

ANEXO I

PLANO DE TRABALHO DO ACORDO DE PARCERIA PARA PESQUISA, DESENVOLVIMENTO E INOVAÇÃO

ITEM 1: JUSTIFICATIVA PARA EXECUÇÃO E ESCOPO DO PROJETO

Este projeto visa melhorar a experiência dos empreendedores no registro de marcas, fornecendo um sistema inteligente que os orienta e representa suas demandas, bem como apoiar os examinadores de pedidos de registro de marca. O projeto propõe aplicar técnicas de Inteligência Artificial (IA) para facilitar o registro de marcas por empreendedores, através de uma consulta guiada e contextualizada, e apoiar os examinadores na identificação de impedimentos ao registro de uma marca. Os benefícios esperados incluem simplificação do processo de registro, identificação prévia de erros, e maior previsibilidade nas decisões do INPI. A etapa de transferência de conhecimento para as equipes técnica e de negócio do INPI promoverá ganho significativo de capacidade, e também servirá de auxílio no estabelecimento de padrões na governança de IA.

O escopo do projeto é o desenvolvimento de uma solução de software Web, alternativa à solução existente do INPI, que utilizará tecnologias de Processamento de Linguagem Natural (PLN) e de Visão Computacional (VC) no processo de consulta de marcas. A solução deve seguir os requisitos e padrões de desenvolvimento de software do INPI (ANEXO II), onde couber, para garantir a manutenibilidade posterior pela equipe técnica do INPI.

§1º A solução deverá ser formada a partir de detalhamento do escopo técnico e por 5 (cinco) módulos principais:

Escopo Técnico: Relatório da UFG, aprovado pelo INPI, com o detalhamento técnico do escopo de cada módulo a ser desenvolvido, incluindo a definição dos testes e conteúdos previstos nos treinamentos a serem realizados.

1) Módulo de análise inteligente de elementos nominativos de marcas anteriores: à medida em que o usuário fornece elementos nominativos da marca que deseja pesquisar, este módulo interage com o usuário guiando esse processo de coleta de informações. O módulo então analisa de forma inteligente essas informações e informa ao usuário quando existirem marcas anteriores que impeçam o registro da marca pretendida.

2) Módulo de análise inteligente de elementos figurativos de marcas anteriores: ao realizar o upload da imagem de uma marca, este módulo irá buscar por marcas anteriores similares, considerando inclusive o segmento mercadológico.

3) Módulo de análise inteligente de elementos nominativos e figurativos impeditivos ao registro de marca: à medida que elementos nominativos ou figurativos são fornecidos pelo usuário em sua busca, este módulo deve analisar se esses elementos impedem o registro

de marca, conforme determina o Art. 124 da Lei nº 9.279/96 – Lei da Propriedade Industrial (LPI).

4) Módulo de suporte às tarefas do examinador de pedido de registro de marcas: este módulo é voltado para o examinador, usuário que analisa cada pedido de registro de marca. Por meio deste módulo, o examinador poderá autenticar-se, consultar por elementos nominativos e figurativos de marcas e identificar termos impeditivos ao registro de uma marca.

5) Módulo de testes, ajustes e treinamentos: esta etapa será voltada para apoiar os testes dos sistemas no portal do INPI e pelos examinadores, realização de revisão e ajustes dos módulos 1 ao 4, se necessário, e treinamento da equipe do INPI.

§2º Objetivo e Contexto:

Este projeto tem como objetivo geral melhorar a experiência dos usuários empreendedores no registro de marcas ao lhes fornecer um sistema inteligente com informações que os orientam e melhor representam as suas demandas. O mesmo se almeja em relação ao usuário examinador de pedido de registro de marcas.

O Instituto Nacional da Propriedade Industrial (INPI), criado em 1970, é uma autarquia federal atrelada ao Ministério da Economia, responsável pelo aperfeiçoamento, disseminação e gestão do sistema de concessão e garantia de direitos de propriedade intelectual para a indústria no Brasil. Na economia atual, estes direitos se transformam em diferenciais competitivos, o que estimula o surgimento contínuo de novas identidades e soluções técnicas.

Dentre os serviços ligados a direitos de propriedade intelectual da indústria, destaca-se o serviço de registro de marcas. Para ter exclusividade sobre uma marca, é necessário que se faça o seu registro no INPI. No entanto, não é possível registrar uma marca muito similar a uma marca registrada por outrem que identifica um produto ou serviço de mesma natureza. Para tanto, existe um passo ao longo do registro de marcas que pode auxiliar na decisão pelo registro: a consulta à base de dados de marcas do INPI.

Atualmente, esse processo de consulta é feito via serviço disponibilizado na Web, cuja interface permite fazer uma busca por elementos nominativos (um termo exato ou um radical). Neste caso, o serviço de consulta realiza a análise lexical do texto informado pelo usuário. Como resultado, o sistema exibe uma lista de marcas que atendem os termos da busca e respectivos metadados, p.ex., nome do titular da marca, classificação e status (p.ex., arquivado, indeferido, em análise, em vigor).

Entretanto, a simplicidade desse processo de consulta contrasta com as dificuldades experimentadas pelos seus usuários, em geral, o pequeno empreendedor, que não comprehende as instruções fornecidas para consulta de uma marca. Soma-se a este problema, a ausência de um serviço de consulta por elementos figurativos (i.e., imagem) de marcas anteriores, que poderia integrar-se ao processo de registro de marcas do INPI. Considera-se, portanto, que o serviço de consulta de elementos nominativos e figurativos



de marcas anteriores do INPI é uma oportunidade para a aplicação de técnicas de Inteligência Artificial (IA). Neste contexto, a Unidade EMBRAPII CEIA/UFG (UE CEIA/UFG) espera, com este projeto, oportunizar a empreendedores o registro de uma marca apoiado por uma consulta guiada e contextualizada às suas necessidades, com o apoio de tecnologias de IA visando melhorar a experiência desse usuário e, assim, aumentar as chances de aprovação no registro de uma marca. Além disso, as tarefas do examinador de pedido de registro de marcas também serão apoiadas por um módulo de consultas por elementos nominativos e figurativos de marcas e identificação de termos impeditivos ao registro de uma marca.

ITEM 2: CRONOGRAMA DO PROJETO

Os prazos de entrega de cada módulo são em meses corridos são consecutivos, iniciando o primeiro módulo na assinatura do ACORDO, e a aceitação dos módulos fica vinculada aos termos do presente ACORDO e seus anexos.

As entregas deverão ser realizadas por meio de apresentação de documentos que evidenciam a sua execução (impresso e eletrônico) conforme **detalhamento do escopo no item 1 §1º deste PLANO DE TRABALHO e das condições de aceitação e pagamento** relacionadas a seguir no cronograma de pagamentos, e validadas pelo SEBRAE e pelo INPI, conforme o seguinte cronograma:

	prazo (em meses)
Escopo Técnico	2
1) Módulo de análise inteligente de elementos nominativos de marcas anteriores	5
2) Módulo de análise inteligente de elementos figurativos de marcas anteriores	5
3) Módulo de análise inteligente de elementos nominativos e figurativos impeditivos ao registro de marca	5
4) Módulo de suporte às tarefas do examinador de pedido de registro de marcas	5
5) Módulo de testes, ajustes e treinamentos	2

§1º Pelas entregas acordadas e serviços objeto deste ACORDO e PLANO DE TRABALHO, o SEBRAE repassará à FUNAPE um total de **até R\$ 1.650.000,00 (um milhão e seiscientos e cinquenta mil reais)**, conforme tabela a seguir.

