisquer das obrigações contratuais, calculada em percentual de 0,5% a 30% sobre o valor total do contrato, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, ou descontada das parcelas devidas à CONTRATADA, sem prejuízo de outras sanções previstas contratualmente;

18.1.3. resolução unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais;

18.1.4. os casos de descumprimento das entregas mínimas aceitáveis, serão enquadrados como inexecução parcial do instrumento contratual.

18.1.5. em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico.

18.1.6. as multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

18.1.7. não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

18.1.8. sendo resolvido o presente contrato, o pagamento devido será proporcional aos serviços prestados até a data da resolução.

18.1.9. para se ressarcir de eventuais prejuízos causados pela CONTRATADA e do valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar esses valores dos créditos decorrentes deste mesmo contrato ou de outros contratos que a CONTRATADA possua com a CONTRATANTE.

18.1.10. caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA.

18.1.11. no processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

19. VIGÊNCIA

19.1. O presente contrato terá vigência desde a data de sua assinatura e vigorará até ___ de _____ de 20__.

20. CONDIÇÕES GERAIS

20.1. Este contrato e a Proposta Técnica e Comercial constituem a totalidade do acordo entre os signatários com relação às matérias aqui previstas e superam, substituem e revogam os entendimentos, negociações e acordos anteriores.

20.2. Em caso de divergências entre a proposta da CONTRATADA e este instrumento fica desde já acordado que prevalecerão as condições estabelecidas neste contrato.

20.3. Não valerá como precedente, novação, ou renúncia aos direitos que a lei e o presente instrumento asseguram a CONTRATANTE, sua tolerância a eventuais descumprimentos de cláusulas, seus itens e subitens, pela CONTRATADA.

21. FORO

21.1. As partes elegem o Foro da Circunscrição Judiciária de Brasília para dirimir quaisquer questões oriundas do presente contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

Nos termos do disposto no art. 107 do Código Civil; art. 3º, da Lei nº 13.874, de 2019; e Decreto nº 10.278, de 2020, as partes e testemunhas, quando for o caso, declaram a autoria, integridade e confiabilidade deste contrato, acordando, assim, em não contestar a sua validade, conteúdo e autenticidade. E, por estarem justos e acertados, as partes concordam que o presente instrumento contratual será assinado digitalmente, bem como os demais documentos correlatos, sendo as assinaturas válidas, vinculantes e executáveis. Admite-se qualquer modalidade de assinatura eletrônica prevista em lei, quando a integridade dessas for conferida por provedor de assinatura, nos termos da Lei nº 14.620, de 2023.

Brasília-DF, de de 2025.

CONTRATANTE	CONTRATADA

TESTEMUNHAS:

Nome:	Nome:

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ____/2025 - POUPEX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE SOLUÇÕES DE SEGURANÇA CIBERNÉTICA FIRMADO ENTRE A POUPEX E A _____.

A **ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO - POUPEX**, sediada na Av. Duque de Caxias s/n.º, Parte A, Setor Militar Urbano - SMU, Brasília/DF, CEP 70630-902, inscrita no CNPJ nº 00.655.522/0001-21, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) (cargo) _____, na forma autorizada por (documento) _____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado(a) em _____, doravante denominada **CONTRATANTE**, e a **(razão social – nome fantasia)** _____, sediada no endereço _____, CEP _____, inscrita no CNPJ nº _____, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) _____ (cargo), conforme (documento - contrato social, procuração)_____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado (a) em _____, doravante denominada **CONTRATADA**, têm justo e avençado o presente contrato de prestação de serviços, conforme Proposta Técnica e Comercial de Preço de ____/____/_____ e Especificação Técnica, de ___/____/____, partes integrantes deste instrumento, regido pelas cláusulas seguintes e pelas normas de Direito Privado:

1. OBJETO

1.1. O objeto do presente contrato consiste na contratação de empresa especializada para soluções de segurança cibernética visando à proteção contínua dos ativos informacionais da CONTRATANTE, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação, contendo os seguintes itens:

Tabela 1

Item	Descrição	Qtd.
1.	Solução de Cofre de Senha e Gestão de Altas Credenciais – PAM (deve vir com o suporte técnico do fabricante incluso)	500
1.1	Implementação da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1
1.2	Repasse de conhecimento da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM	1

2. CONDIÇÕES PARA EXECUÇÃO DOS SERVIÇOS

2.1. A CONTRATADA realizará todas as atividades, preferencialmente, no horário comercial, de segunda a sexta-feira exceto feriados, das 8h às 18h.

2.2. A entrega da(s) solução(ões) será(ão) realizada(s) de forma digital, por meio de disponibilização remota dos *softwares* e respectivos componentes.

2.3. A execução dos serviços de implementação e repasse de conhecimento, se necessário, deverá ocorrer de forma remota.

2.4. As soluções de segurança deverão ser fornecidas por meio de licenciamento anual, contemplando todos os componentes necessários para sua plena operação, incluindo *software*, atualizações, suporte técnico e documentação. O modelo de fornecimento será tradicional, com licenças válidas por 12 meses, renováveis conforme a necessidade da CONTRATANTE, garantindo o funcionamento integral das funcionalidades contratadas durante todo o período de vigência.

2.5. A solução deverá oferecer acesso contínuo a atualizações de segurança, correções de vulnerabilidades, melhorias de desempenho e novas funcionalidades disponibilizadas pelo fabricante, sem custos adicionais durante o período de licenciamento.

2.6. A CONTRATADA será responsável por fornecer os meios necessários para ativação, instalação e configuração inicial da solução, além de disponibilizar manuais, guias técnicos e acesso à base de conhecimento. A solução deverá ser compatível com o ambiente tecnológico da CONTRATANTE e permitir integração com outras ferramentas de segurança já existentes, quando aplicável.

2.7. A efetividade da solução será avaliada por meio de relatórios técnicos, indicadores de desempenho e evidências de funcionamento, conforme critérios definidos pela área técnica da CONTRATANTE.

2.8. Descrição das soluções:

2.8.1. **Solução de cofre de senha e gestão de altas credenciais (PAM)**: plataforma que protege, controla e audita o uso de credenciais privilegiadas em ambientes corporativos. Armazena senhas de forma segura em cofres criptografados, automatiza a rotação de credenciais e aplica políticas de acesso baseado em risco e necessidade. Reduz a superfície de ataque, evita uso indevido de contas administrativas e garante conformidade com normas como ISO 27001, LGPD e NIST.

2.9. Serviços de implementação: a CONTRATADA será responsável pela instalação, configuração e validação inicial da solução, garantindo sua plena operação conforme os requisitos técnicos definidos pela CONTRATANTE.

2.10. Repasse de Conhecimento**:** serão realizadas atividades de repasse de conhecimento técnico às equipes da CONTRATANTE, com foco na solução implementada, visando assegurar o entendimento aprofundado de sua arquitetura, funcionalidades e procedimentos operacionais. Esse processo tem como objetivo promover autonomia na gestão e manutenção da solução. O repasse de conhecimento poderá ser disponibilizado também sob demanda, por meio de acesso a plataformas especializadas oferecidas pelo fabricante, proporcionando maior flexibilidade e continuidade no processo de assimilação técnica.

2.11. Suporte Técnico: o suporte técnico deverá estar incluso no licenciamento e prestado exclusivamente pelo fabricante da solução, assegurando domínio completo da tecnologia ofertada e maior eficiência na identificação e resolução de incidentes. O serviço deverá estar disponível em regime 24x7, com atendimento remoto e escalonamento conforme a criticidade dos chamados, assegurando a continuidade operacional da solução durante todo o período de vigência do contrato.

2.12. Acordo de Nível de Serviço para Chamados de Suporte Técnico: o suporte técnico será prestado diretamente pelo fabricante da solução mediante abertura de chamado por parte da CONTRATANTE e o Acordo de Nível de Serviço – ANS obedecerá ao descrito na plataforma do fabricante, sendo obrigatoriamente na modalidade de 24 x 7 para resolução de incidentes e demandas.

2.12.1. será dado início a abertura do chamado para o suporte técnico através dos canais: e-mail (_____) ou telefone (_____) para a centralização dos chamados e controles de SLA.

2.13. A CONTRATANTE e a CONTRATADA são pessoas jurídicas totalmente distintas e independentes, não configurando este contrato nenhuma forma de sociedade, pelo que os profissionais terceirizados, designados pela CONTRATADA para a prestação dos serviços objeto deste contrato, atuarão sem qualquer subordinação laboral à CONTRATANTE e, portanto, inexistente vínculo ou relação de trabalho com a CONTRATANTE.

3. PREÇO

3.1. O valor total deste contrato é de R$ _____ (_____).

3.2. As despesas decorrentes deste contrato correrão por conta dos recursos próprios da POUPEX, consignados na conta orçamentária. Centro de custo: _____. Conta contábil/orçamentaria _____.

3.3. Nos preços fixados nesta cláusula estão compreendidos todos os custos e despesas que, direta ou indiretamente, decorram do cumprimento pleno e integral do objeto deste contrato, tais como e sem se limitar a: telefone, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, softwares, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

4. FORMA E CONDIÇÕES DE PAGAMENTO

4.1. A CONTRATANTE pagará à CONTRATADA, conforme quadro abaixo, pela prestação dos serviços objeto deste contrato, após a conclusão dos serviços, mediante a emissão do Termo de Recebimento, Aceitação dos Serviços e atesto na nota fiscal a ser apresentada com 10 (dez) dias de antecedência do vencimento:

Item	Descrição	Qtd	Valor Unitário (R$)	Valor Total (R$)
1.	Solução de Cofre de Senha e Gestão de Altas Credenciais – PAM	1		
1.1	Implementação da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1		
1.2	Repasse de conhecimento da solução de Cofre de Senha e Gestão de Altas Credenciais – PAM.	1		

4.2. As notas fiscais (NFe/DANFE) deverão ser preenchidas com os dados da CONTRATANTE informados a seguir:

Razão Social: ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO – POUPEX

CNPJ: 00.655.522/0001-21

Inscrição municipal ou CF/DF: 07.451.631/001-57

End.: Avenida Duque de Caxias, s/n.º, Parte A, Setor Militar Urbano – SMU

Cidade: Brasília/DF

CEP: 70630-902

4.3. A CONTRATANTE obriga-se a efetuar as retenções tributárias incidentes nos percentuais e alíquotas determinados por Leis e Decretos, para as quais a CONTRATADA deverá destacar na nota fiscal os respectivos valores das retenções cabíveis.

4.4. Não serão efetuados os recolhimentos referentes ao IRPJ, CSLL, PIS e COFINS, quando a Declaração de Optante pelo SIMPLES Nacional for apresentada junto com a nota fiscal. Neste caso, o documento original da Declaração deverá ser enviado pelos Correios para o endereço do item 4.2.

4.5. Para que o pagamento seja realizado por meio de depósito bancário, as informações abaixo devem estar atualizadas, vinculadas ao CNPJ da CONTRATADA, ou de alguma de suas filiais, desde que devidamente registrado na nota fiscal.

Nome do Favorecido – (RAZÃO SOCIAL DA CONTRATADA)

CNPJ – 00.000.000/0000-00

Número do Banco - 000

Nome do Banco - BANCO FULANO S/A

Número da Agência Bancária – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Número da Conta Corrente – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Modalidade de Conta – CONTA CORRENTE/CONTA POUPANÇA

Chave PIX – (INFORMAR)

4.6. Na impossibilidade de o pagamento ser realizado em conta corrente, poderá ser emitido Boleto Bancário pela CONTRATADA, fazendo-se referência à nota fiscal emitida.

