ANEXO II - REQUISITOS MÍNIMOS DE SEGURANÇA PARA SISTEMAS ADQUIRIDOS

1. REQUISITOS GERAIS DE SEGURANÇA PARA A CONTRATADA

1.1. A contratada deverá assinar, no início do contrato, o Termo de Confidencialidade e Sigilo que terá como objetivo definir as regras relativas ao tratamento, acesso, proteção e revelação das informações corporativas do Banco da Amazônia.

1.2. Todos os empregados da empresa contratada que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato deverão assinar o Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado. O referido termo deverá ser entregue ao gestor do contrato antes do início das atividades do profissional.

1.3. A contratada deverá:

1.3.1. adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do BANCO DA AMAZÔNIA;

1.3.2. comunicar com antecedência mínima de 15 (quinze) dias ao BANCO DA AMAZÔNIA qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do BANCO DA AMAZÔNIA, porventura colocados à disposição para realização dos serviços contratados;

1.3.3. manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo BANCO DA AMAZÔNIA a tais documentos;

1.3.4. não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do BANCO DA AMAZÔNIA, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;

1.3.5. manter seus empregados devidamente informados das normas disciplinares do BANCO DA AMAZÔNIA, bem como das normas de utilização e de segurança das instalações e do manuseio dos documentos;

1.3.6. manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do BANCO DA AMAZÔNIA;

1.3.7. garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do Banco da Amazônia;

1.3.8. assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;

1.3.9. assumir inteira responsabilidade por quaisquer danos ou prejuízos causados ao BANCO DA AMAZÔNIA e a terceiros, incluindo prejuízos financeiros, por dolo ou culpa, de seus empregados, decorrentes dos serviços ora contratados;

1.3.10. garantir e manter total e absoluto sigilo sobre as informações manuseadas as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;

1.3.11. não repassar a terceiros, em nenhuma hipótese, qualquer informação sobre a arquitetura e/ou documentação, assim como dados e/ou metadados trafegados, produtos desenvolvidos e entregues, ficando responsável juntamente com o BANCO DA AMAZÔNIA por manter a segurança da informação relativa aos dados e procedimentos durante a execução das atividades e em período posterior ao término da execução do contrato;

1.3.12. assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BANCO DA AMAZÔNIA através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado;

1.3.13. providenciar para que os produtos e artefatos da contratação sejam entregues em perfeito estado, com a segurança necessária, garantindo o transporte, o seguro, a entrega e a implantação nos locais indicados pelo BANCO DA AMAZÔNIA sem quaisquer danos, avarias ou ônus adicionais para o BANCO DA AMAZÔNIA.

2. COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM

2.1. A contratada deve garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo que o BANCO DA AMAZÔNIA tenha todas as garantias legais enquanto tomador do serviço e proprietário das informações, se hospedadas na nuvem.

2.2. A contratada deverá:

2.2.1. cumprir integralmente as diretrizes da Resolução CMN 4.893/21;

2.2.2. fornecer acesso ao BANCO DA AMAZÔNIA aos dados e às informações a serem processados ou armazenados pela empresa contratada;

2.2.3. assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador;

2.2.4. apresentar conformidade com a norma ABNT NBR ISO/IEC 27001:2013 referente aos serviços de computação em nuvem e aos data centers que hospedem esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao BANCO DA AMAZÔNIA promover diligência destinada a esclarecer ou complementar informações;

2.2.5. fornecer ao BANCO DA AMAZÔNIA acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e aos controles utilizados na execução dos serviços a serem contratados;

2.2.6. fornecer informações e recursos de gestão para possibilitar o monitoramento dos serviços a serem prestados;

2.2.7. assegurar, enquanto o contrato estiver vigente, a identificação e a segregação dos dados dos clientes do BANCO DA AMAZÔNIA por meio de controles físicos ou lógicos e forneça ao BANCO DA AMAZÔNIA documentos e/ou relatórios que evidenciem o cumprimento desta exigência;

2.2.8. assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do BANCO DA AMAZÔNIA;

2.2.9. adotar um padrão de identidade federada para permitir o uso de tecnologia single sign-on no processo de autenticação dos usuários do serviço de nuvem, o qual deve ser acompanhado de autenticação multifator (MFA).