ETAPA	EVIDÊNCIA DE FINALIZAÇÃO DA ETAPA	VALOR DE REPASSE
ESCOPO TÉCNICO	Relatório, aprovado pelo INPI, com o detalhamento técnico do escopo de cada módulo a ser desenvolvido, incluindo a definição dos testes e conteúdos previstos nos treinamentos a serem realizados	R\$ 350.000,00, após a assinatura do acordo
MÓDULO 1 Análise inteligente de elementos nominativos de marcas anteriores	Relatório, validado pelo INPI, que demonstre a nova solução interage com o usuário guiando esse processo de coleta de informações à medida em que o usuário fornece elementos nominativos da marca que deseja pesquisar, e que analisa de forma inteligente essas informações e informa ao usuário quando existirem marcas anteriores que impeçam o registro da marca pretendida	R\$ 350.000,00, após a conclusão da etapa anterior
MÓDULO 2 Análise inteligente de elementos figurativos de marcas anteriores	Relatório, validado pelo INPI, que demonstre que ao realizar o upload da imagem de uma marca, o módulo busca por marcas anteriores similares, considerando inclusive o segmento mercadológico.	R\$ 350.000,00 após a conclusão da etapa anterior
MÓDULO 3 Análise inteligente de elementos nominativos ou figurativos que impedem o registro de marcas	Relatório, validado pelo INPI, que demonstre que, à medida que elementos nominativos ou figurativos são fornecidos pelo usuário em sua busca, esão analisados se esses elementos impedem o registro de marca, conforme ao determina o Art. 124 da Lei nº 9.279/96 – Lei da Propriedade Industrial (LPI).	R\$ 350.000,00 após a conclusão da etapa anterior

MÓDULO 4	2 relatórios: i) Relatório, validado pelo INPI, que demonstre que este módulo atende à etapa anterior R\$ 250.000,00 após a conclusão da etapa anterior
Supporte às tarefas do examinador de pedido de registro de marcas	permite que o examinador analise cada pedido de registro de marca. Por meio deste módulo, o examinador deverá poder autenticar-se, consultar por elementos nominativos e figurativos de marcas e identificar termos impeditivos ao registro de uma marca. ii) Relatório, aprovado pelo INPI, que ateste que foram feitos testes dos sistemas no portal do INPI e pelos examinadores, realizada revisão e ajustes dos módulos 1 ao 4, se necessário, e concluído o treinamento da equipe do INPI.

§ 2º Os pagamentos serão realizados no prazo de até 30 (trinta) dias, após o aceite do objeto, aqui representado pelo ateste das respectivas notas fiscais/faturas pelo SEBRAE, mediante apresentação de relatório referente as atividades demandadas, por meio de ordem bancária creditada na conta corrente da FUNAPE, PARCEIRA 3.

§ 3º A cada pagamento, a FUNAPE deverá apresentar as Certidões de Regularidade Fiscal acompanhadas de suas respectivas autenticações, obtidas nos sítios que as emitirem, sendo o descumprimento dessa exigência ensejador de aplicação das penalidades descritas na Cláusula Penal deste instrumento.

§ 4º Todas as despesas de locomoção, acomodação, alimentação, comunicação e mão de obra, dentre outras necessárias à execução do contratado, correrão por conta da FUNAPE, não ocasionando ao SEBRAE nenhum ônus de acréscimo ou majoração nos valores dos serviços, bem como nenhum tipo de pagamento correspondente a horas extras, deslocamentos, adicionais noturnos ou encargos afins.

§ 5º Para liquidação dos valores relativos à prestação dos serviços será ainda observado o que segue: I. O SEBRAE reserva-se o direito de suspender o pagamento se os serviços não estiverem sendo prestados de acordo com o proposto, aceito e acordado; II. O SEBRAE poderá deduzir do montante a ser pago os valores correspondentes a eventuais multas ou indenizações, devidas pela FUNAPE. Caso a multa seja superior ao crédito eventualmente existente, a diferença será cobrada administrativa ou judicialmente – no último caso, se necessário. III. Havendo erro no documento de cobrança, ou qualquer circunstância que desprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado até que a FUNAPE providencie as medidas saneadoras necessárias, não ocorrendo, neste caso quaisquer ônus para o SEBRAE.



§ 6º Serão suspensos os pagamentos se: I. os serviços, no ato da atestação, não estiverem sendo prestados de acordo com o proposto, aceito e contratado; II. as notas fiscais ou recibos contiverem incorreções, caso em que serão devolvidas, acompanhadas dos motivos de sua rejeição, contando-se, então, o prazo para pagamento a partir da reapresentação da nota devidamente corrigida.

§ 7º Quaisquer despesas decorrentes de transações bancárias correrão por conta da FUNAPE.

§ 8º A FUNAPE deverá arcar com o recolhimento de todos os tributos e contribuições federais, estaduais e municipais, devidos em decorrência do objeto deste ACORDO, exceto aqueles retidos pelo SEBRAE na forma da lei, devendo destacar as retenções tributárias devidas em suas Notas Fiscais/Faturas ou entregar documentação que comprove a necessidade de não retenção de determinado(s) tributo(s).

§ 9º Os valores correspondentes a eventual aplicação de multa, pagamentos indevidos e/ou danos causados ao SEBRAE, serão descontados do crédito devido à FUNAPE em favor do SEBRAE. Caso os valores sejam superiores ao crédito eventualmente existente, a diferença será cobrada administrativa ou judicialmente – no último caso, se necessário.

ITEM 3: DA EXECUÇÃO E OBRIGAÇÕES DE CADA PARCEIRO NO PLANO DE TRABALHO

As ações serão desenvolvidas de forma descentralizada, nas instalações do Centro de Excelência em Inteligência Artificial da Universidade Federal de Goiás - CEIA/UFG e/ou Instituto Nacional da Propriedade Industrial – INPI.

Em caso de haver necessidade da prestação de serviços na sede do SEBRAE ou do INPI, a UFG é a única responsável pela saúde e bem-estar dos seus colaboradores, bem como pelo fornecimento de equipamentos de trabalho, cabendo ao SEBRAE ou INPI fornecer acesso às dependências e infraestrutura de tecnologia e serão custeados pela UFG, nas despesas relacionadas ao transporte, alimentação e estadias.

§1º A execução de que o objeto deste PLANO DE TRABALHO ocorrerá em conformidade com a proposta apresentada pelo PARCEIRO 2, UFG, e com o ABS nº 159/2023 de 06 de dezembro de 2023 da Unidade de Inovação do SEBRAE, PARCEIRO 1, cujos termos acatam o SEBRAE, UFG e FUNAPE e se comprometem a cumprir.