4.7. O pagamento será liquidado em até 10 (dez) dias úteis após a entrada da nota fiscal na Gerência de Compras e Contratos (GECOC), desde que o serviço esteja devidamente prestado.

4.7.1. A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela

CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas notas fiscais nesse prazo, essas deverão ser emitidas com data do 1º (primeiro) dia do mês subsequente.

4.7.2. Todos os campos da nota fiscal deverão ser corretamente preenchidos, sem exceção, sob pena de devolução da Nota. A nota fiscal emitida com irregularidades (rasuras, dados incompletos, vencimento em desacordo, etc.) será devolvida com as informações que motivaram a rejeição para nova emissão, e será iniciada a contagem de novo prazo para pagamento após as correções pertinentes.

4.8. O custo das tarifas bancárias deverá ser suportado pela CONTRATADA nos casos em que os dados bancários informados estejam em desacordo com o CNPJ da CONTRATADA, ou que apresentem alguma inconsistência que motivaram a rejeição do pagamento.

4.9. Será considerada inválida qualquer forma de cobrança realizada em desacordo com o previsto nesta cláusula.

4.10. O não pagamento de quaisquer valores devidos pela CONTRATANTE no prazo acima mencionado implicará a incidência dos seguintes encargos moratórios, até a data do efetivo pagamento:

4.10.1. Juros de mora de 1% (um por cento) ao mês, calculados “pro rata die”; e

4.10.2. Multa de 2% (dois por cento) sobre o parcelamento em atraso.

5. PRAZO

5.1. O prazo para a execução dos serviços será de 12 (doze) meses, contados a partir da data de assinatura deste contrato, podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 120 (cento e vinte) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea:

5.1.1. que os serviços tenham sido prestados regularmente e satisfatoriamente;

5.1.2. a CONTRATADA não tenha sofrido qualquer punição de natureza pecuniária;

5.1.3. a CONTRATANTE ainda tenha interesse na realização do serviço;

5.1.4. o valor do contrato permaneça economicamente vantajoso para a CONTRATANTE; e

5.1.5. a CONTRATADA concorde com a prorrogação do contrato.

5.2. A CONTRATADA deverá, ainda, cumprir os seguintes prazos:

Item	Descrição	Prazo
1.	Assinatura do instrumento contratual	Em até 5 (cinco) dias úteis após aprovação da fase de validação
2.	Apresentação de plano de implementação e entrega da subscrição da solução Cofre de Senha e Gestão de Altas Credenciais – PAM.	Em até 7 dias úteis, após a assinatura do contrato.
2.1	Implementação da solução Cofre de Senha e Gestão de Altas Credenciais – PAM, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
2.2	Repasse de conhecimento da solução Cofre de Senha e Gestão de Altas Credenciais – PAM, se necessário.	Em até 7 dias úteis, após a implementação da solução.

6. RECEBIMENTO DOS SERVIÇOS E EMISSÃO DO TERMO DE ACEITAÇÃO DOS SERVIÇOS

6.1. O recebimento dos serviços com a consequente emissão do Termo de Aceitação dos Serviços está condicionado ao atendimento, quando for o caso:

6.1.1. dos prazos de entrega previstos no item 5.2.;

6.1.2. da implementação com todas as soluções operacionais. A validação técnica pela CONTRATANTE se dará com base em testes de funcionamento e checklist de entrega, e

6.1.3. do repasse de conhecimento à equipe da CONTRATANTE, com a execução de 100% das ações previstas no plano e entrega dos materiais de apoio.

6.2. A aferição ocorrerá com base no acompanhamento e validação realizados pela CONTRATANTE, mediante relatórios de acompanhamento apresentados pela CONTRATADA.

7. REAJUSTE

7.1. O valor pactuado da cláusula 4ª poderá ser reajustado após 12 (doze) meses da assinatura deste contrato, após solicitação da CONTRATADA, mediante negociação entre as partes, tendo como limite máximo a variação do Índice Nacional de Preços ao Consumidor Amplo (IPCA/IBGE) ocorrida nos últimos 12 (doze) meses, a contar da data da apresentação da proposta ou do último reajuste.

7.2. No caso da extinção ou não divulgação do índice IPCA/IBGE, o valor será reajustado com outro índice equivalente, que melhor se ajuste ao objeto do contrato, ou ainda, por acordo entre as partes.

7.3. A CONTRATADA, ao realizar a solicitação de reajuste, deverá encaminhar a memória de cálculo, com base no índice utilizado no item 7.1

7.4. O reajuste deverá ser solicitado antes do término da atual vigência do contrato, sob pena de preclusão.

8. OBRIGAÇÕES DA CONTRATADA

8.1. São obrigações da CONTRATADA:

8.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

8.1.2. auxiliar a equipe técnica da CONTRATANTE na implementação do plano de ação, fornecendo orientações e suporte técnico necessário para garantir o funcionamento adequado da solução;

8.1.3. a CONTRATADA não poderá realizar alterações nos ambientes computacionais preexistentes da CONTRATANTE, salvo mediante autorização formal e prévia, respeitando os limites definidos pela área técnica.

8.1.4. realizar todos os procedimentos e as demais atividades relativas ao objeto contratado por meio de equipe técnica especializada e devidamente qualificada, necessária à completa e perfeita execução do objeto contratado, em conformidade com a especificação técnica e melhores práticas;

8.1.5. manter a confidencialidade e a segurança dos documentos durante todo o processo;

8.1.6. comunicar por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários;

8.1.7. alertar seus prepostos, empregados e/ou prestadores de serviços acerca da boa conduta, principalmente, no tocante à disciplina e discrição quando da execução de suas tarefas;

8.1.8. garantir o ambiente de segurança necessário em atendimento à Lei Geral de Proteção de Dados (LGPD);

8.1.9. prestar os serviços com zelo e desempenho necessário à execução dos serviços;

8.1.10. comunicar imediatamente a CONTRANTANTE qualquer irregularidade na prestação dos serviços;

8.1.11. propiciar os meios e facilidades necessárias à fiscalização dos serviços, observando as penalidades cabíveis;

8.1.12. refazer, sem ônus para a CONTRATANTE, os serviços executados em desacordo com as características e especificações exigidas neste contrato e constantes da Proposta Comercial da CONTRATADA;

8.1.13. atender as exigências previstas na Circular BACEN n.º 3.978 – (PLD/FT), que dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens,

direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016;

8.1.14. não designar, para a prestação dos serviços objeto deste contrato, familiar de dirigente ou de empregado da CONTRATANTE ou da Fundação Habitacional do Exército – FHE;

8.1.14.1. considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

8.1.15. não transferir, por qualquer forma, os direitos e obrigações que o presente contrato lhe atribui, salvo com a expressa anuência da CONTRATANTE, manifestada por escrito e por quem detenha poderes para tanto;

8.1.16. não se pronunciar em nome da CONTRATANTE, inclusive junto a órgãos de imprensa, sobre nenhum assunto relativo à sua atividade, guardar sigilo absoluto quanto a toda informação obtida da CONTRATANTE em decorrência do presente contrato, bem como não divulgar ou reproduzir nenhum documento, instrumentos normativos e materiais encaminhados pela CONTRATANTE;

8.1.17. não utilizar o nome da CONTRATANTE, ou sua qualidade de prestadora de serviços, em qualquer forma de divulgação de suas atividades, tais como cartões de visita, anúncios, impressos ou qualquer outro tipo de propaganda;

8.1.18. ressarcir toda e qualquer quantia que for efetivamente paga pela CONTRATANTE, em decorrência do ato ou fato culposo e/ou doloso dos empregados, prestadores de serviços e/ou prepostos da CONTRATADA;

8.1.19. pagar todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços objeto do contrato. Fica, desde logo, convencionado que a CONTRATANTE poderá descontar, de qualquer crédito da CONTRATADA, a importância correspondente a eventuais pagamentos dessa natureza, que venha a efetuar por imposição legal;

8.1.20. apresentar, quando solicitado pela CONTRATANTE cópia de todo e qualquer documento que ateste a regularidade da CONTRATADA;

8.1.21. cumprir todas as leis e instrumentos normativos reguladores da sua atividade empresarial, bem como satisfazer, às suas próprias expensas, todas e quaisquer exigências legais decorrentes da execução do presente contrato; e

8.1.22. assumir responsabilidade pelos danos diretos provocados à CONTRATANTE, decorrente de atos comissivos e omissivos, praticados por seus sócios, associados, integrantes não sócios, empregados, representantes, prestadores de serviços e prepostos, durante a execução do contrato. Os danos causados à CONTRATANTE serão suportados pela CONTRATADA, até o limite equivalente a 50% (cinquenta por cento) dos últimos 6 (seis) pagamentos realizados pela CONTRATANTE à CONTRATADA. Nenhuma das partes responderá por lucros cessantes, danos morais ou quaisquer danos indiretos.

8.2. A CONTRATADA é, para todos os fins e efeitos jurídicos, única e exclusiva responsável por seus empregados, prepostos e/ou prestadores de serviços, afastando a CONTRATANTE, em todas as hipóteses, de qualquer responsabilidade fiscal, trabalhista, comercial, civil, penal, administrativa e previdenciária pelos contratos firmados pela CONTRATADA. Desde já, a CONTRATADA e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se a excluir a CONTRATANTE de toda demanda judicial promovida por seu empregado, preposto e/ou seu contratado para prestação de serviços objeto deste contrato, isentando a CONTRATANTE de todo e qualquer ônus, responsabilidade e/ou vínculo para com esses.

8.2.1. Caso seja mantida a presença da CONTRATANTE em eventuais reclamações trabalhistas ou quaisquer outras ações, administrativas ou judiciais, que tenham como fundamento matérias reguladas na legislação já referida, a CONTRATADA, seus sócios e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se, desde logo e sem qualquer discussão, a ressarcir a CONTRATANTE de todos os valores despendidos e de adiantar pagamentos a serem efetuados em razão de eventuais condenações, no prazo de 24 (vinte e quatro) horas, contados da solicitação nesse sentido, sob pena de multa de 10% (dez por cento) sobre o valor da condenação ou do valor efetivamente pago, em conformidade com o art. 408 do Código Civil.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. São obrigações da CONTRATANTE:

9.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

9.1.2. acompanhar e fiscalizar a execução do serviço contratado;

9.1.3. fornecer a infraestrutura, os dados e as informações necessárias para o funcionamento e parametrização da solução, além da equipe técnica para acompanhamento das atividades;

9.1.4. disponibilizar os acessos necessários às informações da CONTRATANTE, desde que atenda os critérios de segurança estipulados pela CONTRATANTE;

9.1.5. permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, caso necessário, o acesso remoto da CONTRATANTE, respeitadas as normas de segurança vigentes;

9.1.6. receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita;

9.1.7. notificar a CONTRATADA, por escrito, sobre ou a respeito de quaisquer irregularidades encontradas nas execuções de serviços fixando-lhe prazos para as correções;

9.1.8. proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços dentro das condições estabelecidas neste contrato;

9.1.9. efetuar os pagamentos de sua responsabilidade nas datas previstas, desde que cumpridos todos os procedimentos administrativos de responsabilidade da CONTRATADA.

