ANEXO XI - INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. FINALIDADE

Este anexo estabelece os requisitos mínimos de segurança da informação, confidencialidade e responsabilidade aplicáveis aos profissionais contratados que possuam acesso aos ambientes, sistemas, informações ou recursos tecnológicos do CONTRATANTE.

O objetivo é garantir a proteção dos ativos, informações e serviços do CONTRATANTE durante toda a vigência da prestação de serviços.

2. INFRAESTRUTURA PARA REALIZAÇÃO DOS SERVIÇOS

2.1. O acesso aos ambientes, sistemas e recursos tecnológicos do CONTRATANTE será concedido exclusivamente para execução das atividades previstas no escopo contratual, observando os princípios de necessidade, rastreabilidade e menor privilégio.

2.2. O acesso remoto aos ambientes do CONTRATANTE deverá ocorrer exclusivamente por meio de conexão segura VPN *Client-to-Site*, utilizando mecanismos de autenticação e controles de segurança definidos pelo CONTRATANTE.

2.3. O profissional contratado deverá utilizar credenciais de acesso individuais, pessoais e intransferíveis, sendo expressamente proibido o compartilhamento, reutilização ou cessão de acessos a terceiros.

2.4. Todo acesso remoto aos ambientes do CONTRATANTE deverá obrigatoriamente utilizar autenticação multifator (MFA), conforme padrões de segurança estabelecidos pelo CONTRATANTE.

2.5. O CONTRATANTE poderá, a qualquer tempo e sem aviso prévio, monitorar, registrar, auditar, revisar, restringir, suspender ou revogar acessos concedidos, sempre que identificar necessidade operacional, risco de segurança ou descumprimento das diretrizes estabelecidas.

2.6. Os ambientes, sistemas e recursos disponibilizados pelo CONTRATANTE deverão ser utilizados exclusivamente para fins profissionais relacionados à execução das atividades contratadas, sendo vedada qualquer utilização diversa da finalidade autorizada.

2.7. O acesso concedido não caracteriza autorização irrestrita aos ambientes do CONTRATANTE, permanecendo limitado exclusivamente aos recursos, sistemas, informações e permissões necessárias à execução das atividades previstas contratualmente.

3. ACESSO A INFRAESTRUTURA PARA REALIZAÇÃO DOS SERVIÇOS

3.1. Os dispositivos utilizados para acesso aos ambientes, sistemas e recursos tecnológicos do CONTRATANTE deverão atender aos requisitos mínimos de segurança estabelecidos pelo CONTRATANTE, incluindo, obrigatoriamente:

3.2. Sistema operacional em versão suportada pelo fabricante e devidamente atualizado;
3.3. Solução de antivírus e/ou EDR ativa, operacional e atualizada;
3.4. Firewall local habilitado, caso não seja gerenciado por solução de antivírus/EDR;
3.5. Aplicação regular de atualizações e correções de segurança;

Este documento está classificado como: Interno

3.6. Fica expressamente proibida a instalação, utilização ou execução de softwares, ferramentas, serviços, extensões, plugins, agentes ou mecanismos de acesso remoto não autorizados pelo CONTRATANTE, incluindo AnyDesk, TeamViewer, RustDesk, VNC e similares, bem como quaisquer recursos tecnológicos não homologados nos ambientes, dispositivos ou ativos disponibilizados para a prestação dos serviços, sujeitando a CONTRATADA às medidas contratuais cabíveis e à responsabilização por eventuais incidentes, impactos ou danos decorrentes do uso não autorizado.

3.7. Será disponibilizado um segmento de rede específico para acesso remoto pelos profissionais da CONTRATADA alocados aos serviços, denominado Extranet de Acesso Remoto, conforme abaixo.

3.7.1. Na Extranet de Acesso Remoto serão disponibilizados desktops remotos de trabalho a serem usados pelos colaboradores da CONTRATADA para realização dos serviços.

3.7.2. A solicitação da(s) credencial (is) de acesso deverá ser feita através da FERRAMENTA DE CONTROLE.

3.8. O acesso aos ambientes do CONTRATANTE deverá ocorrer exclusivamente por meio dos mecanismos, canais e soluções de acesso remoto autorizados, incluindo conexão VPN *Client-to-Site* disponibilizada ou homologada pelo CONTRATANTE.

3.9. É vedada a utilização de conexões paralelas, *proxies* externos, túneis não autorizados, ferramentas de redirecionamento de tráfego ou quaisquer mecanismos que comprometam a rastreabilidade, monitoramento ou segurança da conexão estabelecida com o CONTRATANTE.