§2º A execução será realizada conjuntamente pela UFG - que exercerá a condução técnica da Pesquisa para o Desenvolvimento do projeto - e pela FUNAPE que será responsável pela gestão financeira e administrativa dos recursos aportados. Os serviços serão executados pelos profissionais da UFG e FUNAPE, sem subordinação jurídica com o SEBRAE, e na forma descrita na proposta e no processo nº 2023/NA/1003.

§3º O INPI fica obrigado a: I. alocar recursos humanos e tecnológicos associados ao atual sistema de registro de marcas da autarquia a fim de possibilitar o desenvolvimento do novo sistema pela UFG de forma alinhada e integrada aos sistemas e banco de dados vigentes no INPI. O INPI também se responsabilizará por apoiar no que for de seu alcance a



integração da solução desenvolvida pela UFG com: a) sistema de autenticação de usuários do INPI, por meio de API disponibilizada pelo INPI; b) sistema PAG de geração de GRU (Guia de Recolhimento da União) e Protocolo do INPI (serviços 389 (especificação pré-aprovada) ou 394 (especificação livre)); c) sistema e-Marcas do INPI, por meio de API a ser desenvolvida pela CEIA/UFG.

§4º o SEBRAE fica obrigado a: I. Prestar as informações e os esclarecimentos sobre as ações que venham a ser solicitados pela UFG; II. Exigir o cumprimento de todas as obrigações assumidas pela UFG, de acordo com as cláusulas contratuais e os termos de sua proposta; III. Exercer o acompanhamento e a fiscalização dos serviços, nos termos da Instrução Normativa de Gestão dos PLANOS DE TRABALHOS do SEBRAE. IV. Notificar a UFG por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção; V. Pagar à UFG o valor resultante da prestação do serviço de desenvolvimento, após a realização do mesmo, no prazo e condições estabelecidos; VI. Verificar os produtos/serviços para aceite do objeto e ateste da fatura em até 10 (dez) dias. VII. Exigir o fiel cumprimento de todos os requisitos acordados e da proposta apresentada, avaliando, também, a qualidade dos serviços apresentados, podendo rejeitá-los no todo ou em parte; VIII. Disponibilizar a infraestrutura necessária para a plena execução dos serviços; IX. Garantir que o pessoal da UFG terá acesso a todas as áreas, informações e ambientes necessários para a execução das tarefas previstas, respeitando as normas de segurança do SEBRAE; X. Dar ciência à UFG, por meio de documento escrito, sobre o caráter sigiloso que porventura venha a caracterizar qualquer dado e/ou informação fornecido pelo SEBRAE manipulados pela equipe dos técnicos da UFG e do INPI.

§5º a UFG fica obrigada a: I. Executar os serviços conforme especificações contidas no processo e nas suas propostas; II. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no menor prazo possível a ser fixado em comum acordo entre as partes, os serviços efetuados em que comprovadamente se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados, causados por culpa exclusiva da UFG; III. Responsabilizar-se pelos vícios e danos diretos decorrentes da execução do objeto, ficando o SEBRAE autorizado a descontar dos pagamentos devidos à UFG, o valor correspondente aos danos diretos sofridos, observados os limites e condições estabelecidas neste PLANO DE TRABALHO; IV. Relatar ao SEBRAE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços; V. Negociar com os PARCEIROS as alterações das atividades decorrentes de orientações recebidos ao longo da execução do Gestor do PLANO DE TRABALHO e, quando requisitada, prestar os esclarecimentos e atender às reclamações formuladas, sujeitando-se a mais ampla e irrestrita fiscalização; VI. Não transferir a outrem, por qualquer forma, nem mesmo parcialmente, nem subcontratar qualquer das prestações e serviços a que está obrigada, por força do presente PLANO DE TRABALHO, sem prévio assentimento escrito do SEBRAE; VII. Responder por qualquer ação judicial movida por terceiros com base na legislação de proteção da propriedade intelectual, relacionada com os serviços objeto deste PLANO DE TRABALHO; VIII. Manter entendimentos com o SEBRAE, objetivando evitar transtornos e atrasos nos serviços; IX. Entregar ao SEBRAE os documentos necessários para a realização dos pagamentos e prestar contas ao SEBRAE das atividades desenvolvidas; X. Assinar termo de encerramento do PLANO DE TRABALHO a ser enviado

pelo gestor do PLANO DE TRABALHO quando do término do PLANO DE TRABALHO; XI. Garantir que os profissionais da UFG portem crachá de identificação quando estiverem prestando serviços nas dependências do SEBRAE. XII. Participar de reuniões de planejamento, definição e de validações, quando necessário; XIII. Nomear preposto para, durante o período de vigência, representá-lo na execução do PLANO DE TRABALHO. XIV. Estabelecer e manter contato com os técnicos do INPI alocados para acompanhar a execução do projeto de desenvolvimento do novo sistema de registro de marcas XV. Prestar as informações e esclarecimentos que venham a ser solicitados pelos técnicos do SEBRAE e/ou INPI; XVI. Executar, dentro da melhor técnica e qualidade, os serviços necessários à realização do objeto deste Termo de Referência; XVII. Atender à solicitação de reformulação ou correção apontada pelo SEBRAE e/ou INPI, sempre que oriunda de problemas decorrentes de falha nos serviços prestados, considerando o escopo das atividades previstas; XVIII. Manter entendimentos com o SEBRAE e INPI, objetivando evitar transtornos e atrasos na execução dos serviços; XIX. Responder legalmente pela quebra do sigilo ou pelo mal-uso de dados ou informações previamente identificadas pelos outros parceiros como de caráter sigiloso ou confidencial; XX. Acompanhar e avaliar a execução dos projetos, devendo realizar eventuais pedidos de correção. XXI. Utilizar empregados habilitados e com conhecimentos suficientes à execução dos serviços previstos neste PLANO DE TRABALHO, em conformidade com as normas e determinações em vigor; XXII. Custear todas as despesas com passagem, hospedagem, deslocamentos diversos, locações de veículos, ajudas de custo, seguros e outras de viagem, para os empregados da empresa e seus contratados; XXIII. Dispor de equipamentos para realizar reuniões de planejamento através de videoconferência; XXIV. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade ao SEBRAE; XXV. Apresentar, quando solicitado pelo SEBRAE, a comprovação de que todos os requisitos em relação aos encargos e obrigações trabalhistas, previdenciários e fiscais estão sendo satisfeitos; XXVI. Manter durante toda a vigência do PLANO DE TRABALHO, em compatibilidade com as obrigações assumidas, todas as condições de regularidade fiscal, jurídicas e qualificação, conforme as exigências legais aplicáveis e as exigidas na contratação, durante a vigência deste ACORDO; XXVII. Garantir que a equipe de suporte guarde sigilo e confidencialidade sobre todas as informações obtidas em decorrência do cumprimento do PLANO DE TRABALHO, não podendo divulgá-las a terceiros sem prévia autorização por escrito do SEBRAE; XXVIII. Com a anuência do SEBRAE, indicar preposto da equipe de suporte que será o responsável pelo relacionamento com o SEBRAE. O mesmo deverá possuir os conhecimentos e capacidade profissional necessária para resolver imediatamente todo e qualquer assunto relacionado com os serviços contratados; XXIX. Responsabilizar-se por quaisquer acidentes de que possam ser vítimas seus empregados, equipes de suporte e prepostos, desde que causados por seus funcionários, quando nas dependências do SEBRAE, ou em qualquer outro local onde estejam prestando os serviços, devendo adotar as providências que, a respeito, exigir a legislação em vigor; XXX. Não retirar das dependências do SEBRAE quaisquer documentos e/ou informações a que tiver acesso, bem como não copiar, reproduzir e divulgar qualquer informação pessoal do quadro de colaboradores do SEBRAE, exceto quando autorizado pelo SEBRAE e pertinente à prestação do serviço objeto do presente PLANO DE TRABALHO; XXXI. Não divulgar, nem fornecer a terceiros dados ou informações referentes aos serviços prestados ao SEBRAE, salvo com autorização expressa e por escrito; XXXII. Responsabilizar-se, no