10. DA RESPONSABILIDADE SOCIAL E AMBIENTAL

10.1. Em cumprimento às diretrizes da Política de Responsabilidade Socioambiental da CONTRATANTE, a CONTRATADA se compromete a:

10.1.1. não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal na execução de suas atividades, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

10.1.2. não empregar menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre, e nem menores de 16 (dezesseis) anos, salvo na condição de jovem aprendiz;

10.1.3. não permitir a prática ou a manutenção de atos discriminatórios que limitem o acesso a relação de emprego, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.4. buscar prevenir e erradicar práticas danosas ao meio ambiente, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos à produção, consumo e destinação dos resíduos sólidos de maneira sustentável, implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.5. comprovada a não observância dos preceitos acima, a CONTRATANTE notificará a CONTRATADA para a respectiva regularização. O não atendimento da notificação sujeitará a CONTRATADA às penalidades previstas contratualmente e, até mesmo, impossibilitar a renovação do pacto sem prejuízo das cominações legais.

11. DA PROTEÇÃO DOS DADOS E DAS INFORMAÇÕES DA CONTRATANTE E DE TERCEIROS

11.1. Para os fins deste contrato, os termos utilizados deverão ser interpretados conforme o disposto no art. 5º da Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, a CONTRATANTE atuará como CONTROLADORA dos dados pessoais eventualmente tratados no âmbito deste contrato, enquanto a CONTRATADA atuará como OPERADORA.

11.2. As partes se comprometem a tratar os dados pessoais a que tiveram acesso em decorrência do presente contrato, única e exclusivamente para cumprir com a finalidade a que se destina seu tratamento e em respeito a toda a legislação

aplicável sobre segurança da informação, privacidade e proteção de dados pessoais, inclusive, a LGPD, sem exclusão das demais normas setoriais ou gerais sobre os temas (Legislação Aplicável).

11.3. As partes deverão tratar os dados pessoais como informações confidenciais, responsabilizando-se por quem quer que venha acessá-los e garantindo que tais pessoas estejam sujeitas a idêntico dever de confidencialidade e a regras não menos rigorosas que aquelas estabelecidas neste contrato.

11.4. A OPERADORA se compromete a restringir o tratamento ao número mínimo de dados pessoais necessários ao atingimento das finalidades lícitas, específicas e informadas aos titulares, que sejam imprescindíveis à execução do objeto deste contrato.

11.5. Na hipótese de a OPERADORA considerar necessária a realização de qualquer atividade de tratamento de dados pessoais para outro fim, que possa extrapolar as atividades necessárias à execução do objeto deste contrato, passará a figurar como CONTROLADORA INDEPENDENTE na atividade em questão, e se responsabilizará integralmente pela legitimidade do tratamento.

11.6. Sem prejuízo do disposto no item acima, caso a OPERADORA realize atividades que extrapolem aquelas necessárias à execução do objeto deste Contrato, sua conduta poderá se enquadrar em descumprimento contratual, hipótese na qual poderá ser responsabilizado nos termos deste Contrato.

11.7. Para a execução do objeto do contrato, sem prejuízo das demais disposições legais ou contratuais, as partes se submetem às seguintes obrigações:

a) a CONTROLADORA compromete-se a colocar à disposição da OPERADORA os dados pessoais e informações necessárias para o atingimento das finalidades necessárias à execução do objeto do presente contrato;

b) a CONTROLADORA compromete-se a definir as finalidades para as quais os dados pessoais serão tratados, estabelecendo as bases legais para tanto;

c) a OPERADORA compromete-se a aplicar, durante todo período de tratamento, medidas técnicas e administrativas aptas a garantir um nível de segurança ao tratamento necessário à execução do objeto do presente contrato;

d) a OPERADORA deve considerar o estado da técnica, os custos de implementação e a natureza, âmbito, contexto e objetivos do tratamento, bem como os riscos para os direitos e liberdades dos titulares, garantindo, entre outras medidas:

i. pseudonimização e criptografia de dados pessoais;

ii. a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência continuada do tratamento dos sistemas e serviços;

iii. a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais rapidamente no caso de um incidente físico ou técnico;

iv. um processo de verificação regular e avaliação da eficácia das medidas técnicas e organizacionais, a fim de garantir a segurança do tratamento.

e) a OPERADORA prestará auxílio à CONTROLADORA para garantir o cumprimento tempestivo de todos as disposições da legislação aplicável.

11.8. A OPERADORA assegurará que os dados pessoais que venham a ser tratados em decorrência deste contrato não sejam acessados, compartilhados ou transferidos, inclusive internacionalmente, para terceiros, incluindo subcontratados, sem a autorização prévia, expressa e por escrito da CONTROLADORA.

11.9. Caso a CONTROLADORA autorize essas operações de tratamento, a OPERADORA é integralmente responsável pelas ações e omissões do terceiro, se comprometendo a garantir que tais terceiros se obriguem contratualmente a observar regras equivalentes às previstas neste contrato.

11.10. No caso de transferência internacional, a OPERADORA se compromete a garantir a confidencialidade, disponibilidade e integridade dos dados pessoais e a cumprir com os requisitos da legislação aplicável para a sua efetivação.

11.11. Caberá exclusivamente à CONTROLADORA elaborar as respostas às requisições dos titulares ou de terceiros incluindo, mas não se limitando, a Autoridade Nacional de Proteção de Dados (“ANPD”), que versem sobre o tratamento de dados pessoais realizado em decorrência do presente contrato (“Requisição”).

11.12. Na hipótese de recebimento de qualquer requisição pela OPERADORA, esta deverá transmiti-la à CONTROLADORA imediatamente ou em prazo não superior a 24 (vinte e quatro) horas, de modo a assegurar o atendimento tempestivo pela CONTROLADORA.

11.13. A OPERADORA se compromete a prestar toda e qualquer assistência à CONTROLADORA para o fim de viabilizar o atendimento tempestivo das requisições que estejam relacionadas às atividades de tratamento executadas pela OPERADORA no âmbito deste contrato.

11.14. Na ocorrência ou suspeita de qualquer acesso não autorizado, divulgação indevida, exposição indesejada e/ou situação acidental ou intencional de destruição, deleção, perda, alteração ("Incidente") que envolva os dados pessoais tratados em razão deste contrato, a OPERADORA deverá seguir um plano escrito e estruturado com a previsão, mínima, dos seguintes passos:

a) Notificação à CONTROLADORA no prazo de até 24 (vinte e quatro) horas, devendo conter, no mínimo, as seguintes informações:

i. data e hora do incidente;

ii. data e hora da ciência;

iii. relação dos tipos de dados pessoais afetados pelo incidente;

iv. número de titulares afetados (volumetria do incidente);

v. categorias de titulares afetados;

vi. os riscos relacionados ao incidente;

vii. as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente;

viii. a indicação das medidas de segurança técnicas e administrativas utilizadas para a proteção dos dados pessoais;

ix. os motivos da demora, no caso de a comunicação não ter ocorrido dentro do prazo de 24 (vinte e quatro) horas, sem prejuízo de incorrer nas penalidades contratuais por inadimplemento de seus termos;

x. dados de contato do Encarregado da OPERADORA ou, não havendo Encarregado, de outra pessoa junto à qual seja possível obter mais informações sobre o ocorrido; e

xi. descrição das possíveis consequências do evento.

b) Ainda, a OPERADORA e/ou SUBOPERADORA envolvido no incidente deverá fornecer à CONTROLADORA, dentro do mesmo prazo, todas as informações, documentos e materiais técnicos que contenham evidências relacionadas ao Incidente e que possibilitem a condução de investigação e perícia forense (tais como relatórios internos, informações sobre a preservação de vestígios digitais relacionados ao Incidente, detalhes cronológicos e técnicos sobre cadeia de custódia e mecanismos de garantia de integridade aplicados aos vestígios relacionados ao Incidente), a fim de que a CONTROLADORA possa cumprir as possíveis obrigações em relação ao determinado pela legislação aplicável.

c) Na hipótese de a OPERADORA não dispor da integralidade das informações no momento do envio da comunicação, deverá transmiti-las gradualmente, comprometendo-se a enviar informações completas no prazo limite de 10 (dez) dias.

d) Após notificado sobre o incidente, cabe à CONTROLADORA determinar a estratégia acerca das medidas a serem adotadas, providenciando, quando aplicável:

i. a notificação dos titulares afetados e da autoridade competente, como a Autoridade Nacional de Proteção de Dados, nos termos da Legislação Aplicável;

ii. a adoção, em colaboração com a OPERADORA, de um plano de ação que pondere os fatores que levaram à causa do incidente e aplique medidas que visem garantir a não recorrência de incidentes da mesma natureza.

11.15. Para os incidentes que tenham sido causados em decorrência de ação ou omissão da OPERADORA, este será responsável por eventuais sanções aplicadas pelas autoridades competentes, sem prejuízo das demais disposições legais e contratuais aplicáveis.

11.16. Na hipótese de a OPERADORA deixar de observar a legislação aplicável, as disposições contratuais ou as instruções lícitas da CONTROLADORA, incidirá em multa não compensatória, sem prejuízo da obrigação de indenizar a

CONTROLADORA e terceiros porventura impactados. O dever de indenização incide sobre as perdas e danos, bem como quaisquer consequências do referido descumprimento que exijam o desembolso de valores.

11.17. Caso a CONTROLADORA assuma responsabilidade atribuível a OPERADORA, conforme disposto nas cláusulas 11.15 e 11.16 deste contrato, poderá exercer o direito de regresso em relação a OPERADORA.

11.18. Ao término da relação contratual estabelecida, a OPERADORA deverá devolver ou deletar a integralidade dos Dados Pessoais tratados no âmbito deste Contrato, de acordo com os critérios e instruções da CONTROLADORA.

11.19. Mesmo após o término da vigência deste contrato, as obrigações das partes, enquanto Agentes de Tratamento, perdurarão enquanto qualquer delas realizar atividade de tratamento de dados pessoais a que tiveram acesso em decorrência deste contrato.

11.20. As comunicações relacionadas ao tratamento de dados pessoais realizado no âmbito deste contrato deverão ser direcionadas por uma parte à outra, aos contatos indicados a seguir:

E-mail da CONTRATANTE: **dpo@poupex.com.br**

E-mail da CONTRATADA:_____

12. CONFIDENCIALIDADE

12.1. A CONTRATADA obriga-se a manter o sigilo sobre as informações fornecidas ou obtidas junto à CONTRATANTE, sejam estas classificadas como "informações confidenciais", ou não, abrangendo inclusive informações cadastrais, comerciais ou outras obtidas em decorrência da presente contratação, que são de propriedade exclusiva da CONTRATANTE, respondendo a CONTRATADA pelo pagamento das perdas e danos apurados em processo próprio, quando ocorrer a violação ou a divulgação das mesmas, inclusive por atos de seus empregados, prepostos, prestadores de serviços ou terceiros que as obtiverem junto à CONTRATADA.

12.1.1. O referido sigilo se estende mesmo após o término do compromisso contratual, por tempo indeterminado.

12.1.2. A CONTRATANTE tornará disponível à CONTRATADA as informações públicas e não-públicas sobre suas contas, bens, propriedades, direitos, obrigações, negócios e operações, além de outras, doravante referidas, em conjunto, como as "INFORMAÇÕES".

12.1.3. Serão consideradas como informações públicas aquelas de caráter oficial que forem publicamente divulgadas pela CONTRATANTE.