3.10. O CONTRATANTE poderá realizar verificações, monitoramentos e validações de conformidade dos dispositivos e conexões utilizados no acesso aos seus ambientes, podendo restringir ou bloquear acessos em caso de identificação de não conformidades ou riscos de segurança.

3.11. Os dispositivos utilizados para acesso aos ambientes, sistemas e informações do CONTRATANTE deverão possuir mecanismos de criptografia habilitados para proteção dos dados armazenados, incluindo, no mínimo, criptografia de disco completo ou tecnologia equivalente compatível com as boas práticas de segurança da informação.

3.11.1. A solução de criptografia utilizada deverá estar ativa, configurada adequadamente e protegida contra desativação não autorizada.

3.11.2. O CONTRATANTE poderá solicitar evidências da implementação dos mecanismos de criptografia nos dispositivos utilizados na prestação dos serviços.

3.11.3. A ausência de criptografia ou a utilização inadequada dos mecanismos de proteção poderá resultar na restrição, suspensão ou bloqueio do acesso aos ambientes do CONTRATANTE.

Este documento está classificado como: Interno

4. CONFIDENCIALIDADE E PROTEÇÃO DAS INFORMAÇÕES

4.1. Todas as informações, dados, documentos, credenciais, registros, sistemas e demais ativos acessados durante a execução das atividades deverão ser tratados como confidenciais, independentemente do meio, formato ou classificação da informação.

4.2. Fica expressamente proibido:

4.3. Compartilhar, divulgar ou disponibilizar informações do CONTRATANTE a pessoas não autorizadas;
4.4. Realizar cópia, extração, reprodução ou armazenamento indevido de informações corporativas;
4.5. Armazenar informações do CONTRATANTE em dispositivos, repositórios, aplicações ou serviços pessoais não autorizados;
4.6. Utilizar informações, dados ou recursos do CONTRATANTE para finalidades particulares ou distintas do escopo contratual;
4.7. Remover, transferir ou transmitir informações corporativas sem autorização formal do CONTRATANTE.

4.8. A CONTRATADA compromete-se a cumprir integralmente as diretrizes, normas e controles relacionados à segurança da informação, privacidade, proteção de dados e uso adequado dos recursos tecnológicos definidos pelo CONTRATANTE.

4.9. **SEGURANÇA DA INFORMAÇÃO**

4.10. A CONTRATADA compromete-se a adotar e manter controles, procedimentos e boas práticas de segurança da informação adequados à proteção dos ambientes, sistemas, dados e ativos do CONTRATANTE, garantindo a confidencialidade, integridade, disponibilidade e rastreabilidade das informações acessadas durante a execução contratual.

4.11. A CONTRATADA deverá assegurar que os profissionais envolvidos na prestação dos serviços observem integralmente as diretrizes, normas e controles de segurança definidos pelo CONTRATANTE, incluindo requisitos relacionados a controle de acesso, proteção de dados, uso adequado dos recursos tecnológicos, prevenção de incidentes e confidencialidade das informações.

4.12. CONTRATADA deverá garantir que os profissionais alocados possuam conhecimento técnico e estejam capacitados para aplicar práticas de desenvolvimento seguro, incluindo controle de versões, gestão de mudanças, revisão de código, tratamento de vulnerabilidades conhecidas, gestão de dependências e testes de segurança, de forma compatível com o escopo e o nível de risco dos serviços prestados ao CONTRATANTE.

4.13. A CONTRATADA será responsável por comunicar imediatamente ao CONTRATANTE qualquer incidente, suspeita de incidente, acesso indevido, vazamento de informação ou evento que possa representar risco à segurança dos ambientes, sistemas ou dados do CONTRATANTE.

4.14. Todos os códigos-fonte, scripts, integrações, parametrizações, documentações, customizações e demais entregáveis desenvolvidos pela CONTRATADA no âmbito deste contrato serão de titularidade do CONTRATANTE, ficando cedidos, em caráter definitivo, os respectivos direitos patrimoniais de propriedade intelectual, ressalvados softwares, frameworks, bibliotecas e componentes preexistentes de titularidade da CONTRATADA ou de terceiros.

4.15. A CONTRATADA compromete-se a não reutilizar, divulgar ou disponibilizar a terceiros os entregáveis desenvolvidos especificamente para o CONTRATANTE sem autorização formal

Este documento está classificado como: Interno

deste, bem como a assegurar que quaisquer componentes de terceiros utilizados na execução contratual estejam em conformidade com suas respectivas licenças de uso.

4.16. O descumprimento das obrigações de segurança da informação previstas neste contrato poderá resultar na aplicação de medidas administrativas, suspensão de acessos, rescisão contratual e responsabilização civil e criminal, sem prejuízo das demais medidas cabíveis.