âmbito administrativo e civil, objetivamente, por qualquer ato de seus prepostos, empregados ou não, lesivos ao SEBRAE, a exemplo de fraude, corrupção ou dolo; XXXIII. Providenciar todos os recursos necessários à execução dos serviços às suas expensas, sem custos adicionais o SEBRAE, para os seus empregados ou contratados que estiverem prestando serviço nas instalações do SEBRAE Nacional. Para isso deverão ser seguidas todas as normas de segurança pessoal; XXXIV. Não possuir na composição do seu capital social ou em seu quadro social/diretivo, dirigentes e/ou empregados do SEBRAE, bem como ex-dirigentes e/ou ex-empregados até 18 meses contados do seu desligamento, demissão ou do pedido de demissão, conforme o caso. XXXV. Não possuir sócios ou dirigentes, que figurem como cônjuges, companheiros ou parentes em linha reta ou colateral, por consanguinidade ou afinidade, até o segundo grau, de empregados do SEBRAE; XXXVI. Respeitar as normas de controle de bens e de fluxo de pessoas nas dependências do SEBRAE; XXXVII. Adotar posturas que promovam a segurança no trabalho e o exercício da responsabilidade socioambiental; XXXVIII. Abster-se de utilizar, em todas as atividades relacionadas com a execução deste PLANO DE TRABALHO, trabalho infantil, degradante ou forçado, bem como exigir que as referidas medidas sejam adotadas no PLANO DE TRABALHO firmado com os fornecedores de seus insumos; XXXIX. Não empregar menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, de acordo com o disposto no inciso XXXIII do artigo 7º da Constituição da República Federativa do Brasil, de 05 de outubro de 1988. XXXIV. Responder, por escrito, com brevidade, inclusive por e-mail, os esclarecimentos que se fizerem necessários; XXXV. Substituir imediatamente o(s) membro(s) da equipe técnica e preposto que não esteja(m) atendendo aos níveis e à qualidade dos serviços adequados, quando solicitado pelo SEBRAE; XXXVI. Solicitar, em tempo hábil, todas as informações de que necessite para cumprimento de suas obrigações; XXXVII. Informar, imediatamente, ao SEBRAE toda e qualquer excepcionalidade ocorrida durante o processo de realização dos serviços, de modo que sejam tomadas imediatas providências; XXXVIII. Cumprir rigorosamente os prazos e orientações do SEBRAE; XXXIX. Fornecer relatórios solicitados por tipo de serviço no prazo a ser definido pela fiscalização, com todas as informações referentes a prestação do serviço.

§6º. Se houver ação trabalhista envolvendo os serviços prestados, a UFG adotará as providências necessárias para preservar o SEBRAE e mantê-lo a salvo de reivindicações, demandas, queixas ou representações de qualquer natureza e, não o conseguindo, se houver condenação, reembolsará o SEBRAE das importâncias que este tenha sido obrigado a pagar, dentro do prazo improrrogável de dez dias úteis a contar da data do efetivo pagamento.

ITEM 4: PROTEÇÃO DE DADOS

A UFG, por si e por seus colaboradores, obriga-se, a atuar no presente PLANO DE TRABALHO em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física (“Titular”) identificada ou identificável (“Dados Pessoais”) e as determinações de órgãos reguladores/fiscalizadores sobre a matéria.

§1º A UFG seguirá as instruções recebidas pelo SEBRAE em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, devendo a UFG garantir sua lícitude e idoneidade, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis.

§2º A UFG deverá corrigir, completar, excluir e/ou bloquear os Dados Pessoais, caso seja solicitado pelo SEBRAE.

§3º A UFG, no caso de recebimento de reclamações, solicitações e/ou notificações de Titulares de Dados Pessoais, que indiquem estar diretamente relacionados ao PLANO DE TRABALHO e ao SEBRAE, deverá informar ao Titular que direcione sua reclamação, solicitação e/ou notificação diretamente ao controlador de dados, conforme preconiza o artigo 18 da LGPD.

§4º A UFG, incluindo todos os seus colaboradores, compromete-se a tratar todos os Dados Pessoais como confidenciais, exceto se já eram de conhecimento público sem qualquer contribuição da UFG, ainda que este ACORDO venha a ser resolvido e independentemente dos motivos que derem causa ao seu término ou resolução.

§5º A UFG compromete-se a adotar medidas, ferramentas e tecnologias necessárias para garantir a segurança dos dados e cumprir com suas obrigações, sempre considerando o estado da técnica disponível e o nível de segurança necessário. I. A UFG deverá cumprir com os requisitos das medidas de segurança técnicas e organizacionais para garantir a confidencialidade por meio de pseudonimização ou criptografia dos Dados Pessoais, inclusive no seu armazenamento e transmissão. II. A UFG compromete-se a utilizar tecnologias visando à proteção das informações em todas as comunicações com compartilhamentos de Dados Pessoais pela UFG ao SEBRAE. III. A UFG deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado por ela para o tratamento de Dados Pessoais sejam estruturados de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos em Lei e às demais normas regulamentares aplicáveis.

§6º A UFG deverá realizar o registro de todas as atividades realizadas em seus sistemas/ambientes (“Registros”) que realizem tratamento de Dados Pessoais sob determinação do SEBRAE, de modo a permitir a identificação de quem as realizou. Tais Registros deverão conter, no mínimo: I. Ação; II. Identificação de usuários do sistema; III. Dados de IP no momento da ação; IV. Data/hora da ação, com referência UTC (Universal Time Coordinated), sendo que os relógios de seus sistemas estão sincronizados com a hora legal brasileira e de acordo com o protocolo NTP (ntp.br) de sincronização dos relógios; e V. Session ID da conexão utilizada.

§7º A UFG somente poderá subcontratar qualquer parte dos Serviços que envolvam o tratamento de Dados Pessoais para um ou mais terceiros (“Suboperadores”) mediante consentimento prévio e por escrito do SEBRAE. Neste caso, a UFG deverá celebrar um

Plano de Trabalho escrito com o Suboperador para (i) obrigar o Suboperador às mesmas obrigações impostas por este PLANO DE TRABALHO em relação à UFG, no que for aplicável aos Serviços subcontratados, (ii) descrever os Serviços subcontratados e (iii) descrever as medidas técnicas e organizacionais que o Suboperador deverá implementar.