12.2. As Partes se obrigam, por si, suas controladas, coligadas, seus empregados, administradores, prepostos, terceiros de sua confiança e por seus representantes legais a:

12.2.1. manter confidencialidade sobre todas as INFORMAÇÕES e a não as transmitir nem as revelar a terceiros;

12.2.2. não discutir, perante terceiros, nem usar, divulgar, revelar ou dispor das INFORMAÇÕES para outra finalidade que não aquelas relacionadas à avaliação de seus interesses recíprocos em negociar com a outra parte, cumprindo-lhes adotar cautelas e precauções adequadas no sentido de impedir o uso indevido das INFORMAÇÕES por qualquer pessoa que a estas venha a ter acesso; e

12.2.3. guardar e manter confidencialidade sobre todas as cópias, reproduções, sumários, análises ou comunicados referentes às INFORMAÇÕES ou nestas baseadas, devendo devolvê-los à CONTRATANTE, quando solicitado.

12.3. A parte que estiver recebendo as INFORMAÇÕES ou qualquer outro dado referente às atividades desenvolvidas pela outra parte se obriga e se compromete a protegê-los, a fim de que não sejam revelados a terceiros não autorizados. Todavia, essa obrigação não se aplica às INFORMAÇÕES e/ou dados que:

12.3.1. já forem do domínio público à época em que tiverem sido revelados;

12.3.2. passarem a ser de domínio público, após sua revelação, sem que a divulgação seja efetuada em violação ao disposto neste Acordo;

12.3.3. já forem notoriamente do conhecimento da parte recipiente antes de lhe terem sido revelados; ou

12.3.4. forem legalmente revelados à parte recipiente por terceiros que não os tiverem recebido sob a vigência de uma obrigação de confidencialidade.

13. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

13.1. Em cumprimento às diretrizes contidas na ISO/IEC 27001, ISO/IEC 27035 e LGPD, a CONTRATADA compromete-se em estabelecer, implementar, manter e aprimorar continuamente um sistema de gestão de segurança da informação (SGSI), mas não se limitando à:

13.1.1. apresentar Plano de Gestão de Incidentes de Segurança da Informação para conhecimento e análise da CONTRATANTE;

13.1.2. possuir e manter processo estruturado de Gestão de Incidentes de Segurança da Informação, conforme ISO/IEC 27001 e ISO/IEC 27035;

13.1.3. permitir auditoria ou verificação de conformidade durante a vigência do contrato pela CONTRATANTE;

13.1.4. definir prazos e formas de comunicação de incidentes, incluindo:

e) canal de comunicação;

f) notificação imediata (até 1h após a detecção);

g) comunicação de incidentes com impacto relevante (ex.: vazamento de dados); e

h) obrigatoriedade de investigação e relatório de lições aprendidas.

13.2. Sanções contratuais em caso de falhas graves ou reincidentes na gestão de incidentes.

14. FISCALIZAÇÃO E GESTÃO DO CONTRATO

14.1. A execução do contrato será acompanhada e fiscalizada pelos seguintes representantes, abaixo CREDENCIADOS:

CONTRATANTE
Gestor do contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
Fiscal do Contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
CONTRATADA
Preposto:
Nome: XXXXXXX – Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX
Responsável Técnico:
Nome: XXXXXXX – Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX

14.2. As alterações dos representantes acima nomeados como Gestor, Fiscais, Preposto e Responsável Técnico, poderão ser realizadas por meio de simples APOSTILAMENTO, sendo estabelecido novo CREDENCIAMENTO.

14.3. O representante da CONTRATANTE denominado Gestor do Contrato, atuará com o apoio dos Fiscais do Contrato, credenciados neste instrumento.

14.4. O Gestor, juntamente com os Fiscais, deverá acompanhar a prestação dos serviços, registrar as ocorrências e determinar as medidas necessárias ao fiel cumprimento do contrato, bem como atestar, no todo ou em parte, a realização dos serviços objeto deste contrato.

14.5. O atesto dos serviços prestados pela CONTRATANTE para pagamento da nota fiscal não exime a plena responsabilidade da CONTRATADA em garantir o cumprimento total e satisfatório do contrato em conformidade com as especificações estabelecidas quando da contratação.

14.6. O descumprimento total ou parcial das responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste contrato.

15. ALTERAÇÕES CONTRATUAIS

15.1. As alterações das obrigações estabelecidas neste contrato deverão ser formalizadas por meio da lavratura de Termo Aditivo, mediante acordo entre as partes, e em conformidade com os preços e condições vigentes.

15.2. Na hipótese de alteração das condições econômicas fundamentais prevalecentes na assinatura deste contrato, as partes ajustarão as cláusulas que assegurarão a recuperação dos valores ora contratados, objetivando a manutenção do equilíbrio econômico-financeiro do contrato.

15.3. A CONTRATADA deverá comunicar à CONTRATANTE quaisquer alterações em seu Contrato Social, razão ou denominação social, objeto, CNPJ e outros e ainda seus dados bancários, endereços, telefones, fax, e demais dados que, porventura, venham interferir na alteração da habilitação e qualificação exigidas para a execução das obrigações contratuais.

16. DO REEQUILÍBRIO CONTRATUAL

16.1. Na hipótese de ocorrência de fatos supervenientes que alterem substancialmente os encargos pactuados, inclusive em decorrência de modificações na legislação tributária que impactem direta ou indiretamente os custos da execução contratual, será assegurado o direito à revisão contratual, mediante requerimento fundamentado e comprovação do desequilíbrio.

16.2. O pedido de revisão deverá ser formalizado durante a vigência do contrato e será decidido pela FHE no prazo de até 90 (noventa) dias, prorrogável por igual período, conforme previsto na legislação aplicável, acompanhados de toda a documentação comprobatória pertinente, que demonstrem de forma clara e inequívoca, incluindo:

16.2.1. O fundamento legal que deu origem ao pleito;

16.2.2. O demonstrativo econômico-financeiro do impacto direto e quantificável das alterações fáticas e/ou normativas na estrutura de custos e/ou receitas do Contrato;

16.2.3. Apresentação de valores e percentuais que justifiquem a necessidade de revisão contratual;

16.2.4. O período em que o impacto se torna mensurável e efetivo.

16.3. Qualquer alteração no Contrato decorrente do reequilíbrio econômico-financeiro deverá ser formalizada por meio de Termo Aditivo, devidamente assinado pelas Partes.

16.4. O pleito de reequilíbrio e as negociações subsequentes não suspenderão a execução do Contrato, que deverá prosseguir em seus termos originais até que o Termo Aditivo de reequilíbrio seja formalizado ou a controvérsia seja definitivamente resolvida.

16.5. A FHE poderá, de ofício, promover a revisão contratual nos casos em que se verificar redução da carga tributária, desde que garantido o contraditório e a ampla defesa.

16.6. A revisão poderá resultar em: a) Reajuste dos valores contratados; b) Alteração de prazos ou condições de execução; c) Outras medidas compensatórias que restabeleçam o equilíbrio econômico-financeiro.

17. RESILIÇÃO DO CONTRATO

17.1. Independentemente de justificativa e sem que caiba qualquer indenização à outra parte, este contrato poderá ser denunciado a qualquer tempo, pela CONTRATANTE ou pela CONTRATADA, mediante comunicação feita por escrito e com antecedência mínima de 30 (trinta) dias.

18. PENALIDADES

18.1. O inadimplemento total ou parcial das obrigações contratuais dá, à CONTRATANTE, o direito de aplicar as seguintes penalidades:

18.1.1. advertência, quando constatadas pequenas irregularidades que não cause grave dano à CONTRATANTE;

18.1.2. multa, que poderá ser aplicada por descumprimento de quaisquer das obrigações contratuais, calculada em percentual de 0,5% a 30% sobre o valor total do contrato, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, ou descontada das parcelas devidas à CONTRATADA, sem prejuízo de outras sanções previstas contratualmente;

18.1.3. resolução unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais;

18.1.4. os casos de descumprimento das entregas mínimas aceitáveis, serão enquadrados como inexecução parcial do instrumento contratual.

18.1.5. em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico.

18.1.6. as multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

18.1.7. não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

18.1.8. sendo resolvido o presente contrato, o pagamento devido será proporcional aos serviços prestados até a data da resolução.

18.1.9. para se ressarcir de eventuais prejuízos causados pela CONTRATADA e do valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar esses valores dos créditos decorrentes deste mesmo contrato ou de outros contratos que a CONTRATADA possua com a CONTRATANTE.

18.1.10. caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA.

18.1.11. no processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

19. VIGÊNCIA

19.1. O presente contrato terá vigência desde a data de sua assinatura e vigorará até ___ de _____ de 20__.

20. CONDIÇÕES GERAIS

20.1. Este contrato e a Proposta Técnica e Comercial constituem a totalidade do acordo entre os signatários com relação às matérias aqui previstas e superam, substituem e revogam os entendimentos, negociações e acordos anteriores.

20.2. Em caso de divergências entre a proposta da CONTRATADA e este instrumento fica desde já acordado que prevalecerão as condições estabelecidas neste contrato.

20.3. Não valerá como precedente, novação, ou renúncia aos direitos que a lei e o presente instrumento asseguram a CONTRATANTE, sua tolerância a eventuais descumprimentos de cláusulas, seus itens e subitens, pela CONTRATADA.

21. FORO

21.1. As partes elegem o Foro da Circunscrição Judiciária de Brasília para dirimir quaisquer questões oriundas do presente contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

Nos termos do disposto no art. 107 do Código Civil; art. 3º, da Lei nº 13.874, de 2019; e Decreto nº 10.278, de 2020, as partes e testemunhas, quando for o caso, declaram a autoria, integridade e confiabilidade deste contrato, acordando, assim, em não contestar a sua validade, conteúdo e autenticidade. E, por estarem justos e acertados, as partes concordam que o presente instrumento contratual será assinado digitalmente, bem como os demais documentos correlatos, sendo as assinaturas válidas, vinculantes e executáveis. Admite-se qualquer modalidade de assinatura eletrônica prevista em lei, quando a integridade dessas for conferida por provedor de assinatura, nos termos da Lei nº 14.620, de 2023.

Brasília-DF, de de 2025.

CONTRATANTE	CONTRATADA

TESTEMUNHAS:

Nome:	Nome:

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ____/2025 - POUPEX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE SOLUÇÕES DE SEGURANÇA CIBERNÉTICA FIRMADO ENTRE A POUPEX E A _____.

A **ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO - POUPEX**, sediada na Av. Duque de Caxias s/n.º, Parte A, Setor Militar Urbano - SMU, Brasília/DF, CEP 70630-902, inscrita no CNPJ nº 00.655.522/0001-21, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) (cargo) _____, na forma autorizada por (documento) _____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado(a) em _____, doravante denominada **CONTRATANTE**, e a **(razão social – nome fantasia)** _____, sediada no endereço _____, CEP _____, inscrita no CNPJ nº _____, (IE ou IM ou CF/DF) _____, neste ato, representada por seu (sua) _____ (cargo), conforme (documento - contrato social, procuração)_____, Sr.(a) (nome completo) _____, CPF nº _____, residente e domiciliado (a) em _____, doravante denominada **CONTRATADA**, têm justo e avençado o presente contrato de prestação de serviços, conforme Proposta Técnica e Comercial de Preço de ____/____/_____ e Especificação Técnica, de ___/____/____, partes integrantes deste instrumento, regido pelas cláusulas seguintes e pelas normas de Direito Privado:

1. OBJETO

1.1. O objeto do presente contrato consiste na contratação de empresa especializada para soluções de segurança cibernética visando à proteção contínua dos ativos informacionais da CONTRATANTE, em conformidade com órgãos reguladores e alinhada às boas práticas de segurança da informação, contendo os seguintes itens:

Tabela 1

Item	Descrição	Qtd.
1.	Solução de *Endpoint* com EDR para servidores (deve vir com o suporte técnico do fabricante incluso)	500
1.1	Implementação da solução de *Endpoint* com EDR para servidores.	1
1.2	Repasse de conhecimento da solução de *Endpoint* com EDR para servidores.	1
2.	Solução de Conformidade Equipamentos de Terceiro – NAC (deve vir com o suporte técnico do fabricante incluso)	2.200
2.1	Implementação da solução de Conformidade Equipamentos de Terceiro – NAC.	1
2.2	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC.	1

2. CONDIÇÕES PARA EXECUÇÃO DOS SERVIÇOS

2.1. A CONTRATADA realizará todas as atividades, preferencialmente, no horário comercial, de segunda a sexta-feira exceto feriados, das 8h às 18h.