2.2.10. registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.

2.2.11. apoiar o BANCO DA AMAZÔNIA, quando necessário, nas atividades de investigação de incidentes de cibersegurança. Isso inclui fornecer prontamente informações e recursos necessários para a investigação, como logs, registros de eventos e relatórios de auditoria.

2.2.12. adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, caso o serviço a ser contratado seja relativo ao serviço de execução de aplicação por meio da internet;

2.2.13. garantir que o ambiente seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados por outros usuários do serviço em nuvem;

2.2.14. assegurar que toda atualização do sistema seja previamente analisada e homologada antes que possa ser instalada/configurada, além de dispor de documentação de todas

as alterações realizadas no serviço e/ou sistema mediante processos formalizados de Gestão e Mudanças;

2.2.15. assegurar a adoção de medidas de segurança para a transmissão e armazenamento dos dados e das informações processados ou armazenados pelo prestador, e fornecer ao BANCO DA AMAZÔNIA evidências da adoção das referidas medidas;

2.2.16. notificar ao BANCO DA AMAZÔNIA sobre a subcontratação de serviços relevantes para a prestação do serviço contratado;

2.2.17. notificar ao BANCO DA AMAZÔNIA sobre a intenção de interromper a prestação de serviços com pelo menos trinta dias de antecedência da data prevista para a interrupção;

2.2.18. conceder o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

2.2.19. manter o BANCO DA AMAZÔNIA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

2.2.20. dispor de Plano de Comunicação de Incidentes e/ou dashboards com informações referentes a saúde dos serviços oferecidos de incidentes que possam ocorrer, informando o BANCO DA AMAZÔNIA os casos de incidentes de segurança da informação, assim considerados os eventos não previstos ou não desejados que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do BANCO DA AMAZÔNIA;

2.2.21. realizar a análise e gestão de riscos de segurança de informação. A análise deve ter periodicidade no mínimo mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes;

2.2.22. possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção;

2.2.23. desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços ou envolvendo dados pessoais de empregados e/ou clientes do BANCO DA AMAZÔNIA;

2.2.24. realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) e auditorias por terceira parte reconhecidamente confiável, disponibilizando relatório comprobatório a cada três meses para o BANCO DA AMAZÔNIA;

2.2.25. prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;

2.2.26. deverá fornecer, sempre que solicitado pelo BANCO DA AMAZÔNIA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de Application Programming Interface (API), caso haja, para análise de segurança e auditorias;

2.2.27. dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do BANCO DA AMAZÔNIA, incluindo os seguintes itens: solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações), solução de prevenção e detecção de intrusão (IDS/IPS), antivírus, anti-malware, solução anti-DDoS, solução de gestão de logs, solução de gestão integrada de pacotes de correção (patches), solução de correlação de eventos de segurança (SIEM);

2.2.28. realizar backups e salvaguardas dos conteúdos das comunicações realizadas por meio da solução e permitir a consulta desses dados;

2.2.29. garantir a exclusividade de direitos, por parte do BANCO DA AMAZÔNIA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança.

2.2.30. comprometer-se a preservar os dados do BANCO DA AMAZÔNIA contra acessos indevidos e abster-se de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente ao BANCO DA AMAZÔNIA qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados;

2.2.31. operar o serviço dentro do uso proposto, com desempenho razoável e exigindo o mínimo possível de permissões dos demais sistemas do BANCO DA AMAZÔNIA, além de proteger os dados transmitidos por meio dele, quando necessário;

2.2.32. atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:

a) as diretrizes de tratamento;
b) o modo de atendimento a solicitações de titulares de dados pessoais;
c) as medidas protetivas para garantia da confidencialidade dos dados pessoais;
d) as medidas protetivas durante as comunicações com o BANCO DA AMAZÔNIA;
e) o registro de atividades de tratamento de dados pessoais;
f) a solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;
g) a medidas de devolução / descarte dos dados.