§8º A UFG deverá monitorar, por meios adequados, sua própria conformidade e a de seus funcionários e Suboperadores com as respectivas obrigações de proteção de Dados Pessoais em relação aos Serviços e deverá fornecer ao SEBRAE relatórios sobre esses controles sempre que solicitado por ela.

§9º A UFG deverá notificar o SEBRAE em até 48h (quarente e oito) horas (i) de qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (ii) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (iii) de qualquer violação de segurança na UFG ou nos seus Suboperadores; (iv) de qualquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (v) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente.

§10º A UFG compromete-se a auxiliar o SEBRAE: I. com suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados Pessoais aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e II. no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.

§ 11º O presente PLANO DE TRABALHO não transfere a propriedade ou controle dos dados do SEBRAE ou dos seus clientes, inclusive Dados Pessoais, para a UFG (“Dados”). Os Dados gerados, obtidos ou coletados a partir da prestação dos Serviços ora contratados são e continuarão de propriedade do SEBRAE, inclusive sobre qualquer novo elemento de Dados criado a partir do tratamento de Dados estabelecido por este PLANO DE TRABALHO.

§12º Todo e qualquer tratamento de dados fora do Brasil, depende de autorização prévia e por escrito pelo SEBRAE à UFG.

§13º Sempre que Dados ou Registros forem solicitados pelo SEBRAE à UFG, esta deverá disponibilizá-los em até 48 (quarenta e oito) horas, podendo ser em menor prazo nos casos em que a demanda judicial, a norma aplicável ou o pedido de autoridade competente assim o exija. Caso a UFG receba diretamente alguma ordem judicial para fornecimento de quaisquer Dados, deverá comunicar ao SEBRAE antes de fornecê-los, se possível.

§14º O SEBRAE não autoriza a usar, compartilhar ou comercializar quaisquer eventuais elementos de Dados, produtos ou subprodutos que se originem, ou sejam criados, a partir do tratamento de Dados estabelecido por este PLANO DE TRABALHO.

§15º A UFG se compromete a devolver todos os Dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que (i) o PLANO DE TRABALHO for rescindido; ou (ii) com o

término do presente PLANO DE TRABALHO. Em adição, a UFG não deve guardar, armazenar ou reter os Dados por tempo superior ao prazo legal ou necessário para a execução do presente PLANO DE TRABALHO. §16º Caso os Dados da UFG estejam contidos em um banco de Dados, além de restituir este banco de Dados de inteira propriedade do SEBRAE em qualquer hipótese de extinção deste instrumento, a UFG deverá remeter em adição o dicionário de dados que permita entender a organização do banco de Dados, em até 10 (dez) dias ou em eventual prazo acordado entre as Partes.

§17º Fica assegurado ao SEBRAE, nos termos da lei, o direito de regresso em face da UFG diante de eventuais danos causados por esta em decorrência do descumprimento das obrigações aqui assumidas em relação a Proteção dos Dados.

§18º A UFG, sempre que tiver dúvidas ou necessidades de esclarecimentos, bem como solicitações específicas, em relação ao tratamento de seus dados pessoais, pode buscar entrar em contato com o Encarregado de Proteção de Dados Pessoais do SEBRAE por meio do e-mail dpo@sebrae.com.br.

§19º A UFG reconhece e aceita que o SEBRAE tem o direito de realizar auditoria, por si ou por terceiro indicado pelo SEBRAE, com a finalidade de verificar, por meio documental, a conformidade da UFG quanto à legislação de proteção de dados aplicável. Caso, mesmo após o envio dos documentos e informações pela UFG, o SEBRAE, de forma justificada, ainda possua questionamentos quanto à conformidade da UFG à LGPD, o SEBRAE poderá realizar auditoria presencial, mediante autorização e nos limites estabelecidos pela UFG, se obrigando a encaminhar o escopo da auditoria com 20 (vinte) dias de antecedência e se comprometendo a não solicitar documento de clientes. O SEBRAE também garante que o andamento das operações da UFG não serão afetados em caso de realização de auditoria presencial;

§20º O SEBRAE terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da UFG com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a UFG possui perante a Lei e este PLANO DE TRABALHO.

ITEM 5: VIGÊNCIA DO PLANO DE TRABALHO

O prazo de vigência deste PLANO DE TRABALHO é de 30 (trinta) meses, a partir da data de assinatura do ACORDO ao qual é vinculado, podendo ser prorrogado junto com o ACORDO mediante acordo entre as partes, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

- I. Os serviços tenham sido prestados regularmente;
- II. O SEBRAE mantenha interesse na realização do serviço;
- III. O valor do PLANO DE TRABALHO permaneça economicamente vantajoso para o SEBRAE; e
- IV. A FUNAPE manifeste expressamente interesse na prorrogação.

§1º A FUNAPE não tem direito subjetivo à prorrogação contratual.



INF
INSTITUTO DE INFORMÁTICA



§2º A prorrogação da vigência será formalizada, mediante justificativa da Unidade responsável, por termo aditivo específico, não podendo ultrapassar o limite máximo do prazo previsto no RLCSS, incluídos o período inicial de vigência e suas eventuais prorrogações.

ITEM 6: FORO

Fica eleito o foro da Circunscrição Especial Judiciária de Brasília/DF, com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer questões oriundas do presente instrumento.

ITEM 7: ASSINATURA DO PLANO DE TRABALHO

E por estarem de acordo, as partes expressamente concordam em utilizar e reconhecem como válida a plataforma de assinaturas do SEBRAE: <https://www.assinaturadigital.sebrae.com.br/portal/#/>, admitindo válidas as assinaturas realizadas eletronicamente, na presença das testemunhas abaixo assinadas.

Brasília/DF, XX de XXXXXXXX de 2024.

Pelo SEBRAE: RODRIGO DE SOUSA SOARES ALESSANDRO e ALESSANDRO VASCONCELOS MACHADO

Pela UFG (CEIA/UFG): ANGELITA PEREIRA DE LIMA Reitora e TELMA WOERLE DE LIMA SOARES Diretora Executiva

Pela UFG (FUNAPE): SANDRAMARA MATIAS CHAVES Diretora Executiva

Pelo INPI: JULIO CESAR CASTELO BRANCO REIS MOREIRA Presidente

Testemunhas:

1ª. _____ (NOME E CPF)

2ª. _____ (NOME E CPF)

ANEXO II

REQUISITOS TÉCNICOS DA ÁREA DE TI DO INPI

1) Modelo de Processo de Software – o INPI utiliza

- a) princípios e práticas de desenvolvimento de software ágil, incluindo Scrum;
- b) padrões de projeto (Enterprise Integration Patterns, Design Patterns, SOA, Microservices Patterns)
- c) Arquitetura de aplicações em três camadas, modelo MVC.
- d) Java, NodeJS, XML, Rest, Json, SOAP, JavaScript, SOAP, JSP, HTML, CSS, API, Web Services;
- e) Banco de dados transacionais como MySQL ou PostgreSQL, SqlServer e Oracle;
- f) Ferramenta de controle de versão: Git;
- g) Ferramenta de análise de código: SonarQube;
- h) Ferramentas CI/CD (integração e entrega contínuas): Jenkins, GitLab, Maven;
- i) Containers: Kubernets, Docker;
- j) Testes funcionais e automatizados: Junit, Selenium, Cucumber
- k) Ferramentas de avaliação de performance: Jmeter