4.17. **GESTÃO DE RISCO DE TERCEIROS**

4.18. A CONTRATADA estará sujeita ao processo de Gestão de Risco de Terceiros do CONTRATANTE, comprometendo-se a atender integralmente às políticas, normas e procedimentos estabelecidos para avaliação, monitoramento e mitigação de riscos associados à prestação dos serviços.

4.19. A CONTRATADA deverá fornecer, sempre que solicitado, informações completas, atualizadas e verídicas sobre seus controles internos, processos e práticas de segurança.

4.20. O CONTRATANTE poderá, a qualquer tempo, realizar ou requerer avaliações nos ambientes, processos, ferramentas e recursos utilizados pela CONTRATADA na prestação de serviços de desenvolvimento, sustentação, testes, integração e manutenção de software, incluindo ambientes de desenvolvimento, homologação, ferramentas de versionamento, *pipelines* de CI/CD e possíveis integrações com sistemas do CONTRATANTE.

4.21. O CONTRATANTE poderá classificar o nível de risco da CONTRATADA, podendo exigir controles adicionais conforme a criticidade dos serviços prestados.

4.22. A CONTRATADA será submetida a processo de *due diligence* prévia à contratação, bem como a avaliações periódicas, realizadas, no mínimo, anualmente, ao longo da vigência contratual. Referido processo poderá incluir, mas não se limitando, ao preenchimento de questionários de avaliação de segurança da informação, acompanhado do envio de evidências comprobatórias das respostas apresentadas, tais como documentos técnicos, relatórios de auditoria independente, políticas e normativos internos, certificações ou materiais equivalentes que demonstrem a efetiva implementação dos controles declarados. Caso seja exigido o envio de relatório de auditoria independente, os custos decorrentes de sua elaboração, emissão ou obtenção serão de responsabilidade exclusiva da CONTRATADA.

4.23. A recusa ou atraso injustificado no fornecimento de informações poderá ser caracterizada como descumprimento contratual.

4.24. O CONTRATANTE poderá realizar, durante a vigência contratual, avaliações periódicas de risco relacionadas à CONTRATADA e aos serviços prestados, incluindo análise de segurança, verificação de controles aplicáveis, revalidação de informações e evidências, bem como o monitoramento de exposições que possam impactar a confidencialidade, integridade, disponibilidade ou demais requisitos de segurança da informação relacionados ao objeto contratado.

4.25. A CONTRATADA deverá adotar controles para gestão de riscos associados a seus profissionais alocados nas dependências do CONTRATANTE ou em regime remoto. Previamente à alocação de qualquer profissional, a CONTRATADA deverá realizar processo formal de verificação de antecedentes, idoneidade e qualificação, incluindo, no mínimo:

4.25.1. Verificação de antecedentes criminais por meio de certidões ou consultas a bases oficiais, em conformidade com a legislação vigente;

Este documento está classificado como: Interno

4.25.2. Confirmação de vínculos empregatícios e histórico profissional;

4.25.3. Verificação de eventuais restrições em listas de sanções, impedimentos regulatórios ou vedações aplicáveis, especialmente no âmbito do setor financeiro.

4.26. Adicionalmente, a CONTRATADA deverá assegurar a implementação de controles contínuos, incluindo:

4.26.1. Segregação adequada de funções, de forma a evitar conflitos de interesse e acessos indevidos;

4.26.2. Capacitação em segurança da informação e treinamentos periódicos de conscientização;

4.26.3. Formalização das responsabilidades dos profissionais quanto à proteção dos ativos e das informações do CONTRATANTE.

4.27. A CONTRATADA deverá emitir declaração formal de conformidade, atestando que os profissionais alocados foram devidamente submetidos aos procedimentos de verificação e que não apresentam impedimentos relevantes para o desempenho das atividades contratadas, permanecendo responsável por eventuais omissões, inconsistências ou falsidades.

4.28. O processo de verificação deverá ser renovado sempre que houver substituição de profissional ou, para profissionais em alocação contínua, no mínimo a cada 24 (vinte e quatro) meses.

4.29. O CONTRATANTE poderá, mediante justificativa fundamentada em risco de segurança, solicitar a substituição de qualquer profissional da CONTRATADA, sem necessidade de divulgação dos motivos específicos, cabendo à CONTRATADA promover a substituição no prazo acordado.

4.30. O acesso dos profissionais da CONTRATADA aos ambientes, sistemas, ferramentas e repositórios do CONTRATANTE será concedido com base no princípio do menor privilégio, limitado ao estritamente necessário para execução dos serviços, e revisto periodicamente ou sempre que houver mudanças na alocação ou no escopo das atividades.