2.2. A entrega da(s) solução(ões) será(ão) realizada(s) de forma digital, por meio de disponibilização remota dos *softwares* e respectivos componentes.

2.3. A execução dos serviços de implementação e repasse de conhecimento, se necessário, deverá ocorrer de forma remota.

2.4. As soluções de segurança deverão ser fornecidas por meio de licenciamento anual, contemplando todos os componentes necessários para sua plena operação, incluindo *software*, atualizações, suporte técnico e documentação. O modelo de fornecimento será tradicional, com licenças válidas por 12 (doze) meses, renováveis conforme a necessidade da CONTRATANTE, garantindo o funcionamento integral das funcionalidades contratadas durante todo o período de vigência.

2.5. A solução deverá oferecer acesso contínuo a atualizações de segurança, correções de vulnerabilidades, melhorias de desempenho e novas funcionalidades disponibilizadas pelo fabricante, sem custos adicionais durante o período de licenciamento.

2.6. A CONTRATADA será responsável por fornecer os meios necessários para ativação, instalação e configuração inicial da solução, além de disponibilizar manuais, guias técnicos e acesso à base de conhecimento. A solução deverá ser compatível com o ambiente tecnológico da CONTRATANTE e permitir integração com outras ferramentas de segurança já existentes, quando aplicável.

2.7. A efetividade da solução será avaliada por meio de relatórios técnicos, indicadores de desempenho e evidências de funcionamento, conforme critérios definidos pela área técnica da CONTRATANTE.

2.8. Descrição das soluções:

2.8.1. **Solução de *Endpoint* com EDR para servidores**: solução de segurança centralizada voltada à proteção avançada de servidores contra ameaças digitais como vírus, *worms, ransomware, trojans* e ataques de dia zero. Monitora continuamente o comportamento dos sistemas, detecta atividades suspeitas em tempo real e responde automaticamente a incidentes, garantindo integridade, disponibilidade e conformidade dos ambientes críticos.

2.8.2. **Solução de conformidade de equipamentos de terceiros (NAC):** plataforma que garante o acesso seguro à rede corporativa, identificando, classificando e controlando todos os dispositivos conectados — sejam gerenciados ou não. Avalia a conformidade com políticas de segurança antes de permitir o acesso, isolando ou bloqueando dispositivos não autorizados ou vulneráveis. Suporta ambientes com políticas de *BYOD* (*Bring Your Own Device*), oferecendo visibilidade e controle sobre dispositivos pessoais, e integra-se a outras soluções de cibersegurança para fortalecer a proteção contra ameaças internas e externas.

2.9. Serviços de implementação: a CONTRATADA será responsável pela instalação, configuração e validação inicial da solução, garantindo sua plena operação conforme os requisitos técnicos definidos pela CONTRATANTE.

2.10. Repasse de Conhecimento**:** serão realizadas atividades de repasse de conhecimento técnico às equipes da CONTRATANTE, com foco na solução implementada, visando assegurar o entendimento aprofundado de sua arquitetura, funcionalidades e procedimentos operacionais. Esse processo tem como objetivo promover autonomia na gestão e manutenção da solução. O repasse de conhecimento poderá ser disponibilizado também sob demanda, por meio de acesso a plataformas especializadas oferecidas pelo fabricante, proporcionando maior flexibilidade e continuidade no processo de assimilação técnica.

2.11. Suporte Técnico: o suporte técnico deverá estar incluso no licenciamento e prestado exclusivamente pelo fabricante da solução, assegurando domínio completo da tecnologia ofertada e maior eficiência na identificação e resolução de incidentes. O serviço deverá estar disponível em regime 24x7, com atendimento remoto e escalonamento conforme a criticidade dos chamados, assegurando a continuidade operacional da solução durante todo o período de vigência do contrato.

2.12. Acordo de Nível de Serviço para Chamados de Suporte Técnico: o suporte técnico será prestado diretamente pelo fabricante da solução mediante abertura de chamado por parte da CONTRATANTE e o Acordo de Nível de Serviço – ANS obedecerá ao descrito na plataforma do fabricante, sendo obrigatoriamente na modalidade de 24 x 7 para resolução de incidentes e demandas.

2.12.1. será dado início a abertura do chamado para o suporte técnico através dos canais: e-mail (_____) ou telefone (_____) para a centralização dos chamados e controles de SLA.

2.13. A CONTRATANTE e a CONTRATADA são pessoas jurídicas totalmente distintas e independentes, não configurando este contrato nenhuma forma de sociedade, pelo que os profissionais terceirizados, designados pela CONTRATADA para a prestação dos serviços objeto deste contrato, atuarão sem qualquer subordinação laboral à CONTRATANTE e, portanto, inexistente vínculo ou relação de trabalho com a CONTRATANTE.

3. PREÇO

3.1. O valor total deste contrato é de R$ _____ (_____).

3.2. As despesas decorrentes deste contrato correrão por conta dos recursos próprios da POUPEX, consignados na conta orçamentária. Centro de custo: _____. Conta contábil/orçamentaria _____.

3.3. Nos preços fixados nesta cláusula estão compreendidos todos os custos e despesas que, direta ou indiretamente, decorram do cumprimento pleno e integral do objeto deste contrato, tais como e sem se limitar a: telefone, salários, honorários, encargos sociais, trabalhistas, securitários, previdenciários e acidentários, lucro, taxa de administração e tributos, softwares, direitos autorais, licenças de uso e custos operacionais, constituindo a qualquer título, a única e completa remuneração pela adequada e perfeita execução dos serviços, de modo que nenhuma outra será devida.

4. FORMA E CONDIÇÕES DE PAGAMENTO

4.1. A CONTRATANTE pagará à CONTRATADA, conforme quadro abaixo, pela prestação dos serviços objeto deste contrato, após a conclusão dos serviços, mediante a emissão do Termo de Recebimento, Aceitação dos Serviços e atesto na nota fiscal a ser apresentada com 10 (dez) dias de antecedência do vencimento:

Item	Descrição	Qtd	Valor Unitário (R$)	Valor Total (R$)
1.	Solução de *Endpoint* com EDR para servidores	500		
1.1	Implementação da solução de *Endpoint* com EDR para servidores.	1		
1.2	Repasse de conhecimento da solução de *Endpoint* com EDR para servidores.	1		
2.	Solução de Conformidade Equipamentos de Terceiro – NAC	2.200		
2.1	Implementação da solução de Conformidade Equipamentos de Terceiro – NAC.	1		
2.2	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC.	1		

4.2. As notas fiscais (NFe/DANFE) deverão ser preenchidas com os dados da CONTRATANTE informados a seguir:

Razão Social: ASSOCIAÇÃO DE POUPANÇA E EMPRÉSTIMO – POUPEX

CNPJ: 00.655.522/0001-21

Inscrição municipal ou CF/DF: 07.451.631/001-57

End.: Avenida Duque de Caxias, s/n.º, Parte A, Setor Militar Urbano – SMU

Cidade: Brasília/DF

CEP: 70630-902

4.3. A CONTRATANTE obriga-se a efetuar as retenções tributárias incidentes nos percentuais e alíquotas determinados por Leis e Decretos, para as quais a CONTRATADA deverá destacar na nota fiscal os respectivos valores das retenções cabíveis.

4.4. Não serão efetuados os recolhimentos referentes ao IRPJ, CSLL, PIS e COFINS, quando a Declaração de Optante pelo SIMPLES Nacional for apresentada junto com a nota fiscal. Neste caso, o documento original da Declaração deverá ser enviado pelos Correios para o endereço do item 4.2.

4.5. Para que o pagamento seja realizado por meio de depósito bancário, as informações abaixo devem estar atualizadas, vinculadas ao CNPJ da CONTRATADA, ou de alguma de suas filiais, desde que devidamente registrado na nota fiscal.

Nome do Favorecido – (RAZÃO SOCIAL DA CONTRATADA)

CNPJ – 00.000.000/0000-00

Número do Banco - 000

Nome do Banco - BANCO FULANO S/A

Número da Agência Bancária – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Número da Conta Corrente – 0000-0 (INFORMAR INCLUSIVE O DÍGITO)

Modalidade de Conta – CONTA CORRENTE/CONTA POUPANÇA

Chave PIX – (INFORMAR)

4.6. Na impossibilidade de o pagamento ser realizado em conta corrente, poderá ser emitido Boleto Bancário pela CONTRATADA, fazendo-se referência à nota fiscal emitida.

4.7. O pagamento será liquidado em até 10 (dez) dias úteis após a entrada da nota fiscal na Gerência de Compras e Contratos (GECOC), desde que o serviço esteja devidamente prestado.

4.7.1. A nota fiscal juntamente com o arquivo XML somente serão recebidos no e-mail corporativo pagamento.gecoc@poupex.com.br, até o dia 20 do mês de sua emissão, para que as retenções sejam processadas pela CONTRATANTE até o último dia útil do mesmo mês. Caso não seja possível à CONTRATADA encaminhar as referidas notas fiscais nesse prazo, essas deverão ser emitidas com data do 1º (primeiro) dia do mês subsequente.

4.7.2. Todos os campos da nota fiscal deverão ser corretamente preenchidos, sem exceção, sob pena de devolução da Nota. A nota fiscal emitida com irregularidades (rasuras, dados incompletos, vencimento em desacordo, etc.) será devolvida com as informações que motivaram a rejeição para nova emissão, e será iniciada a contagem de novo prazo para pagamento após as correções pertinentes.

4.8. O custo das tarifas bancárias deverá ser suportado pela CONTRATADA nos casos em que os dados bancários informados estejam em desacordo com o CNPJ da CONTRATADA, ou que apresentem alguma inconsistência que motivaram a rejeição do pagamento.

4.9. Será considerada inválida qualquer forma de cobrança realizada em desacordo com o previsto nesta cláusula.

4.10. O não pagamento de quaisquer valores devidos pela CONTRATANTE no prazo acima mencionado implicará a incidência dos seguintes encargos moratórios, até a data do efetivo pagamento:

4.10.1. Juros de mora de 1% (um por cento) ao mês, calculados “pro rata die”; e

4.10.2. Multa de 2% (dois por cento) sobre o parcelamento em atraso.

5. PRAZO

5.1. O prazo para a execução dos serviços será de 12 (doze) meses, contados a partir da data de assinatura deste contrato, podendo ser prorrogado por igual(is) e sucessivo(s) período(s), mediante assinatura de Termo(s) Aditivo(s), até o limite de 120 (cento e vinte) meses, caso sejam preenchidos os requisitos abaixo enumerados de forma simultânea:

5.1.1. que os serviços tenham sido prestados regularmente e satisfatoriamente;

5.1.2. a CONTRATADA não tenha sofrido qualquer punição de natureza pecuniária;

5.1.3. a CONTRATANTE ainda tenha interesse na realização do serviço;

5.1.4. o valor do contrato permaneça economicamente vantajoso para a CONTRATANTE; e

5.1.5. a CONTRATADA concorde com a prorrogação do contrato.