2) Alguns critérios para aceitação de produtos:

- a) código-fonte submetido ao controle de versões;
- b) existência de testes unitários e de Relatório de Testes;
- c) existência de scripts de banco de dados com dicionário de dados embutido nos metadados (ausência apenas quando não houver mudança no modelo de dados);
- d) existência de arquivo para geração de Build; e) disponibilização de processos prontos para execução na ferramenta de CI/CD adotada, juntamente com a entrega e configuração de containers configurados pela ferramenta orquestração adotada;
- f) existência de manual de implantação;
- g) existência documentação concluída;
- h) resultado da execução de teste de segurança SAST indicando ausência de vulnerabilidades de nível HIGH ou CRITICAL, ou equivalente.

3) Testes prévios à entrega:

- a) testes funcionais automatizados existentes e corretamente implementados, com resultados correspondentes ao esperado;
- b) testes unitários que envolvam porções críticas do produto;
- c) testes funcionais executados nos principais fluxos do produto entregue.

4) Indicadores de qualidade do código fonte - metas a serem alcançadas, conforme relação a seguir:

Grupo	Indicador	Unidade	Meta
Projeto	Complexity / file ou equivalente	média total	<= 10
	Complexity / class ou equivalente	média total	<= 10
	Complexity /function ou equivalente	média total	<= 3
	Duplications ou equivalente	%	<= 4%
	Security Issue Tags ou equivalente	unidades	=0
	Technical Debt ratio ou equivalente	%	<= 2,5%
	SQALE RATING ou equivalente	Nota	=A
Violações de código (possíveis bugs, estilo de codificação, más práticas de codificação)	Critical Issues ou equivalente	unidades	=0
	Blocker Issues ou equivalente	unidades	=0
Indicadores relacionados a testes	Unit Tests Coverage - camada negócio / Impl ou equivalente	%	>=70%
	Unit Test Success ou equivalente	%	>=100%
	Skipped Tests ou equivalente	unidades	=0

O Indicador de qualidade de código (IQC) deve ser $\geq 90\%$, e será calculado dividindo a quantidade de requisitos de qualidade de código atendidos (ΣQrc) pela quantidade total de requisitos de qualidade de código avaliados (ΣQtr): $IQC = 100 * (\Sigma Qrc / \Sigma Qtr)$

5) Roteiro de codificação:

a) DIRETRIZES GERAIS

Além das diretrizes constantes deste Roteiro, deve-se adotar no que couber as orientações constantes dos:

- i) Guia de Requisitos e Obrigações quanto a Privacidade e à Segurança da Informação, disponível em: https://www.gov.br/governodigital/ptbr/seguranca-e-protecao-de-dados/ppsi/guia_requisitos_obrigacoes.pdf 25
- ii) Guia de Segurança em Aplicações Web, disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/quias/guia_seguranca_aplicacoesweb.pdf.

iii) Guia de Requisitos Mínimos de Segurança e Privacidade para APIs, disponível em:
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_seguranca_apis.pdf.

iv) Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis, disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_seguranca_apps.pdf.

b) ESCRITA DE CÓDIGO

i) Nomes Significativos

- (1) Os nomes utilizados para variáveis, funções, classes e métodos devem ser autoexplicativos, ou seja deve responder as seguintes perguntas: "Por que ele existe?", "o que ele faz?" e "como é usado?".
- (2) Não se deve incluir no código informações inverídicas ou falas para mascarar o código ou dificultar sua manutenção.
- (3) Os nomes devem ser pronunciáveis e ter significado adequado ao contexto em língua portuguesa.
- (4) Evite codificações ou encriptações em nomes de variáveis, classes, funções e métodos.
- (5) Os nomes devem ser de fácil entendimento associado ao contexto do domínio do negócio.

ii) Funções e Classes

- (1) As funções e classes devem ter o mínimo de linhas possível, mantendo-se a clareza e implementando o código necessário para traduzir o objetivo esperado da função ou da classe.
- (2) As funções e classes devem ter objetivos específicos possuindo um nível de abstração (deve ter apenas uma responsabilidade ou objetivo, ou seja, deve fazer coisa).
- (3) A escrita do código deve seguir uma narrativa top-down.
- (4) As funções e classes não devem possuir efeitos escondidos ou colaterais, ou seja, não devem produzir efeitos distintos daqueles que se propõe a realizar.
- (5) Deve-se evitar níveis de herança exagerados, superior a 4 (quatro)

iii) Comentários

- (1) O código útil deve ser autoexplicativo, limpo e eficiente, devendo possuir apenas os mínimos de comentário possível.
- (2) Evite comentários redundantes ou óbvios, que descrevem o que o código faz sem acrescentar nenhuma informação útil.

iv) Estruturas

- (1) Não se deve criar estruturas de código redundantes ou sem efetiva geração de valor à finalidade pretendida.
- (2) Não se deve replicar linhas de códigos ou estruturas tornando-as redundantes.

(3) Deve-se evitar duplicar ou replicar funções ou classes que possuam a mesma responsabilidade ou objetivo.

v) Indentação

(1) Deve-se adotar a indentação adequada para melhor entendimento e clareza do código, evitando-se identações exageradas ou nenhuma indentação.

vi) Complexidade ciclomática

(1) Deve-se adotar a menor complexidade ciclomática possível por algoritmo.

(2) Deve-se evitar o aninhamento excessivo de instruções de condições (If's dentro de If's).

(3) Deve-se evitar o exagero de condições ("Case") dentro de instruções de escolha ("switch")

(4) Deve-se remover construções desnecessárias, ou seja, aquelas que podem ser removidas sem alterar a semântica e a finalidade do código.

c) DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

i) Armazenamento de dados

(1) Nos casos de armazenamento de dados abertos (Dados públicos), não se deve utilizar meio de armazenamento que não possua acesso para escrita restrito por senha. (2) Nos casos de armazenamento de dados fechados (Dados cujo acesso é restrito a um grupo específico de pessoas), não se deve utilizar meio de armazenamento que não possua acesso para leitura e escrita restrito por senha.

(3) Não se deve disponibilizar à aplicações acesso à algum banco de dados utilizando login de usuário com permissões de root.

(4) Não se deve utilizar o armazenamento de senhas em código-fonte.

(5) Não se deve utilizar as mesmas senhas para ambientes de desenvolvimento ou homologação e produção

(6) Deve-se armazenar de forma segura os dados de usuários e os sistemas que utilizam cada senha fornecida.

ii) Gerenciamento de Acessos e Permissões de Usuários

(1) Não se deve armazenar senhas em texto plano sem utilizar um algoritmo de hash seguro e salt.