4.31. A CONTRATADA deverá comunicar imediatamente quaisquer alterações relevantes que impactem seu perfil de risco, incluindo mudanças estruturais, tecnológicas ou organizacionais, além de alterações relacionadas à composição, alocação, substituição, perfil de acesso ou modelo de trabalho dos profissionais envolvidos na execução dos serviços (presencial ou remoto).

4.32. Nos casos em que os serviços forem executados de forma remota, a CONTRATADA deverá utilizar exclusivamente os meios de acesso autorizados pelo CONTRATANTE, observando requisitos de segurança de rede, criptografia, autenticação forte e proteção de estações de trabalho utilizadas no acesso aos ambientes do CONTRATANTE.

4.33. Os dispositivos utilizados pela CONTRATADA para executar atividades nos ambientes, sistemas e ferramentas disponibilizadas pelo CONTRATANTE deverão ser passíveis de rastreabilidade adequada das ações realizadas, por meio de registros e logs compatíveis com os controles de segurança adotados pelo CONTRATANTE, sem prejuízo ao desempenho e à confidencialidade das informações.

4.34. Durante a vigência do contrato, a CONTRATADA não poderá subcontratar, total ou parcialmente, atividades relacionadas ao objeto deste contrato sem autorização prévia e

Este documento está classificado como: Interno

expressa do CONTRATANTE.

4.35. Em caso de subcontratação autorizada pelo CONTRATANTE, a CONTRATADA permanecerá integralmente responsável pelas obrigações assumidas neste contrato, bem como deverá garantir que o subcontratado atenda aos mesmos requisitos de segurança, conformidade e gestão de riscos.

4.36. A CONTRATADA deverá adotar medidas para mitigar riscos de descontinuidade dos serviços decorrentes de indisponibilidade de profissionais-chave, garantindo mecanismos adequados de transferência de conhecimento e substituição de recursos sem impacto relevante à execução contratual.

4.37. A CONTRATADA deverá comunicar ao CONTRATANTE qualquer incidente, suspeita de incidente ou evento que possa representar risco à operação, aos dados ou aos serviços contratados, cabendo o envio detalhado sobre o incidente e as medidas corretivas e preventivas adotadas.

4.38. Caso sejam identificados riscos relevantes, a CONTRATADA deverá elaborar e executar plano de ação para mitigação que deverá conter a descrição do risco, ações corretivas, prazos definidos e responsáveis pela execução. O CONTRATANTE poderá acompanhar e validar a efetividade das ações implementadas.

4.39. O CONTRATANTE poderá rescindir o contrato, sem ônus, nos casos em que identifique que a CONTRATADA apresente risco elevado não mitigado, haja descumprimento recorrente de requisitos de gestão de risco ou seja identificada omissão ou falsidade de informações relevantes.

4.40. Ao término ou rescisão do contrato, por qualquer motivo, a CONTRATADA deverá adotar todas as medidas necessárias para garantir a adequada mitigação dos riscos decorrentes da descontinuidade da prestação dos serviços, assegurando a integridade, confidencialidade e disponibilidade das informações e ativos do CONTRATANTE.

4.41. A CONTRATADA compromete-se a cooperar integralmente com o processo de transição ou encerramento dos serviços, incluindo a transferência ordenada de conhecimentos e documentações necessários à continuidade operacional do CONTRATANTE ou de terceiros por ela indicados.

4.42. A CONTRATADA deverá, no prazo estabelecido pelo CONTRATANTE:

4.42.1. Disponibilizar todos os dados, informações e demais ativos relacionados ao objeto contratual, em formato estruturado, íntegro e utilizável;

4.42.2. Descartar, de forma segura e irreversível, quaisquer cópias remanescentes ou ativo de informação sob sua guarda que contenham dados pertencentes ao CONTRATANTE, no fim do ciclo de vida da informação ou quando considerados desnecessários à execução contratual;

4.42.3. Apresentar evidências formais da transferência e/ou eliminação dos dados e informações.

4.43. A CONTRATADA deverá revogar, imediatamente após o encerramento do contrato, todos os acessos lógicos e físicos relacionados aos ambientes do CONTRATANTE, garantindo que não subsistam credenciais ativas ou permissões indevidas.

Este documento está classificado como: Interno

4.44. Permanecem vigentes, mesmo após o término do Contrato, as obrigações relacionadas à confidencialidade, proteção de dados, segurança da informação e responsabilidade por incidentes ocorridos durante a vigência contratual.

Este documento está classificado como: Interno