5.2. A CONTRATADA deverá, ainda, cumprir os seguintes prazos:

Item	Descrição	Prazo
1.	Assinatura do instrumento contratual	Em até 5 (cinco) dias úteis após aprovação da fase de validação
2.	Apresentação de plano de implementação e entrega da subscrição da solução *Endpoint* com EDR para servidores.	Em até 7 dias úteis, após a assinatura do contrato.
2.1	Implementação da solução *Endpoint* com EDR para servidores, se	Em até 15 dias úteis, após a apresentação do

	necessário.	plano de implementação.
2.2	Repasse de conhecimento da solução *Endpoint* com EDR para servidores, se necessário.	Em até 7 dias úteis, após a implementação da solução.
3.	Apresentação de plano de implementação e entrega da subscrição da solução de Conformidade Equipamentos de Terceiro – NAC.	Em até 7 dias úteis, após a assinatura do contrato.
3.1	Implementação da solução de Conformidade Equipamentos de Terceiro – NAC, se necessário.	Em até 15 dias úteis, após a apresentação do plano de implementação.
3.2	Repasse de conhecimento da solução de Conformidade Equipamentos de Terceiro – NAC, se necessário.	Em até 7 dias úteis, após a implementação da solução.

6. RECEBIMENTO DOS SERVIÇOS E EMISSÃO DO TERMO DE ACEITAÇÃO DOS SERVIÇOS

6.1. O recebimento dos serviços com a consequente emissão do Termo de Aceitação dos Serviços está condicionado ao atendimento, quando for o caso:

6.1.1. dos prazos de entrega previstos no item 5.2.;

6.1.2. da implementação com todas as soluções operacionais. A validação técnica pela CONTRATANTE se dará com base em testes de funcionamento e checklist de entrega, e

6.1.3. do repasse de conhecimento à equipe da CONTRATANTE, com a execução de 100% das ações previstas no plano e entrega dos materiais de apoio.

6.2. A aferição ocorrerá com base no acompanhamento e validação realizados pela CONTRATANTE, mediante relatórios de acompanhamento apresentados pela CONTRATADA.

7. REAJUSTE

7.1. O valor pactuado da cláusula 4ª poderá ser reajustado após 12 (doze) meses da assinatura deste contrato, após solicitação da CONTRATADA, mediante negociação entre as partes, tendo como limite máximo a variação do Índice Nacional de Preços ao Consumidor Amplo (IPCA/IBGE) ocorrida nos últimos 12 (doze) meses, a contar da data da apresentação da proposta ou do último reajuste.

7.2. No caso da extinção ou não divulgação do índice IPCA/IBGE, o valor será reajustado com outro índice equivalente, que melhor se ajuste ao objeto do contrato, ou ainda, por acordo entre as partes.

7.3. A CONTRATADA, ao realizar a solicitação de reajuste, deverá encaminhar a memória de cálculo, com base no índice utilizado no item 7.1

7.4. O reajuste deverá ser solicitado antes do término da atual vigência do contrato, sob pena de preclusão.

8. OBRIGAÇÕES DA CONTRATADA

8.1. São obrigações da CONTRATADA:

8.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

8.1.2. auxiliar a equipe técnica da CONTRATANTE na implementação do plano de ação, fornecendo orientações e suporte técnico necessário para garantir o funcionamento adequado da solução;

8.1.3. a CONTRATADA não poderá realizar alterações nos ambientes computacionais preexistentes da CONTRATANTE, salvo mediante autorização formal e prévia, respeitando os limites definidos pela área técnica.

8.1.4. realizar todos os procedimentos e as demais atividades relativas ao objeto contratado por meio de equipe técnica especializada e devidamente qualificada, necessária à completa e perfeita execução do objeto contratado, em conformidade com a especificação técnica e melhores práticas;

8.1.5. manter a confidencialidade e a segurança dos documentos durante todo o processo;

8.1.6. comunicar por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários;

8.1.7. alertar seus prepostos, empregados e/ou prestadores de serviços acerca da boa conduta, principalmente, no tocante à disciplina e discrição quando da execução de suas tarefas;

8.1.8. garantir o ambiente de segurança necessário em atendimento à Lei Geral de Proteção de Dados (LGPD);

8.1.9. prestar os serviços com zelo e desempenho necessário à execução dos serviços;

8.1.10. comunicar imediatamente a CONTRANTANTE qualquer irregularidade na prestação dos serviços;

8.1.11. propiciar os meios e facilidades necessárias à fiscalização dos serviços, observando as penalidades cabíveis;

8.1.12. refazer, sem ônus para a CONTRATANTE, os serviços executados em desacordo com as características e especificações exigidas neste contrato e constantes da Proposta Comercial da CONTRATADA;

8.1.13. atender as exigências previstas na Circular BACEN n.º 3.978 – (PLD/FT), que dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016;

8.1.14. não designar, para a prestação dos serviços objeto deste contrato, familiar de dirigente ou de empregado da CONTRATANTE ou da Fundação Habitacional do Exército – FHE;

8.1.14.1. considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

8.1.15. não transferir, por qualquer forma, os direitos e obrigações que o presente contrato lhe atribui, salvo com a expressa anuência da CONTRATANTE, manifestada por escrito e por quem detenha poderes para tanto;

8.1.16. não se pronunciar em nome da CONTRATANTE, inclusive junto a órgãos de imprensa, sobre nenhum assunto relativo à sua atividade, guardar sigilo absoluto quanto a toda informação obtida da CONTRATANTE em decorrência do presente contrato, bem como não divulgar ou reproduzir nenhum documento, instrumentos normativos e materiais encaminhados pela CONTRATANTE;

8.1.17. não utilizar o nome da CONTRATANTE, ou sua qualidade de prestadora de serviços, em qualquer forma de divulgação de suas atividades, tais como cartões de visita, anúncios, impressos ou qualquer outro tipo de propaganda;

8.1.18. ressarcir toda e qualquer quantia que for efetivamente paga pela CONTRATANTE, em decorrência do ato ou fato culposo e/ou doloso dos empregados, prestadores de serviços e/ou prepostos da CONTRATADA;

8.1.19. pagar todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços objeto do contrato. Fica, desde logo, convencionado que a CONTRATANTE poderá descontar, de qualquer crédito da CONTRATADA, a importância correspondente a eventuais pagamentos dessa natureza, que venha a efetuar por imposição legal;

8.1.20. apresentar, quando solicitado pela CONTRATANTE cópia de todo e qualquer documento que ateste a regularidade da CONTRATADA;

8.1.21. cumprir todas as leis e instrumentos normativos reguladores da sua atividade empresarial, bem como satisfazer, às suas próprias expensas, todas e quaisquer exigências legais decorrentes da execução do presente contrato; e

8.1.22. assumir responsabilidade pelos danos diretos provocados à CONTRATANTE, decorrente de atos comissivos e omissivos, praticados por seus sócios, associados, integrantes não sócios, empregados, representantes, prestadores de serviços e prepostos, durante a execução do contrato. Os danos causados à CONTRATANTE serão suportados pela CONTRATADA, até o limite equivalente a 50% (cinquenta por cento) dos últimos 6 (seis) pagamentos realizados pela CONTRATANTE à CONTRATADA. Nenhuma das partes responderá por lucros cessantes, danos morais ou quaisquer danos indiretos.

8.2. A CONTRATADA é, para todos os fins e efeitos jurídicos, única e exclusiva responsável por seus empregados, prepostos e/ou prestadores de serviços, afastando a CONTRATANTE, em todas as hipóteses, de qualquer responsabilidade fiscal, trabalhista, comercial, civil, penal, administrativa e previdenciária pelos contratos firmados pela CONTRATADA. Desde já, a CONTRATADA e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se a excluir a CONTRATANTE de toda demanda judicial promovida por seu empregado, preposto e/ou seu contratado para prestação de serviços objeto deste contrato, isentando a CONTRATANTE de todo e qualquer ônus, responsabilidade e/ou vínculo para com esses.

8.2.1. Caso seja mantida a presença da CONTRATANTE em eventuais reclamações trabalhistas ou quaisquer outras ações, administrativas ou judiciais, que tenham como fundamento matérias reguladas na legislação já referida, a CONTRATADA, seus sócios e empresas ligadas, coligadas ou integrantes do grupo econômico (formal ou informal) obrigam-se, desde logo e sem qualquer discussão, a ressarcir a CONTRATANTE de todos os valores despendidos e de adiantar pagamentos a serem efetuados em razão de eventuais condenações, no prazo de 24 (vinte e quatro) horas, contados da solicitação nesse sentido, sob pena de multa de 10% (dez por cento) sobre o valor da condenação ou do valor efetivamente pago, em conformidade com o art. 408 do Código Civil.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. São obrigações da CONTRATANTE:

9.1.1. credenciar, por escrito, o(s) representante(s) que será(ão) o(s) seu(s) interlocutor(es), no que diz respeito à execução do presente contrato;

9.1.2. acompanhar e fiscalizar a execução do serviço contratado;

9.1.3. fornecer a infraestrutura, os dados e as informações necessárias para o funcionamento e parametrização da solução, além da equipe técnica para acompanhamento das atividades;

9.1.4. disponibilizar os acessos necessários às informações da CONTRATANTE, desde que atenda os critérios de segurança estipulados pela CONTRATANTE;

9.1.5. permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, caso necessário, o acesso remoto da CONTRATANTE, respeitadas as normas de segurança vigentes;

9.1.6. receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita;

9.1.7. notificar a CONTRATADA, por escrito, sobre ou a respeito de quaisquer irregularidades encontradas nas execuções de serviços fixando-lhe prazos para as correções;

9.1.8. proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços dentro das condições estabelecidas neste contrato;

9.1.9. efetuar os pagamentos de sua responsabilidade nas datas previstas, desde que cumpridos todos os procedimentos administrativos de responsabilidade da CONTRATADA.

10. DA RESPONSABILIDADE SOCIAL E AMBIENTAL

10.1. Em cumprimento às diretrizes da Política de Responsabilidade Socioambiental da CONTRATANTE, a CONTRATADA se compromete a:

10.1.1. não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal na execução de suas atividades, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

10.1.2. não empregar menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre, e nem menores de 16 (dezesseis) anos, salvo na condição de jovem aprendiz;

10.1.3. não permitir a prática ou a manutenção de atos discriminatórios que limitem o acesso a relação de emprego, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.4. buscar prevenir e erradicar práticas danosas ao meio ambiente, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos à produção, consumo e destinação dos resíduos sólidos de maneira sustentável, implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

10.1.5. comprovada a não observância dos preceitos acima, a CONTRATANTE notificará a CONTRATADA para a respectiva regularização. O não atendimento da notificação sujeitará a CONTRATADA às penalidades previstas contratualmente e, até mesmo, impossibilitar a renovação do pacto sem prejuízo das cominações legais.

11. DA PROTEÇÃO DOS DADOS E DAS INFORMAÇÕES DA CONTRATANTE E DE TERCEIROS

11.1. Para os fins deste contrato, os termos utilizados deverão ser interpretados conforme o disposto no art. 5º da Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, a CONTRATANTE atuará como CONTROLADORA dos dados pessoais eventualmente tratados no âmbito deste contrato, enquanto a CONTRATADA atuará como OPERADORA.