(2) Deve-se utilizar controle de usuário e senha nominais para determinar a identidade do usuário.

(3) Deve-se utilizar HTTPS para controle de autenticação ao menos nas telas de login do sistema web.

iii) Comunicação

(1) Deve-se empregar canal de comunicação com controle de duplicação e perda de informações/mensagens.

(2) Deve-se empregar canal de comunicação com controle de autenticação (eg, HTTPS, certificados digitais gerados por autoridades confiáveis, VPNs).

(3) Deve-se empregar canal de comunicação que provenha confidencialidade dos dados transmitidos (eg, HTTPS, VPNs).

iv) Medidas contra-ataques

(1) Deve-se prevenir ataques de injeção de SQL (SQL Injection), a exemplo das seguintes medidas mínimas:

(a) Não se deve criar SQLs concatenando parâmetros textuais de origem não-segura, como parâmetros preenchidos pelo usuário ou mesmo armazenados no banco de dados.

(b) Deve-se restringir permissões de acesso ao banco de dados para o usuário da aplicação.

(c) Deve-se, sempre que possível, passar parâmetros em comandos SQL (DML ou DDL) utilizando prepared statements.

(d) Consultas que não podem ser parametrizadas deverão receber tratamento especial, como escapes ou codificação em hexadecimal.

(2) Deve-se prevenir ataques de injeção de HTML e Javascript.

(3) Deve-se prevenir ataques do tipo cross-site scripting (XSS).

(4) Deve-se prevenir ataques de quebra de autenticação e gerenciamento de sessão (Broken Authentication and Session Management).

v) Auditoria, rastreamento e Logs

(1) Permitir que eventos sejam registrados a exemplo de:

(a) operações de login e logout;

(b) acessos a determinadas telas ou seções do sistema;

(c) acesso a informações com alguma restrição (eg, documentos sigilosos, processos em segredo de justiça, dados pessoais ou bancários);

(d) operações de inclusão, alteração ou exclusão de registros no banco de dados;

(e) alteração de perfil de acesso (para sistemas que possuem acesso com diferentes perfis); e

(f) execução de jobs e tarefas automatizadas.

(2) Permitir que informações sejam auditáveis para cada tipo de evento selecionado para monitoramento:

(a) data e hora;

(b) usuário que efetuou a operação;

(c) endereço IP;

(d) identificador da sessão do usuário (quando aplicável, eg, cookie);

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

(f) identificador da instância (para sistemas clusterizados);

(g) 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;

- (h) parâmetros informados pelo usuário (eg, parâmetros GET ou POST), tomando cuidado de não armazenar dados sensíveis, como senhas;
- (i) tempo de resposta do sistema;
- (j) para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada, etc.

(3) Permitir formas de captura dos dados para auditoria, a exemplo:

- (a) alterações aplicadas no banco de dados podem ser auditadas via triggers;
- (b) auditar as alterações a partir da própria aplicação, sendo que algumas informações poderão não ser registradas (eg, operações SQL realizadas por fora da aplicação).
- (c) Em sistemas web desenvolvidos em Java, um Filtro pode interceptar as requisições feitas à aplicação.

(4) Deve-se definir no documento de especificação de requisitos do sistema quais informações deverão ser registradas e o local de armazenamento dos dados da auditoria.

vi) Cópias de Segurança (Backups)

- (1) Deve-se incluir no plano de projeto a especificação da necessidade e a atribuição da responsabilidade de realização de backups do banco de dados e dos códigos-fonte do sistema, bem como as políticas de acesso a este backup.
- (2) Deve-se definir um procedimento estruturado para a restauração de backups.
- (3) Deve-se definir e capacitar responsáveis pela recuperação dos backups.

vii) Testes

- (1) Deve-se realizar testes manuais de segurança antes de cada versão do software que modifique sua estrutura (telas de login, serviços não autenticados, novos formulários com interação com o usuário, etc.).
- (2) Deve-se garantir, através de testes automatizados, que os serviços e dados sigilosos estão protegidos e disponíveis apenas para os usuários detentores das informações.
- (3) Deve-se elaborar uma política de testes, automatizados ou não, visando a garantia de não vulnerabilidade aos principais ataques conhecidos em sistemas.
- (4) Deve-se definir cenários de testes voltados à garantia dos requisitos não funcionais do software, preferencialmente realizado por uma equipe de testes diferente da equipe de desenvolvimento do software, com intuito de se evitar vícios.
- (5) Deve-se definir cenários de testes, principalmente nos aspectos de segurança, para os casos de atualizações na arquitetura do sistema (servidores de aplicação, banco de dados, versões de browser, versões de sistema operacional, etc.).

viii) Medidas contra falhas de segurança

- (1) Deve-se manter procedimento planejado para imediata indisponibilização do sistema e realização de manutenção corretiva.
- (2) Deve-se definir uma política de acompanhamento pós-correção de ocorrências de falha de segurança.

ix) Diretrizes para a instalação, configuração e gerenciamento de ambientes de desenvolvimento de sistemas

- (1) Deve-se utilizar um controle de versão distribuído, que mantém um repositório completo em cada máquina de desenvolvimento, Eg, Git , Mercurial .
- (2) Deve-se utilizar bancos de dados distintos para cada ambiente (Desenvolvimento, produção).
- (3) Deve-se utilizar servidores de aplicação/web distintos para cada ambiente (Desenvolvimento, produção).
- (4) Deve-se prover acesso ao ambiente de desenvolvimento/testes/homologação apenas aos integrantes da equipe de desenvolvimento e aos interessados no projeto (stakeholders).
- (5) Deve-se realizar testes periódicos para assegurar a segurança do ambiente de desenvolvimento/testes/homologação.

x) Diretrizes para a configuração de proteção a dados sensíveis

- (1) Deve-se utilizar um método criptográfico que siga o princípio de Kerckhoffs; o método de encriptação e seus parâmetros devem ser públicos e estar documentados, somente a chave criptográfica deve ser mantida em sigilo.
- (2) Não se deve utilizar um cifrador que admita um método conhecido para quebra da chave criptográfica melhor do que a força bruta, baseada em tentativa e erro.
- (3) Não se deve utilizar o modo de cifrador de bloco electronic codebook (ECB) ou modos menos seguros.
- (4) Não se deve utilizar um tamanho da chave menor que 128 bits (cifrador simétrico) ou 1024 bits (cifrador assimétrico).
- (5) Não se deve utilizar função de hash sem algum tipo de salt.
- (6) Não se deve utilizar algoritmos considerados obsoletos para criptografia e hash criptográfico. Exemplos: MD5, SHA1, DES/3DES, RC2, RC4, MD4.
- (7) Não se deve utilizar um tamanho da chave menor que 192 bits (cifrador simétrico) ou 2048 bits (cifrador assimétrico).
- (8) Não se deve distribuir chaves criptográficas sem a utilização de uma infraestrutura de chave pública e, portanto, sem a utilização de um cifrador assimétrico.

xi) Geração de Senhas

- (1) Não se deve utilizar senhas com menos de 8 caracteres.
- (2) Não se deve utilizar somente um tipo de caractere (letras, dígitos e símbolos).
- (3) Não se deve utilizar palavras comumente utilizadas para senhas (ou variantes destas), como, por exemplo: nome do animal de estimação, membro da família ou pessoa significativa; datas de aniversário; nome do feriado favorito; algo relacionado ao time esportivo favorito; e as palavras “senha” e “password”.
- (4) Não se deve utilizar periodicidade de troca superior a 1 ano.
- (5) Não se deve armazenar senhas em claro.
- (6) Deve-se armazenar ao menos o hash criptográfico com salt.
- (7) Não se deve usar um canal em claro para a transmissão da senha ou elemento correspondente.