2.3. A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:

a) inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;
b) inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
c) não fornecimento a terceiros de dados do BANCO DA AMAZÔNIA, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
d) fornecer ao BANCO DA AMAZÔNIA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BANCO DA AMAZÔNIA.

2.4. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo BANCO DA AMAZÔNIA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se que:

2.4.1. pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

2.4.2. a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, desde que em conformidade com a Resolução CMN 4.893/21.

2.5. A empresa deve garantir a adequação e a adoção de medidas pelo BANCO DA AMAZÔNIA, em decorrência de qualquer determinação do Órgãos Governamentais aos quais o BANCO DA AMAZÔNIA é subordinado que impacte sobre o Contrato vigente.

2.6. A empresa deve manter o BANCO DA AMAZÔNIA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

2.7. É vedado o uso de informações do BANCO DA AMAZÔNIA pela contratada para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

2.8. Em caso de extinção do contrato, a contratada deverá transferir os dados e as informações processados ou armazenados por ele ao novo prestador de serviços ou ao BANCO DA AMAZÔNIA e, após a confirmação da integridade e da disponibilidade dos dados e informações recebidos, os excluir.

2.9. Em caso da decretação de regime de resolução do Banco da Amazônia pelo Banco Central do Brasil, a contratada deverá:

2.9.1. conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações que estejam em poder da empresa contratada; e

2.9.2. notificar previamente o responsável pelo regime de resolução sobre sua a intenção de interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção. A contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

3. REQUISITOS DE ARQUITETURA, DESIGN E MODELAGEM DE AMEAÇAS

3.1. O sistema, com recursos web, deverá incorporar, no mínimo, proteção contra:

3.1.1. **Controle de acesso falho:** as restrições sobre o que os usuários autenticados têm permissão para fazer muitas vezes não são aplicadas de forma adequada. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

3.1.2. **Falhas criptográficas:** Muitos aplicativos da web e APIs não protegem adequadamente os dados sigilosos, como dados pessoais e financeiros. Os invasores podem roubar ou modificar esses dados fracamente protegidos para conduzir fraude de cartão de crédito, roubo de identidade ou outros crimes. Os dados sigilosos podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requerem precauções especiais quando trocados com o navegador.

3.1.3. **Injeção:** Injeções ocorrem quando dados informados pelo usuário são enviados para um interpretador como parte de um comando ou uma query. O dado malicioso do atacante faz o interpretador executar comandos que não deveria ou modificar dados. Algumas das injeções mais comuns são SQL, NoSQL, OS command, Mapeamento Relacional de Objeto (ORM), LDAP e Expression Language (EL) ou Object Graph Navigation Library (OGNL). O conceito é idêntico entre todos. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções.

3.1.4. **Design inseguro:** O design seguro é uma cultura e metodologia que avalia constantemente as ameaças e garante que o código seja desenvolvido e testado de forma robusta para evitar métodos de ataque conhecidos. O design seguro requer um ciclo de vida de desenvolvimento seguro, alguma forma de padrão de design seguro ou biblioteca ou ferramenta de componentes de estradas pavimentadas e modelagem de ameaças.

3.1.5. **Configuração incorreta de segurança:** geralmente é o resultado de configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas também devem ser corrigidos / atualizados em tempo hábil.

3.1.6. **Componentes vulneráveis e desatualizados:** componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios do aplicativo. Se um componente vulnerável for explorado, esse tipo de ataque pode facilitar a perda séria de dados ou o controle do servidor. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas do aplicativo e permitir vários ataques e impactos.

3.1.7. **Falhas de identificação e autenticação:** as funções do aplicativo relacionadas à autenticação e gerenciamento de sessão são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários temporária ou permanentemente.

3.1.8. **Falhas de software e integridade de dados:** As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Por exemplo, quando objetos ou dados são codificados ou serializados em uma estrutura que um invasor pode ver e modificar, logo é vulnerável à desserialização insegura. Outro exemplo é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs).