11.2. As partes se comprometem a tratar os dados pessoais a que tiveram acesso em decorrência do presente contrato, única e exclusivamente para cumprir com a finalidade a que se destina seu tratamento e em respeito a toda a legislação aplicável sobre segurança da informação, privacidade e proteção de dados pessoais, inclusive, a LGPD, sem exclusão das demais normas setoriais ou gerais sobre os temas (Legislação Aplicável).

11.3. As partes deverão tratar os dados pessoais como informações confidenciais, responsabilizando-se por quem quer que venha acessá-los e garantindo que tais pessoas estejam sujeitas a idêntico dever de confidencialidade e a regras não menos rigorosas que aquelas estabelecidas neste contrato.

11.4. A OPERADORA se compromete a restringir o tratamento ao número mínimo de dados pessoais necessários ao atingimento das finalidades lícitas, específicas e informadas aos titulares, que sejam imprescindíveis à execução do objeto deste contrato.

11.5. A OPERADORA, quando realizar operações de tratamento envolvendo dados pessoais sensíveis, deve garantir que as proteções técnicas apropriadas, aptas a manter a integridade, confidencialidade e segurança dessas informações, sejam implementadas, concordando em tratar esses dados pessoais apenas quando estritamente necessário para cumprir com o contrato, sempre em estrita observância à legislação aplicável e sob as instruções fornecidas, a qualquer momento, pela CONTROLADORA.

11.6. Na hipótese de a OPERADORA considerar necessária a realização de qualquer atividade de tratamento de dados pessoais para outro fim, que possa extrapolar as atividades necessárias à execução do objeto deste contrato, passará a figurar como CONTROLADORA INDEPENDENTE na atividade em questão, e se responsabilizará integralmente pela legitimidade do tratamento.

11.7. Sem prejuízo do disposto no item acima, caso a OPERADORA realize atividades que extrapolem aquelas necessárias à execução do objeto deste Contrato, sua conduta poderá se enquadrar em descumprimento contratual, hipótese na qual poderá ser responsabilizado nos termos deste contrato.

11.8. Para a execução do objeto do contrato, sem prejuízo das demais disposições legais ou contratuais, as partes se submetem às seguintes obrigações:

f) a CONTROLADORA compromete-se a colocar à disposição da OPERADORA os dados pessoais e informações necessárias para o atingimento das finalidades necessárias à execução do objeto do presente contrato;

g) a CONTROLADORA compromete-se a definir as finalidades para as quais os dados pessoais serão tratados, estabelecendo as bases legais para tanto;

h) a OPERADORA compromete-se a aplicar, durante todo período de tratamento, medidas técnicas e administrativas aptas a garantir um nível de segurança ao tratamento necessário à execução do objeto do presente contrato;

i) a OPERADORA deve considerar o estado da técnica, os custos de implementação e a natureza, âmbito, contexto e objetivos do tratamento, bem como os riscos para os direitos e liberdades dos titulares, garantindo, entre outras medidas:

v. pseudonimização e criptografia de dados pessoais;

vi. a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência continuada do tratamento dos sistemas e serviços;

vii. a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais rapidamente no caso de um incidente físico ou técnico;

viii. um processo de verificação regular e avaliação da eficácia das medidas técnicas e organizacionais, a fim de garantir a segurança do tratamento.

j) a OPERADORA prestará auxílio à CONTROLADORA para garantir o cumprimento tempestivo de todos as disposições da legislação aplicável.

11.9. A OPERADORA assegurará que os dados pessoais que venham a ser tratados em decorrência deste contrato não sejam acessados, compartilhados ou transferidos, inclusive internacionalmente, para terceiros, incluindo subcontratados, sem a autorização prévia, expressa e por escrito da CONTROLADORA.

11.10. Caso a CONTROLADORA autorize essas operações de tratamento, a OPERADORA é integralmente responsável pelas ações e omissões do terceiro, se comprometendo a garantir que tais terceiros se obriguem contratualmente a observar regras equivalentes às previstas neste contrato.

11.11. No caso de transferência internacional, a OPERADORA se compromete a garantir a confidencialidade, disponibilidade e integridade dos dados pessoais e a cumprir com os requisitos da legislação aplicável para a sua efetivação.

11.12. Caberá exclusivamente à CONTROLADORA elaborar as respostas às requisições dos titulares ou de terceiros incluindo, mas não se limitando, a Autoridade Nacional de Proteção de Dados ("ANPD"), que versem sobre o tratamento de dados pessoais realizado em decorrência do presente contrato ("Requisição").

11.13. Na hipótese de recebimento de qualquer requisição pela OPERADORA, esta deverá transmiti-la à CONTROLADORA imediatamente ou em prazo não superior a 24 (vinte e quatro) horas, de modo a assegurar o atendimento tempestivo pela CONTROLADORA.

11.14. A OPERADORA se compromete a prestar toda e qualquer assistência à CONTROLADORA para o fim de viabilizar o atendimento tempestivo das requisições que estejam relacionadas às atividades de tratamento executadas pela OPERADORA no âmbito deste contrato.

11.15. Na ocorrência ou suspeita de qualquer acesso não autorizado, divulgação indevida, exposição indesejada e/ou situação acidental ou intencional de destruição, deleção, perda, alteração ("Incidente") que envolva os dados pessoais tratados em razão deste contrato, a OPERADORA deverá seguir um plano escrito e estruturado com a previsão, mínima, dos seguintes passos:

a) Notificação à CONTROLADORA no prazo de até 24 (vinte e quatro) horas, devendo conter, no mínimo, as seguintes informações:

xii. data e hora do incidente;

xiii. data e hora da ciência;

xiv. relação dos tipos de dados pessoais afetados pelo incidente;

xv. número de titulares afetados (volumetria do incidente);

xvi. categorias de titulares afetados;

xvii. os riscos relacionados ao incidente;

xviii. as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente;

xix. a indicação das medidas de segurança técnicas e administrativas utilizadas para a proteção dos dados pessoais;

xx. os motivos da demora, no caso de a comunicação não ter ocorrido dentro do prazo de 24 (vinte e quatro) horas, sem prejuízo de incorrer nas penalidades contratuais por inadimplemento de seus termos;

xxi. dados de contato do Encarregado da OPERADORA ou, não havendo Encarregado, de outra pessoa junto à qual seja possível obter mais informações sobre o ocorrido; e

xxii. descrição das possíveis consequências do evento.

e) Ainda, a OPERADORA e/ou SUBOPERADORA envolvido no incidente deverá fornecer à CONTROLADORA, dentro do mesmo prazo, todas as informações, documentos e materiais técnicos que contenham evidências relacionadas ao Incidente e que possibilitem a condução de investigação e perícia forense (tais como relatórios internos, informações sobre a preservação de vestígios digitais relacionados ao Incidente, detalhes cronológicos e técnicos sobre cadeia de custódia e mecanismos de garantia de integridade aplicados aos vestígios relacionados ao Incidente), a fim de que a CONTROLADORA possa cumprir as possíveis obrigações em relação ao determinado pela legislação aplicável.

f) Na hipótese de a OPERADORA não dispor da integralidade das informações no momento do envio da comunicação, deverá transmiti-las gradualmente, comprometendo-se a enviar informações completas no prazo limite de 10 (dez) dias.

g) Após notificado sobre o incidente, cabe à CONTROLADORA determinar a estratégia acerca das medidas a serem adotadas, providenciando, quando aplicável:

iii. a notificação dos titulares afetados e da autoridade competente, como a Autoridade Nacional de Proteção de Dados, nos termos da Legislação Aplicável;

iv. a adoção, em colaboração com a OPERADORA, de um plano de ação que pondere os fatores que levaram à causa do incidente e aplique medidas que visem garantir a não recorrência de incidentes da mesma natureza.

11.16. A OPERADORA declara que possui medidas técnicas e administrativas implementadas aptas a proteger os dados pessoais tratados em razão do presente contrato. Declara, ainda, possuir política de segurança da informação instituída, a qual é capaz de garantir a integridade, disponibilidade e confidencialidade dos dados pessoais tratados, devendo prever, no mínimo:

a) Condução de treinamentos *onboarding* e, posteriormente, de reciclagens periódicas com os funcionários da organização, ao menos uma vez por ano. A OPERADORA manterá registro dos treinamentos realizados, bem como o conteúdo tratado e lista de presenças, devendo disponibilizar tais evidências à CONTROLADORA, sempre que solicitado, em prazo não superior a 5 (cinco) dias úteis; e

b) Medidas técnicas de controle, que deverão incluir ao menos sistema de detecção de invasão ou tentativa de invasão pela *internet*, incluindo, mas não se limitando, a contenção de vírus e *drives* maliciosos; solução que possibilite a encriptação dos dados pessoais tratados em razão do presente contrato, quando necessário e de acordo com o nível de sensibilidade e volume das informações:

i. possibilidade de anonimização e/ou pseudonimização de registros;

ii. sistemas que previnam a acoplagem de sistemas móveis de carregamento de informações ou dispositivos relacionados. O uso de tais dispositivos deve ser previamente autorizado e registrado pela área técnica da CONTROLADORA;

iii. um profissional designado e instituído em tempo integral para figurar como ponto focal responsável pelas medidas de segurança aplicadas;

iv. a realização de *backups* diários nos ambientes nos quais haja o armazenamento de dados pessoais; e

v. controle de acesso com registro de *logs* de funcionários, excluindo aqueles que não tenham necessidade de acessar os dados pessoais relativos ao contrato

11.17. É facultado à CONTROALDORA, a realização de auditorias, à sua discricionariedade, ao menos, 1 (uma) vez ao ano, por si ou mediante terceiros por ele indicados, nos documentos ou sistemas da OPERADORA, desde que haja comunicação prévia com pelo menos 15 (quinze) dias de antecedência.

11.18. Nas auditorias, a CONTROLADORA garante o mínimo de interferência possível nas atividades ordinárias da OPERADORA. As auditorias mencionadas deverão ser restritas a analisar questões que guardem relação com o presente Contrato.

11.19. Para os incidentes que tenham sido causados em decorrência de ação ou omissão da OPERADORA, este será responsável por eventuais sanções aplicadas pelas autoridades competentes, sem prejuízo das demais disposições legais e contratuais aplicáveis.

11.20. Na hipótese de a OPERADORA deixar de observar a legislação aplicável, as disposições contratuais ou as instruções lícitas da CONTROLADORA, incidirá em multa não compensatória, sem prejuízo da obrigação de indenizar a

CONTROLADORA e terceiros porventura impactados. O dever de indenização incide sobre as perdas e danos, bem como quaisquer consequências do referido descumprimento que exijam o desembolso de valores.

11.21. Caso a CONTROLADORA assuma responsabilidade atribuível a OPERADORA, conforme disposto nas cláusulas 11.19 e 11.20 deste Contrato, poderá exercer o direito de regresso em relação a OPERADORA.

11.22. Ao término da relação contratual estabelecida, a OPERADORA deverá devolver ou deletar a integralidade dos Dados Pessoais tratados no âmbito deste Contrato, de acordo com os critérios e instruções da CONTROLADORA.

11.23. Mesmo após o término da vigência deste contrato, as obrigações das partes, enquanto Agentes de Tratamento, perdurarão enquanto qualquer delas realizar atividade de tratamento de dados pessoais a que tiveram acesso em decorrência deste contrato.