(8) Não se deve utilizar método de conferência menos seguro que desafios baseados em hash ou o uso de hashes armazenados.

(9) Não se deve permitir uma taxa de tentativas de validação de senha superior a 5 tentativas por minuto.

(10) Não se deve mostrar diretamente a senha quando esta necessita ser digitada pelo usuário; deve haver opção de habilitar e desabilitar a visualização da senha digitada até então.

xii) Diretrizes para reforço da segurança de software nas fases de especificação, projeto e design

(1) Deve-se empregar modelo de projeto de software que contemple, no mínimo:

- (a) a etapa de modelagem de ameaças;
- (b) definição clara dos riscos de segurança; e
- (c) nível de severidade que o comprometimento de dados sensíveis traria ao sistema e à instituição.

(2) Não se deve omitir, durante o projeto de desenvolvimento de sistema e sua execução, a definição de responsabilidades pela segurança de dados do sistema e como essa responsabilidade será verificada.

(3) Deve-se utilizar cronograma de projeto que contemple pontos de verificação de segurança do sistema desenvolvido ao longo de sua construção.

xiii) Atualização de softwares

(1) Não se deve habilitar as atualizações automáticas de software ou componentes utilizados na construção de um sistema, sob pena de introdução indevida de falhas de segurança.

(2) Somente utilize código de terceiros que sejam confiáveis.

Goiânia, 23 de outubro de 2024

Prof. Dr. Anderson da Silva Soares

Anexo1_PTR_Acordo_de_Parceria_SEBRAE_INPI_UFG_FUNAPE.pdf

Documento número #a20220a8-2dc9-4d49-96f1-35943561962f

Hash do documento original (SHA256): c7ab60b141aaa2c8749434363b229a5214296f7784fd25f2cb01222bdf43e6d2

Assinaturas

Douglas Gaspar Rangel

CPF: 701.946.491-21

Assinou como testemunha em 20 fev 2025 às 15:58:29

ANDERSON DA SILVA SOARES

CPF: 000.509.121-78

Assinou como testemunha em 20 fev 2025 às 16:22:45

Sandramara Matias Chaves

CPF: 167.056.881-49

Assinou em 20 fev 2025 às 17:23:34

Júlio Cesar Castelo Branco Reis Moreira

CPF: 876.282.165-87

Assinou em 21 fev 2025 às 16:06:35

Angelita Pereira de Lima

CPF: 863.357.701-72

Assinou em 26 fev 2025 às 11:57:05

Rodrigo de Sousa Soares

CPF: 933.444.494-00

Assinou em 18 mar 2025 às 14:32:07

Log

20 fev 2025, 15:52:16

Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 criou este documento número a20220a8-2dc9-4d49-96f1-35943561962f. Data limite para assinatura do documento: 22 de março de 2025 (15:52). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.

- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: presidente@inpi.gov.br para assinar, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Júlio Cesar Castelo Branco Reis Moreira.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: andersonsoares@ufg.br para assinar como testemunha, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo ANDERSON DA SILVA SOARES.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: reitoria@ufg.br para assinar, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Angelita Pereira de Lima e CPF 363.357.701-74.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: rodrigo.sousa@sebrae.com.br para assinar, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rodrigo de Sousa Soares.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: alessandro@sebrae.com.br para assinar, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alessandro Vasconcelos Machado.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: douglas@funape.org.br para assinar como testemunha, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Douglas Gaspar Rangel e CPF 701.946.491-21.
- 20 fev 2025, 15:55:22 Operador com email fernandaop@funape.org.br na Conta 508f4656-6261-46a1-8844-0b2126c7f978 adicionou à Lista de Assinatura: sandramara@funape.org.br para assinar, via E-mail.
Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Sandramara Matias Chaves e CPF 167.056.881-49.
- 20 fev 2025, 15:58:29 Douglas Gaspar Rangel assinou como testemunha. Pontos de autenticação: Token via E-mail douglas@funape.org.br. CPF informado: 701.946.491-21. IP: 200.137.204.2. Componente de assinatura versão 1.1132.0 disponibilizado em https://app.clicksign.com.

20 fev 2025, 16:22:45	ANDERSON DA SILVA SOARES assinou como testemunha. Pontos de autenticação: Token via E-mail andersonsoares@ufg.br. CPF informado: 000.509.121-78 . IP: 177.174.212.46. Localização compartilhada pelo dispositivo eletrônico: latitude -15.79462666785818 e longitude -47.87474867052636. URL para abrir a localização no mapa: https://app.clicksign.com/location . Componente de assinatura versão 1.1132.0 disponibilizado em https://app.clicksign.com.
20 fev 2025, 17:23:34	Sandramara Matias Chaves assinou. Pontos de autenticação: Token via E-mail sandramara@funape.org.br. CPF informado: 167.056.881-49 . IP: 200.137.204.2. Componente de assinatura versão 1.1132.0 disponibilizado em https://app.clicksign.com.
21 fev 2025, 16:06:35	Júlio Cesar Castelo Branco Moreira assinou. Pontos de autenticação: Token via E-mail presidente@inpi.gov.br. CPF informado: 376.282.165-83 . IP: 168.90.175.207. Componente de assinatura versão 1.1132.0 disponibilizado em https://app.clicksign.com.
26 fev 2025, 11:57:05	Angelita Pereira de Lima assinou. Pontos de autenticação: Token via E-mail reitoria@ufg.br. CPF informado: 363.357.701-71 . IP: 200.137.208.151. Localização compartilhada pelo dispositivo eletrônico: latitude -16.6068224 e longitude -49.2568576. URL para abrir a localização no mapa: https://app.clicksign.com/location . Componente de assinatura versão 1.1135.0 disponibilizado em https://app.clicksign.com.
18 mar 2025, 14:32:07	Rodrigo de Sousa Soares assinou. Pontos de autenticação: Token via E-mail rodrigo.sousa@sebrae.com.br. CPF informado: 933.444.494-00 . IP: 187.69.65.229. Componente de assinatura versão 1.1154.0 disponibilizado em https://app.clicksign.com.
22 mar 2025, 15:52:43	Processo de assinatura finalizado automaticamente. Motivo: data limite para assinatura foi atingida. Processo de assinatura concluído para o documento número a20220a8-2dc9-4d49-96f1-35943561962f.



Documento assinado com validade jurídica.

Para conferir a validade, acesse <https://www.clicksign.com/validador> e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.

As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº a20220a8-2dc9-4d49-96f1-35943561962f, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.