3.1.9. **Registro (logging) e monitoramento insuficientes:** registro (logging) e monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permite que os invasores ataquem ainda mais os sistemas, mantenham a persistência, ganhem acesso em mais sistemas e adulterem, extraiam ou destruam dados.

3.1.10. **Server-Side Request Forgery (SSRF):** As falhas de SSRF ocorrem sempre que um aplicativo web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de ACL de rede.

3.1.11. **Validação de entrada inadequada:** o produto recebe entradas ou dados, mas não valida ou valida incorretamente se a entrada possui as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado pela aplicação.

3.1.12. **Caracteres Especiais ou maliciosos:** caracteres especiais são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros. Garanta que apenas entradas válidas, esperadas e apropriadas sejam processadas pelo Sistema.

3.2. A solução deverá possuir conformidade com o OWASP TOP 10 vigente visando assegurar a segurança dos dados, gerar confiança entre os usuários, prevenir perdas financeiras e cumprir regulamentações de segurança, proporcionando a integridade e a credibilidade necessárias para um site ou aplicativo.

3.3. A solução não deve ser baseada nos frameworks Wordpress ou Joomla.

3.4. Deverá ser imposto o menor privilégio em conexões com o banco de dados ou outros sistemas de back-end.

3.5. A Contratada deverá realizar configuração segura (hardening) do servidor web no qual a aplicação está hospedada e deverá assegurar que servidores web da aplicação estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmark mais atual.

3.6. As seguintes flags e procedimentos relacionados deverão ser adotados em relação às configurações do cabeçalho para a comunicação entre o servidor e o cliente:

3.6.1. A aplicação deverá instruir o browser a só permitir acesso via HTTPS. Deverá ser ativado o HTTP Strict Transport Security (HSTS) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. O max-age deve ser de pelo menos 31536000 segundos (1 ano);

3.6.2. O cabeçalho X-Content-Type-Options deverá estar configurado como 'nosniff' para todas as páginas da web;

3.6.3. A aplicação deverá retornar o cabeçalho X-Frame-Options com o valor DENY ou SAMEORIGIN, que permitirá “framing” das páginas conforme SAME ORIGIN;

3.6.4. A aplicação deverá ter o CSP habilitado enviando os cabeçalhos de resposta Content-Security-Policy, conforme políticas que atenda critérios de segurança na implementação dessa diretiva;

3.6.5. A aplicação deverá ter o cabeçalho X-XSS-Protection desabilitado, por meio da configuração do seu valor como 0 (zero);

3.6.6. A aplicação não deverá possuir os cabeçalhos “fingerprinting”: X-Powered-By, Server, X-AspNet-Version;

3.6.7. A aplicação deverá forçar content-type para as respostas. Se a aplicação retorna json, a resposta content-type da aplicação deverá ser application/json;

3.6.8. Os tipos de conteúdo text/ *, / + xml e application/xml também devem especificar um conjunto de caracteres seguro (por exemplo, UTF-8, ISO-8859-1);

3.6.9. O conteúdo da aplicação não poderá ser incorporado a um site de terceiro por padrão;

3.6.10. O Cross-Origin Resource Sharing (CORS) e cabeçalho Access-Control-Allow-Origin deverão utilizar uma lista de permissão restrita de domínios e subdomínios confiáveis para correspondência e não oferecer suporte à origem "null", e validar os dados inseridos pelo usuário;

3.6.11. O cookie emitido pela aplicação deverá possuir os atributos SameSite, SECURE e HttpOnly;

3.7. A aplicação deverá utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações

3.8. Antes da entrada em produção, a solução passará por homologação quanto a sua segurança. Quaisquer eventuais vulnerabilidades identificadas pela equipe do BANCO DA AMAZÔNIA serão tratadas como defeito de software e deverão obrigatoriamente ser corrigidas pela CONTRATADA.

3.9. Realizar configuração segura do servidor web, também conhecido como hardening. Assegurar que servidores WEB estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmarks.

3.10. Utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.

4. REQUISITOS DE ARMAZENAMENTO DE DADOS E PRIVACIDADE

4.1. Os recursos de armazenamento de credenciais do sistema deverão ser utilizados para armazenar dados restritos e sigilosos, como dados pessoais, credenciais de usuário ou chaves criptográficas

4.2. Dados restritos e sigilosos não deverão:

4.2.1. ser exibidos em mensagens de erro;

4.2.2. ser armazenados fora do contêiner da aplicação ou de recursos de armazenamento de credenciais do sistema;

4.2.3. ser armazenados em texto claro, como um banco de dados não criptografado;

4.2.4. aparecer nos logs de aplicação;

4.2.5. ser compartilhados com terceiros, exceto se for uma parte necessária da arquitetura;

4.2.6. ser expostos através de mecanismos IPC (Inter-process Communication);

4.2.7. ser armazenados localmente ou em arquivos temporários no dispositivo. Em vez disso, os dados deverão ser recuperados de um terminal remoto quando necessário e mantidos apenas em memória.

4.3. A aplicação não deverá exibir mensagens de erro detalhadas que possa expor informações privilegiadas.

4.4. Senhas ou PINs de acesso não deverão ser expostos através da interface de usuário.

4.5. Credenciais de acesso não deverão ser armazenadas dentro do código-fonte do sistema.

4.6. Será obrigatória a validação, a filtragem e o tratamento de todos os dados inseridos pelo usuário.

4.7. Toda requisição de acesso ao banco de dados deverá passar por processo de validação de autorização.

4.8. Será vedada a filtragem de dados no cliente.

4.9. Não deverá ser utilizado o método GET (URLs) para o envio de dados restritos ou sigilosos ou para a realização transações financeiras.

4.10. O método HTTP deverá ser utilizado de acordo com a operação: GET (read), POST (create), PUT/PATCH (replace/update), e DELETE (delete).

4.11. Será proibida a utilização de dados sensíveis (credenciais de acesso, senhas, tokens ou API keys) na URL, deverá ser utilizado cabeçalho Authorization.

4.12. Toda requisição de acesso à API deverá passar por processo de validação de autorização.

4.13. Um mecanismo de validação de entrada padrão deverá ser utilizado para validar todos os dados em tamanho, tipo, sintaxe e regras de negócio antes de exibi-los ou armazená-los.

4.14. Deverá ser utilizada a estratégia de validação do tipo Whitelist.

4.15. Será obrigatória a validação content-type de dados publicados (POST) aceitáveis (por exemplo application/x-www-form-urlencoded, multipart/form-data, application/json etc.).

4.16. Entradas inválidas deverão ser rejeitadas, ao invés de se tentar sanitizar dados impróprios/maliciosos.

5. REQUISITOS DE AUTENTICAÇÃO

5.1. O sistema deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.

5.2. O sistema deve possuir mecanismo de múltiplo fator de autenticação (MFA);

5.3. O sistema deve ser capaz de admitir integração com MS-AD (Microsoft Active Diretory) do BANCO DA AMAZÔNIA para login único de usuário (Single Sign On = SSO).

5.4. As senhas deverão ser gravadas em banco de dados de forma criptografada.

5.5. A tela de log-on não deverá exibir a senha que está sendo informada.

5.6. O sistema não deverá armazenar ou transmitir senhas em texto plano.

5.7. A tela de entrada dos sistemas deverá validar as informações fornecidas pelo usuário somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar qual parte do dado de entrada está correta ou incorreta.

5.8. Em caso de tentativa de log-on inválida, o sistema deverá exibir uma mensagem genérica e nunca exibir as mensagens "usuário inexistente" ou "senha incorreta", de modo a não fornecer mensagens que permitam a um usuário não autorizado deduzir informações de acesso.

5.9. Todo acesso administrativo deverá ser restrito e deverá ser garantido o acesso apenas aos usuários autorizados.

5.10. Deverá ser utilizado HTTPS para envio de credenciais.

5.11. Os sistemas não deverão passar ID de sessão por método HTTP GET.

5.12. Deverá ser utilizado sempre o método HTTP POST para a requisição de autenticação.

5.13. Será obrigatória a utilização do parâmetro “state” com hash aleatório no processo de autenticação do OAuth.

5.14. Será proibido o uso de Basic Authentication.

5.15. As autorizações de acesso deverão ser validadas, garantindo que nenhum usuário acessará o que não foi previamente definido em seu perfil.

5.16. O processo de login deve ser iniciado através de uma página com um novo cookie de sessão.

5.17. Todos os endpoints do sistema deverão ser protegidos por autenticação.

5.18. Será proibido o incremento de IDs automaticamente. No lugar, deverá ser utilizado UUID.

6. REQUISITOS DE GERENCIAMENTO DE SESSÃO DO USUÁRIO

6.1. As sessões deverão ser invalidadas pelo terminal remoto após um período de, no máximo, 15 minutos de inatividade e os tokens de acessos devem expirar.

6.2. O controle de sessão deverá ser tratado pelo servidor e apenas a persistência dele no cliente.

6.3. Os sistemas deverão implementar token de sessão por requisição com alta aleatoriedade, devendo ser utilizados tokens personalizados e aleatórios em todos os formulários e URLs que não serão automaticamente enviadas pelo navegador.

6.4. Toda as páginas deverão ter um link para o logout o qual, ao clicar, o sistema deverá realizar o logout sem antes questionar o usuário. O logout deve destruir todo o estado da sessão no lado servidor e os cookies no lado cliente.

6.5. Será proibido o uso de “response_type=token”.

6.6. Dados de usuários, atributos e políticas utilizados pelos controles de acesso, não podem ser manipulados pelos usuários finais, a menos que especificamente autorizado na arquitetura do projeto.

6.7. O sistema deverá utilizar o princípio do menor privilégio, os usuários só devem ser capazes de acessar funções, arquivos de dados, URLs, controladores, serviços e outrosoken recursos, para os quais possuam autorização específica.

6.8. Em caso de sistemas que utilizam JWT (JSON Web Token):t

6.8.1. Será obrigatório o uso de chaves randômicas (JWT Secret);

6.8.2. Será proibido armazenar dados confidenciais em tokens JWT.

6.8.3. Será proibida a extração do algoritmo do cabeçalho (deverá ser validado no back-end);

6.8.4. Deverá ser utilizado no back-end o algoritmo RS256;

6.8.5. Será obrigatório regras de time-out de sessão do usuário de 15 minutos, access token de 3 minutos e refresh token de 8 horas.

7. REQUISITOS DE COMUNICAÇÃO DE REDE

7.1. O sistema deverá ser capaz de suportar a pilha dupla IPV4 e IPv6.

7.2. Todas as comunicações externas entre os servidores do sistema e os clientes deverão ser encriptadas.

7.3. O sistema deverá utilizar criptografia para as comunicações externas entre os servidores do sistema e os clientes. Os dados deverão ser criptografados na rede utilizando somente TLS 1.2 ou superior.

7.4. O sistema não deverá permitir o uso do SSL, TLS 1.0 e TLS 1.1.

7.5. Deve-se usar os seguintes algoritmos: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 e SHAKE256.

7.6. Será vedada a utilização de cifras com vulnerabilidades divulgadas e/ou conhecidas.

7.7. As requisições deverão ser limitadas (através de rate limit ou outra solução semelhante), a fim de se evitar ataques de DoS (negação de serviço) ou força bruta.

7.8. Deverá ser utilizada a validação de “redirect_url” no servidor para permitir apenas URL’s da *whitelist*.

7.9. Tráfegos HTTP deverão ser redirecionados para HTTPS.

7.10. A propriedade “readOnly” deverá ser configurada como “true” em esquemas de objeto para todas as propriedades que podem ser recuperadas por meio de APIs, mas nunca deverão ser modificadas.

7.11. Os modos de depuração do servidor da Web ou de aplicativos e da estrutura de aplicativos deverão ser desativados em produção para eliminar recursos de depuração, consoles de desenvolvedor e divulgações de segurança não intencionais.

8. REQUISITOS DE RESPOSTAS HTTP

8.1. Os cabeçalhos HTTP ou qualquer parte da resposta HTTP não deverão expor informações detalhadas da versão dos componentes do sistema.

8.2. A aplicação deverá retornar os seguintes códigos:

8.2.1. 405 Method Not Allowed: sempre que um método solicitado não for apropriado para o recurso solicitado

8.2.2. 406 Not Acceptable: sempre que o formato suportado não for correspondido. Requisições content-type deverão ser validadas para permitir apenas o formato suportado (por exemplo application/xml, application/json etc.)

8.2.3. HTTP 200: código de resposta do status de sucesso do HTTP, indica que a solicitação foi bem-sucedida;

8.2.4. HTTP 302: indica que o recurso solicitado foi movido temporariamente para a URL fornecida pelo cabeçalho Location.

8.2.5. HTTP 401: para qualquer ação não autorizada no sistema.

8.2.6. HTTP 429: para solicitações que excedam o limite de requisição permitido.

8.2.7. HTTP 415: para solicitações contendo cabeçalhos de tipo de conteúdo ausentes ou inesperados

8.3. A aplicação deverá ter defesas contra ataques de poluição de parâmetro HTTP, especialmente se a estrutura do aplicativo não faz distinção sobre a origem dos parâmetros de solicitação (GET, POST, cookies, cabeçalhos ou variáveis de ambiente).

8.4. Redirecionamentos e encaminhamentos de URL deverão permitir apenas destinos que aparecem em uma lista de permissões ou deverão mostrar um aviso ao redirecionar para conteúdo potencialmente não confiável.

8.5. A aplicação deverá ter proteção contra ataques do tipo SSRF, validando ou higienizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos, campos de entrada de URL, listas de protocolos, domínios, caminhos e portas.

9. REQUISITOS DE AUDITORIA

9.1. A solução deve dispor de logs de eventos para fins de auditoria, incluindo todas as ações administrativas e ações envolvendo os itens arquivados e pesquisados no que tange o arquivamento, visualização, recuperação e remoção de itens.

9.2. A solução deve dispor de logs com registro de informações a serem utilizadas na depuração e verificação de falhas da solução, mantendo o registro de toda atividade de arquivamento e recuperação realizada, inclusive para os processos de auditoria realizados.

9.3. A solução deve permitir a configuração de usuários (auditores), com permissão de monitorar (auditar) e acessar grupos específicos de caixas postais e/ou todas as mensagens arquivadas.

9.4. A solução deve suportar a geração e armazenamento de logs no formato IPV4 e IPv6.

9.5. As aplicações deverão implementar um sistema de *logging* que permita auditorias e investigações de incidentes de segurança, fraudes e casos de abuso.

9.6. A identificação do usuário, ou ID, deverá ser única, isto é, cada usuário deverá ter uma identificação própria.

9.7. Os sistemas de informação e suas respectivas infraestruturas deverão ser configurados de modo a registrar um critério mínimo de informações de logging e auditoria, contendo, no mínimo:

9.7.1. operações de login e logout;

9.7.2. tentativas de login malsucedidas;

9.7.3. acesso a telas cujo conteúdo é sigiloso, em segredo de justiça, possua dados pessoais ou bancários;

9.7.4. operações de inclusão, alteração ou exclusão de registros no banco de dados;

9.7.5. execução de jobs e tarefas automatizadas;

9.7.6. criação, leitura, atualização ou exclusão de informações sigilosas;

9.7.7. mudanças de configurações no sistema, na rede ou em serviços (inicialização, suspensão e reinicialização de serviços), inclusive a instalação de patches e atualizações de softwares;

9.7.8. acesso aos bancos de dados de fonte interna e externa;

9.7.9. falhas que resultem no fechamento anormal da aplicação, especialmente devido à exaustão de recurso ou atingimento do limite de um recurso (como memória do CPU, conexões de rede, espaço no disco etc.);

9.7.10. acesso e alteração de trilhas de auditoria;

9.7.11. registros de tráfego de dados de fontes internas e externas; e

9.7.12. registros de processos internos relacionados às atividades do negócio.

9.8. Os registros dos eventos deverão incluir, no mínimo, as seguintes informações:

9.8.1. identificação inequívoca do autor/ativo que realizou a atividade;

9.8.2. sistema onde ocorreu ou foi observada a atividade (logger/observador do evento);

9.8.3. tela (página) do sistema de onde a operação foi realizada;

9.8.4. tipo de atividade ocorrida (tipo de evento/ação);

9.8.5. data, hora e fuso horário, observando os mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);

9.8.6. retorno do sistema em caso de falhas ou sucesso na ação;

9.8.7. identificador da instância (para sistemas clusterizados);

9.8.8. para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;

9.8.9. parâmetros informados pelo usuário (ex: parâmetros repassados aos métodos GET ou POST);

9.8.10. tempo de resposta do sistema;

9.8.11. para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada etc.; e

9.8.12. endereço IP, nome do dispositivo, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

9.9. A aplicação não deve registrar credenciais ou detalhes de pagamento.

9.10. Os tokens de sessão só devem ser armazenados em logs de forma irreversível e com hash.

9.11. Será vedado o envio de informações sensíveis (ex: credenciais de acesso) para logs.

9.12. A solução não deverá registrar logs de auditoria em banco de dados da aplicação.

9.13. As aplicações deverão registrar logs de rastreamento distribuído (distributed tracing) de requisição.

9.14. As aplicações deverão gerar logs em formato que permita a completa identificação dos fluxos de dados

9.15. As aplicações deverão registrar eventos relevantes de segurança, incluindo eventos de autenticação bem-sucedidos e com falha, falhas de controle de acesso, falhas de desserialização e falhas de validação de entrada.

9.16. A solução deve garantir que todas as fontes de tempo estão sincronizadas com a hora e fuso horário corretos.

9.17. Dados de registro devem ser sanitizados para evitar ataques de injeção de registro.

10. REQUISITOS PARA APIs

10.1. A codificação de API deverá incorporar, no mínimo, proteção contra:

a) Broken Object Level Authorization
b) Broken User Authentication
c) Excessive Data Exposure
d) Lack of Resources & Rate Limiting
e) Broken Function Level Authorization
f) Mass Assignment
g) Security Misconfiguration
h) Injection (Injection flaws, tais como SQL e NoSQL, Command Injection etc.)
i) Improper Assets Management
j) Insufficient Logging & Monitoring
k) Conformidade com o OWASP Top 10 API Security Risks em vigor

10.2. Deverão ser utilizadas as classes Encoder e Validator da OWASP ESAPI (Enterprise Security API)

10.3. Deve ser imposto o menor privilégio quando se conectar ao banco de dados ou outros sistemas de back-end.

10.4. O banco de dados não deverá ser acessado por outro canal que não seja a aplicação

10.5. Os URLs da API não deverão expor informações confidenciais, tais como a chave da API, tokens de sessão etc.

10.6. Objetos serializados deverão usar verificações de integridade ou criptografados para evitar a criação de objetos hostis ou adulteração de dados.

10.7. Todos os endpoints acessíveis ao público devem usar um Certificado Digital que tenha sido assinado por uma Autoridade de Certificação aprovada e dentro do prazo de utilização.

10.8. Devem ser aplicadas políticas de limitação de taxa (ratelimit) para evitar o abuso da API.

10.9. Toda entrada pelo usuário por parâmetros da aplicação ou de forma manipulada em qualquer outra parte da aplicação, deverá ser validada, garantindo as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado."

10.10. A solução deve garantir que apenas entradas válidas, esperadas e apropriadas sejam processadas, pois caracteres especiais ou maliciosos são usados para explorar falhas como: SQL injection, XSS, Temlate Injection, entre outros.