11.24. As comunicações relacionadas ao tratamento de dados pessoais realizado no âmbito deste contrato deverão ser direcionadas por uma parte à outra, aos contatos indicados a seguir:

E-mail da CONTRATANTE: **dpo@poupex.com.br**

E-mail da CONTRATADA:_____

12. CONFIDENCIALIDADE

12.1. A CONTRATADA obriga-se a manter o sigilo sobre as informações fornecidas ou obtidas junto à CONTRATANTE, sejam estas classificadas como "informações confidenciais", ou não, abrangendo inclusive informações cadastrais, comerciais ou outras obtidas em decorrência da presente contratação, que são de propriedade exclusiva da CONTRATANTE, respondendo a CONTRATADA pelo pagamento das perdas e danos apurados em processo próprio, quando ocorrer a violação ou a divulgação das mesmas, inclusive por atos de seus empregados, prepostos, prestadores de serviços ou terceiros que as obtiverem junto à CONTRATADA.

12.1.1. O referido sigilo se estende mesmo após o término do compromisso contratual, por tempo indeterminado.

12.1.2. A CONTRATANTE tornará disponível à CONTRATADA as informações públicas e não-públicas sobre suas contas, bens, propriedades, direitos, obrigações, negócios e operações, além de outras, doravante referidas, em conjunto, como as "INFORMAÇÕES".

12.1.3. Serão consideradas como informações públicas aquelas de caráter oficial que forem publicamente divulgadas pela CONTRATANTE.

12.2. As Partes se obrigam, por si, suas controladas, coligadas, seus empregados, administradores, prepostos, terceiros de sua confiança e por seus representantes legais a:

12.2.1. manter confidencialidade sobre todas as INFORMAÇÕES e a não as transmitir nem as revelar a terceiros;

12.2.2. não discutir, perante terceiros, nem usar, divulgar, revelar ou dispor das INFORMAÇÕES para outra finalidade que não aquelas relacionadas à avaliação de seus interesses recíprocos em negociar com a outra parte, cumprindo-lhes adotar cautelas e precauções adequadas no sentido de impedir o uso indevido das INFORMAÇÕES por qualquer pessoa que a estas venha a ter acesso; e

12.2.3. guardar e manter confidencialidade sobre todas as cópias, reproduções, sumários, análises ou comunicados referentes às INFORMAÇÕES ou nestas baseadas, devendo devolvê-los à CONTRATANTE, quando solicitado.

12.3. A parte que estiver recebendo as INFORMAÇÕES ou qualquer outro dado referente às atividades desenvolvidas pela outra parte se obriga e se compromete a protegê-los, a fim de que não sejam revelados a terceiros não autorizados. Todavia, essa obrigação não se aplica às INFORMAÇÕES e/ou dados que:

12.3.1. já forem do domínio público à época em que tiverem sido revelados;

12.3.2. passarem a ser de domínio público, após sua revelação, sem que a divulgação seja efetuada em violação ao disposto neste Acordo;

12.3.3. já forem notoriamente do conhecimento da parte recipiente antes de lhe terem sido revelados; ou

12.3.4. forem legalmente revelados à parte recipiente por terceiros que não os tiverem recebido sob a vigência de uma obrigação de confidencialidade.

13. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

13.1. Em cumprimento às diretrizes contidas na ISO/IEC 27001, ISO/IEC 27035 e LGPD, a CONTRATADA compromete-se em estabelecer, implementar, manter e aprimorar continuamente um sistema de gestão de segurança da informação (SGSI), mas não se limitando à:

13.1.1. apresentar Plano de Gestão de Incidentes de Segurança da Informação para conhecimento e análise da CONTRATANTE;

13.1.2. possuir e manter processo estruturado de Gestão de Incidentes de Segurança da Informação, conforme ISO/IEC 27001 e ISO/IEC 27035;

13.1.3. permitir auditoria ou verificação de conformidade durante a vigência do contrato pela CONTRATANTE;

13.1.4. definir prazos e formas de comunicação de incidentes, incluindo:

i) canal de comunicação;

j) notificação imediata (até 1h após a detecção);

k) comunicação de incidentes com impacto relevante (ex.: vazamento de dados); e

l) obrigatoriedade de investigação e relatório de lições aprendidas.

13.2. Sanções contratuais em caso de falhas graves ou reincidentes na gestão de incidentes.

14. FISCALIZAÇÃO E GESTÃO DO CONTRATO

14.1. A execução do contrato será acompanhada e fiscalizada pelos seguintes representantes, abaixo CREDENCIADOS:

CONTRATANTE
Gestor do contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
Fiscal do Contrato:
Nome: XXXXXXX – UTA/Telefone: XXXXXXXXXX
CONTRATADA
Preposto:
Nome: XXXXXXX – Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX
Responsável Técnico:
Nome: XXXXXXX – Telefone: XXXXXXXXXX – e-mail: XXXX@XXXXX

14.2. As alterações dos representantes acima nomeados como Gestor, Fiscais, Preposto e Responsável Técnico, poderão ser realizadas por meio de simples APOSTILAMENTO, sendo estabelecido novo CREDENCIAMENTO.

14.3. O representante da CONTRATANTE denominado Gestor do Contrato, atuará com o apoio dos Fiscais do Contrato, credenciados neste instrumento.

14.4. O Gestor, juntamente com os fiscais, deverá acompanhar a prestação dos serviços, registrar as ocorrências e determinar as medidas necessárias ao fiel cumprimento do contrato, bem como atestar, no todo ou em parte, a realização dos serviços objeto deste contrato.

14.5. O atesto dos serviços prestados pela CONTRATANTE para pagamento da nota fiscal não exime a plena responsabilidade da CONTRATADA em garantir o cumprimento total e satisfatório do contrato em conformidade com as especificações estabelecidas quando da contratação.

14.6. O descumprimento total ou parcial das responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste contrato.

15. ALTERAÇÕES CONTRATUAIS

15.1. As alterações das obrigações estabelecidas neste contrato deverão ser formalizadas por meio da lavratura de Termo Aditivo, mediante acordo entre as partes, e em conformidade com os preços e condições vigentes.

15.2. Na hipótese de alteração das condições econômicas fundamentais prevalecentes na assinatura deste contrato, as partes ajustarão as cláusulas que assegurarão a recuperação dos valores ora contratados, objetivando a manutenção do equilíbrio econômico-financeiro do contrato.

15.3. A CONTRATADA deverá comunicar à CONTRATANTE quaisquer alterações em seu Contrato Social, razão ou denominação social, objeto, CNPJ e outros e ainda seus dados bancários, endereços, telefones, fax, e demais dados que, porventura, venham interferir na alteração da habilitação e qualificação exigidas para a execução das obrigações contratuais.

16. DO REEQUILÍBRIO CONTRATUAL

16.1. Na hipótese de ocorrência de fatos supervenientes que alterem substancialmente os encargos pactuados, inclusive em decorrência de modificações na legislação tributária que impactem direta ou indiretamente os custos da execução contratual, será assegurado o direito à revisão contratual, mediante requerimento fundamentado e comprovação do desequilíbrio.

16.2. O pedido de revisão deverá ser formalizado durante a vigência do contrato e será decidido pela FHE no prazo de até 90 (noventa) dias, prorrogável por igual período, conforme previsto na legislação aplicável, acompanhados de toda a documentação comprobatória pertinente, que demonstrem de forma clara e inequívoca, incluindo:

16.2.1. O fundamento legal que deu origem ao pleito;

16.2.2. O demonstrativo econômico-financeiro do impacto direto e quantificável das alterações fáticas e/ou normativas na estrutura de custos e/ou receitas do Contrato;

16.2.3. Apresentação de valores e percentuais que justifiquem a necessidade de revisão contratual;

16.2.4. O período em que o impacto se torna mensurável e efetivo.

16.3. Qualquer alteração no Contrato decorrente do reequilíbrio econômico-financeiro deverá ser formalizada por meio de Termo Aditivo, devidamente assinado pelas Partes.

16.4. O pleito de reequilíbrio e as negociações subsequentes não suspenderão a execução do Contrato, que deverá prosseguir em seus termos originais até que o Termo Aditivo de reequilíbrio seja formalizado ou a controvérsia seja definitivamente resolvida.

16.5. A FHE poderá, de ofício, promover a revisão contratual nos casos em que se verificar redução da carga tributária, desde que garantido o contraditório e a ampla defesa.

16.6. A revisão poderá resultar em: a) Reajuste dos valores contratados; b) Alteração de prazos ou condições de execução; c) Outras medidas compensatórias que restabeleçam o equilíbrio econômico-financeiro.

17. RESILIÇÃO DO CONTRATO

17.1. Independentemente de justificativa e sem que caiba qualquer indenização à outra parte, este contrato poderá ser denunciado a qualquer tempo, pela CONTRATANTE ou pela CONTRATADA, mediante comunicação feita por escrito e com antecedência mínima de 30 (trinta) dias.

18. PENALIDADES

18.1. O inadimplemento total ou parcial das obrigações contratuais dá, à CONTRATANTE, o direito de aplicar as seguintes penalidades:

18.1.1. advertência, quando constatadas pequenas irregularidades que não cause grave dano à CONTRATANTE;

18.1.2. multa, que poderá ser aplicada por descumprimento de quaisquer das obrigações contratuais, calculada em percentual de 0,5% a 30% sobre o valor total do contrato, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, ou descontada das parcelas devidas à CONTRATADA, sem prejuízo de outras sanções previstas contratualmente;

18.1.3. resolução unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais;

18.1.4. os casos de descumprimento das entregas mínimas aceitáveis, serão enquadrados como inexecução parcial do instrumento contratual.

18.1.5. em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstâncias do caso específico.

18.1.6. as multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

18.1.7. não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

18.1.8. sendo resolvido o presente contrato, o pagamento devido será proporcional aos serviços prestados até a data da resolução.

18.1.9. para se ressarcir de eventuais prejuízos causados pela CONTRATADA e do valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar esses valores dos créditos decorrentes deste mesmo contrato ou de outros contratos que a CONTRATADA possua com a CONTRATANTE.

18.1.10. caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA.

18.1.11. no processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

19. VIGÊNCIA

19.1. O presente contrato terá vigência desde a data de sua assinatura e vigorará até ___ de _____ de 20__.

20. CONDIÇÕES GERAIS

20.1. Este contrato e a Proposta Técnica e Comercial constituem a totalidade do acordo entre os signatários com relação às matérias aqui previstas e superam, substituem e revogam os entendimentos, negociações e acordos anteriores.

20.2. Em caso de divergências entre a proposta da CONTRATADA e este instrumento fica desde já acordado que prevalecerão as condições estabelecidas neste contrato.

20.3. Não valerá como precedente, novação, ou renúncia aos direitos que a lei e o presente instrumento asseguram a CONTRATANTE, sua tolerância a eventuais descumprimentos de cláusulas, seus itens e subitens, pela CONTRATADA.

21. FORO

21.1. As partes elegem o Foro da Circunscrição Judiciária de Brasília para dirimir quaisquer questões oriundas do presente contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

Nos termos do disposto no art. 107 do Código Civil; art. 3º, da Lei nº 13.874, de 2019; e Decreto nº 10.278, de 2020, as partes e testemunhas, quando for o caso, declaram a autoria, integridade e confiabilidade deste contrato, acordando, assim, em não contestar a sua validade, conteúdo e autenticidade. E, por estarem justos e acertados, as partes concordam que o presente instrumento contratual será assinado digitalmente, bem como os demais documentos correlatos, sendo as assinaturas válidas, vinculantes e executáveis. Admite-se qualquer modalidade de assinatura eletrônica prevista em lei, quando a integridade dessas for conferida por provedor de assinatura, nos termos da Lei nº 14.620, de 2023.

Brasília-DF, de de 2025.

CONTRATANTE	CONTRATADA

TESTEMUNHAS:

Nome:	Nome: