# Cláusulas de Segurança:

* 1. Visando a SEGURANÇA DA INFORMAÇÃO, caberá às PARTES:
     1. Cada PARTE será única responsável pela seleção, implementação, e manutenção de procedimentos e políticas de segurança que sejam suficientes para garantir que: (i) o uso da conexão de rede por tal parte (e o uso do patrimônio de informações dos CONTRATANTES, pela CONTRATADA) seja seguro e utilizado somente para fins autorizados, e (ii) os registros e dados de negócios de tal parte estejam protegidos contra acesso ou uso indevidos, alteração, perda, ou destruição.
     2. Qualquer terceira parte que conecte um dispositivo a uma rede dos CONTRATANTES deverá ser autorizada pelo Encarregado de Segurança de TI local. O Fornecedor deverá prover proteção contra o uso externo não autorizado, modificação, divulgação ou destruição, acidental ou intencional, do patrimônio dos CONTRATANTES. A terceira parte será responsável pela segurança do dispositivo, através de antivírus e patches, para proteger o patrimônio de informações dos CONTRATANTES. Qualquer dispositivo pertencente a uma terceira parte, e que armazene ativos de informações dos CONTRATANTES, deverá ser criptografado.
     3. Somente usuários autorizados pelos CONTRATANTES poderão acessar as informações e dados contidos na infraestrutura dos CONTRATANTES ou na infraestrutura de terceiros contratados ou utilizados pelos CONTRATANTES. O CONTRATANTE deverá deter o poder de decisão final, a respeito de quem estará autorizado a acessar os dados e informações, incluindo o próprio pessoal dos CONTRATANTES, o pessoal da CONTRATADA, todo o pessoal subcontratado, e qualquer outra terceira parte. Todos os acessos deverão atender às Normas e políticas de tecnologia da informação dos CONTRATANTES.
     4. Serão concedidas somente autorizações de acessos individuais (login e senha). Contas genéricas ou compartilhadas são absolutamente proibidas.
     5. Dados ou informações sobre os CONTRATANTES, ou contidos na infraestrutura dos CONTRATANTES, quer possuídos, ou cedidos, ou hospedados nas instalações de uma terceira parte, ou na infraestrutura de um Fornecedor de Serviços de Aplicativos, não deverão ser divulgadas a quaisquer terceiras partes, sem a prévia aprovação por escrito dos CONTRATANTES.
  2. Visando a SEGURANÇA DA INFORMAÇÃO, caberá à CONTRATADA:
     1. Obedecer às normas, procedimentos e Políticas de Tecnologia da Informação dos CONTRATANTES, com todos os regulamentos e todas as atualizações correspondentes deste enquadramento, relativas aos países a partir dos quais a CONTRATADA preste os serviços ou hospede aplicativos ou dados.
     2. Preservar a disponibilidade e precisão das informações dos processos suportados e proteger as informações confidenciais e proprietárias, bem como os direitos de propriedade intelectual dos CONTRATANTES.
     3. Assegurar que o acordo de confidencialidade e as obrigações deste CONTRATO sejam atendidos por seus diretores, funcionários, representantes, agentes, e quaisquer outros subcontratados que irão executar tarefas descritas neste CONTRATO, antes da CONTRATADA direcioná-los à prestação dos serviços objeto deste CONTRATO.
     4. As alterações relativas aos aplicativos, arquitetura, procedimentos operacionais, procedimentos de segurança e sua respectiva avaliação de riscos, deverão ser comunicadas antecipadamente.
     5. Oferecer a sua máxima cooperação, para permitir que os CONTRATANTES realizem a verificação de conformidade dos produtos fornecidos e/ou serviços prestados.
     6. Atender aos requisitos de governança de tecnologia da informação dos CONTRATANTES, o que implica em fornecer informações úteis sobre: (i) infraestrutura / arquitetura de tecnologia da informação e de segurança atualizadas, (ii) organização de tecnologia da informação responsável pelo serviço; e (iii) alterações relativas à arquitetura e procedimentos de segurança, e sua correspondente avaliação de riscos.
     7. Responsabilizar-se exclusivamente perante os CONTRATANTES sobre todas as considerações de segurança de TI. Sob nenhuma circunstância, os CONTRATANTES assumirão ou aceitarão o compartilhamento de responsabilidade entre o Fornecedor e qualquer outra terceira parte, incluindo parceiros de negócios e subcontratados do Fornecedor.
     8. Assegurar que todas as atividades do serviço mantenham adequadamente os registros de negócios apropriados, de acordo com as melhores práticas da indústria e em conformidade com as leis e regulamentações aplicáveis, e assegurar também que os documentos estejam protegidos contra acesso ou uso indevidos, perda, alteração ou destruição. A CONTRATADA deverá realizar revisões regulares para detectar potenciais problemas de segurança. A CONTRATADA poderá ser obrigada a revelar as configurações, o processo de revisão, e os resultados.
     9. Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando os CONTRATANTES de qualquer responsabilidade.
     10. Juntamente com a definição de requisitos de negócios para novos sistemas ou serviços de informação, ou melhorias em sistemas ou serviços de informação existentes, a CONTRATADA deverá assegurar que a avaliação de segurança seja realizada e que controles de segurança apropriado sejam identificados e incorporados aos requisitos. A avaliação e os controles de segurança a serem incluídos deverão ser analisados e aprovados pelos CONTRATANTES.
     11. Não deverá estabelecer qualquer tipo de link de comunicação de dados entre as suas redes e sistemas e os dos CONTRATANTES, incluindo, mas não se limitando a atividades de supervisão, intervenção remota, e qualquer tipo de transferência de dados, por qualquer meio, incluindo, mas não se limitando a links diretos permanentes, Internet, VPN [rede privada virtual], ou dial-up [acesso por linha discada], sem a aprovação dos CONTRATANTES.
     12. Garantir que o ambiente de Tecnologia da Informação, em seu lado, assegure a integridade, disponibilidade e confidencialidade do patrimônio de Tecnologia da Informação dos CONTRATANTES, incluindo dados, informações e direitos de propriedade intelectual.
     13. Somente usuários autenticados e autorizados, com uma data de expiração de usuário pré-definida, deverão ter permissão para acessar sistemas dos CONTRATANTES e o prazo de acesso deverá ser restrito.
     14. Deverão ser mantidos logs de auditoria completos, nos níveis de conexão, sistema operacional, e aplicativos. Os CONTRATANTE se reserva o direito de supervisionar em tempo real, gravar e utilizar os dados armazenados das conexões.
     15. Todas as conexões com a CONTRATADA deverão ser criptografadas e serão estabelecidas somente através de firewalls dos CONTRATANTES. Somente serão permitidos hosts e protocolos previamente autorizados.
     16. Notificar imediatamente os CONTRATANTES, sempre que qualquer funcionário autorizado da CONTRATADA deixe a empresa, ou já não necessite de acesso, ou tenham sido modificadas as responsabilidades para acessar qualquer patrimônio de informações dos CONTRATANTES.
     17. Assim que termine a prestação do serviço pela CONTRATADA, por qualquer razão, normal ou anormal, todos os acessos deverão ser imediatamente revogados. A CONTRATADA não será mais autorizada a acessar o patrimônio de informações dos CONTRATANTES.
     18. Todas as informações de propriedade dos CONTRATANTES deverão ser enviadas os CONTRATANTES, em duas cópias, sendo em seguida removidas com segurança de todos os dispositivos.
     19. Rever a qualquer tempo o acesso de seus empregados ao patrimônio de informações dos CONTRATANTES, e prontamente corrigir qualquer discrepância em potencial. Mediante solicitação dos CONTRATANTES, a CONTRATADA deverá revelar os resultados da última análise de acessos, bem como as respectivas ações corretivas.
     20. Não utilizar qualquer criptografia desenvolvida internamente, para proteger as informações, os aplicativos ou a infraestrutura dos CONTRATANTES. Quaisquer algoritmos simétricos, assimétricos, ou de hashing, utilizado na infraestrutura dos CONTRATANTES, deverá utilizar algoritmos e ferramentas bem conhecidos, publicados, apresentados à comunidade global de criptografia, e adotados como padrão da indústria.
     21. A resistência dos algoritmos de criptografia deverá ser a mais alta possível, aprovada pelo CSO [Chief Security Officer / Chefe de Segurança] local dos CONTRATANTES, e em conformidade com os requisitos de negócios dos CONTRATANTES e com a legislação aplicável.
     22. Conexões que utilizem a Internet deverão ser protegidas utilizando tecnologias de criptografia, adotados como padrão de mercado.
     23. Deverão ser criptografados todos os dispositivos móveis e portáteis utilizados para prover o serviço os CONTRATANTES e que contenham dados confidenciais.
     24. Prover os CONTRATANTES uma lista com os nomes e funções dos funcionários que terão acesso aos Locais dos CONTRATANTES. Pessoas incluídas na lista acima referida deverão apresentar-se na recepção do Local dos CONTRATANTES, onde receberão um cartão de visitante ou crachá, que deverão portar de forma visível, durante todo o tempo de permanência nas instalações dos CONTRATANTES.
     25. Se, por qualquer motivo, uma pessoa não incluída na lista precise acessar o site, ele ou ela deverá ser registrado na recepção, mediante apresentação de sua identificação com foto, ou passaporte. A referida pessoa deverá ser acompanhada por um colaborador dos CONTRATANTES, em todos os momentos.
     26. Caso algum membro do pessoal da CONTRATADA, quer previamente autorizado através da lista ou não, necessite acessar áreas sensíveis (tais como salas de servidores, datacenters, armários de rede, etc.), este deverá ser acompanhado por um colaborador dos CONTRATANTES, em todos os momentos.
     27. Se a CONTRATADA necessitar acessar os Locais, fora dos horários de trabalho, os CONTRATANTES deverão informar à CONTRATADA as regras específicas a serem respeitadas.
     28. Designar uma pessoa como responsável pela proteção e descarte seguro dos meios de armazenamento. Caso qualquer mídia de armazenamento precise ser descartada, a CONTRATADA deverá desativá-la de maneira segura, de tal forma que os dados não possam ser recuperados a partir da mesma. A mídia deverá ser descartada utilizando uma terceira parte certificada para realizar descarte seguro, ou destruída fisicamente (após os dados haverem sido apagados) tornando-a completamente inoperante. A desativação / destruição de mídia requer a aprovação prévia dos CONTRATANTES e a posterior notificação por esta à CONTRATADA.
     29. Quando houver a ocorrência de qualquer incidente envolvendo os serviços contratados, execução do CONTRATO e os dados e/ou informações de clientes do CONTRATANTE (e/ou suas próprias informações), a CONTRATADA obriga-se a comunicar imediatamente o CONTRATANTE tomando de imediato todas as medidas que possam minimizar eventuais perdas e danos causados em razão do incidente, além de aplicar os melhores esforços para cessar o incidente com a maior brevidade possível.
  3. Visando a SEGURANÇA DA INFORMAÇÃO, caberá os CONTRATANTES:
     1. Verificar e controlar a qualquer tempo que os produtos fornecidos e/ou serviços prestados pela CONTRATADA estejam em conformidade com o CONTRATO.
     2. Comunicar à CONTRATADA as regras de segurança estabelecidas em conformidade com a legislação aplicável, bem como as regras de acesso.
     3. Autorizar antecipadamente, conforme sua conveniência, o uso de qualquer tipo de mídia de armazenamento, com exceção dos discos rígidos internos e fitas de backup. O uso de mídias de armazenamento removíveis e portáteis, tais como CDs, DVDs, drives USB, Flashdrives, etc., é estritamente proibido.
     4. Autorizar antecipadamente, conforme sua conveniência, todos os ativos de tecnologia da informação dos CONTRATANTES que devam deixar as instalações da CONTRATADA (por exemplo, para reparação). Todas as informações armazenadas no dispositivo deverão ser previamente removidas de forma segura. Se a remoção não for prática ou possível, a CONTRATADA será o responsável principal por proteger os ativos contra uso não autorizado, modificação, divulgação, ou destruição, acidental ou intencional.
     5. Previamente à remoção dos ativos das instalações dos CONTRATANTES, os controles de segurança a estabelecer deverão ser apresentados pelo CONTRATADA e aprovados pelos CONTRATANTES.
     6. Se os ativos tiverem de ser desativados ou descartados, as informações deverão ser destruídas de forma segura, e o processo de descarte deverá estar em conformidade com as leis e regulamentos locais.
  4. Visando a SEGURANÇA DA INFORMAÇÃO, disposições gerais:
     1. As auditorias poderão verificar, especialmente mas não limitando, a: (i) desempenho e qualidade dos serviços prestados; (ii) o cumprimento das obrigações deste CONTRATO, inclusive os níveis de serviços dos mesmos; (iii) teste internos e externos para assegurar o cumprimento das obrigações de acordo com a legislação e o CONTRATO firmado entre as PARTES; e (iv) aplicação de testes internos de penetração na infraestrutura ou aplicativos hospedados.
     2. Independentemente das tarefas contidas diretamente na atividade de serviço de segurança, ou se o serviço incluir atividades de segurança, a CONTRATADA deverá assegurar que todas as atividades do Serviço atendam às Políticas de Segurança da Informação dos CONTRATANTES e às normas e diretrizes de segurança e arquitetura, tanto aquelas existentes no momento da assinatura, quanto àquelas que venham a ser lançadas no futuro.
     3. As atividades de segurança deverão proporcionar proteção contra o uso não autorizado, modificação, divulgação ou destruição, acidental ou intencional, para o patrimônio de dados corporativos, oferecendo trilhas de auditoria adequada, e em conformidade com as leis aplicáveis.
     4. O escopo das atividades de segurança deverá incluir (não se limitando a) os seguintes processos: antivírus, patches [correções] e atualizações, criptografia, configuração de novos usuários, redefinições de senhas, e exclusão ou modificação de contas de usuários.
     5. Qualquer mudança na configuração do ambiente de produção deverá obedecer ao procedimento de autorização. Quando a CONTRATADA for responsável pela configuração e/ou gestão de equipamentos, deverá informar os CONTRATANTES a configuração atual, as alterações propostas, o protocolo de testes, e os resultados dos testes. As alterações de configuração só poderão ser aplicadas após a notificação os CONTRATANTES e sua aprovação.
     6. Todo o desenvolvimento de software deverá incluir um teste de segurança, com a finalidade de evitar a injeção de código malicioso. O processo e os resultados dos testes de segurança da CONTRATADA deverão ser revelados os CONTRATANTES (por exemplo, testes das funções de autenticação, autorização e contabilização, revisões de código-fonte, e quaisquer outras atividades destinadas a validar a arquitetura de segurança)
     7. Desativar imediatamente a totalidade ou parte da funcionalidade do serviço, caso seja identificado um problema de segurança.
     8. A CONTRATADA deverá apresentar um documento da arquitetura proposta, que inclua um completo diagrama da rede do Ambiente dos CONTRATANTES, ilustrando a relação entre o Ambiente dos CONTRATANTES e quaisquer outras redes relevantes, com um fluxograma de dados completo, detalhando onde residem os dados dos CONTRATANTES, os aplicativos que os manipulam, e a segurança dos mesmos. Quaisquer alterações ou atualizações no modelo de comunicação de dados entre CONTRATADA e CONTRATANTES, mudanças significativas e atualizações nas configurações de segurança, deverão ser previamente comunicadas e aprovadas pelos CONTRATANTES.
     9. A rede que hospeda o aplicativo deverá ser fisicamente isolada [air-gapped] de qualquer outra rede ou cliente que a CONTRATADA possa ter.
     10. As instalações de desenvolvimento, testes e operacionais deverão ser isolados uma das outras. A CONTRATADA deverá cumprir as políticas dos CONTRATANTES para a transferência de software do ambiente de desenvolvimento para o ambiente de produção. Software em desenvolvimento e software operacional deverão ser executados em sistemas ou processadores de computador diferentes, e em domínios, diretórios e segmentos de rede diferentes. Compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistema não deverão ser acessíveis a partir de ambientes produção.
     11. Qualquer administrador de sistemas com acesso ao ambiente de desenvolvimento não deverá ter acesso ao ambiente de produção, sem autorização dos CONTRATANTES
     12. A nenhum desenvolvedor deverá ser concedido acesso ao ambiente de produção. Qualquer exceção ocasionada por uma alteração de emergência deverá ser aprovada pelos CONTRATANTES, notificada e devidamente documentada.
     13. O ambiente de testes deverá emular o ambiente operacional do sistema, tanto quanto possível.
     14. Os dados de testes deverão ser protegidos e controlados em conformidade com as políticas dos CONTRATANTES. O Fornecedor não está autorizado a utilizar dados reais ou dados de produção, para testes. Caso se tornem necessárias quaisquer cópias dos dados de produção, cada cópia deverá ser previamente autorizada pelos CONTRATANTES, registrada, e devidamente sanitizada [depurada] / codificada. O processo a ser usado para sanitização e/ou codificação dos dados deverá ser previamente aprovado pelos CONTRATANTES. Logo que os testes sejam concluídos, os dados deverão ser removidos com segurança, do ambiente de testes.
     15. Para todos os ambientes, a CONTRATADA deverá revelar como, e em que medida, os hosts e servidores que compõem a infraestrutura dos CONTRATANTES foram reforçados contra-ataques. A CONTRATADA deverá fornecer uma lista de patches atuais nos hosts, incluindo patches do Sistema Operacional host, de servidores web, de bancos de dados, e de qualquer outro aplicativo material, bem como informações sobre como e quando os patches de segurança serão aplicados. Em caso de dispositivos de rede, laptops e desktops, os CONTRATANTES poderão exigir estas ou quaisquer outras informações. A CONTRATADA deverá revelar os seus processos para monitoramento da integridade e disponibilidade desses hosts.
     16. A CONTRATADA deverá atender à política de senhas dos CONTRATANTES, para a infraestrutura dos CONTRATANTES (incluindo Sistema Operacional, Bancos de dados, e dispositivos de rede que suportem o serviço), incluindo comprimento mínimo de senhas, diretrizes de geração de senhas, e idade de senhas. Contas de usuário e/ou senhas compartilhadas são proibidas. A CONTRATADA deverá revelar o método utilizado para autenticar usuários.
     17. Deverá ser definido um procedimento de acesso de emergência, para o acesso à infraestrutura dos CONTRATANTES. Este processo precisa ser aprovado pelos CONTRATANTES.
     18. A CONTRATADA deverá fornecer informações sobre a geração, manutenção e processo de encerramento de contas, para "contas especiais" (de administração, de serviço, de monitoramento e de manutenção), bem como para contas de usuários. Esta informação deverá abranger a criação de contas, informação de contas e senhas para usuários finais, e revogação de contas.
     19. A CONTRATADA deverá fornecer informações sobre a sua política de logs, incluindo as configurações de logs implementadas, e procedimento de revisão.
     20. Assim que o serviço prestado termine (vencimento do contrato), a CONTRATADA deverá entregar duas cópias das informações dos CONTRATANTES e realizar de forma segura a destruição das informações armazenadas. O acesso deverá ser imediatamente revogado, e a CONTRATADA não será mais autorizado a acessar o patrimônio de informações dos CONTRATANTES.
     21. A CONTRATADA deverá revelar a forma pela qual irá autenticar os usuários (por exemplo, LDAP, Netegrity, Certificados de Cliente).
     22. A CONTRATADA deverá fornecer informações sobre a sua política de senhas para a infraestrutura de aplicativos dos CONTRATANTES, incluindo comprimento mínimo de senhas, diretrizes de geração de senhas, e a frequência com que as senhas serão alteradas.
     23. A CONTRATADA deverá revelar a forma pela qual protege as senhas, quando armazenadas e transmitidas dentro da infraestrutura de aplicativos dos CONTRATANTES, e a forma pela qual destrói as informações, quando não tenham mais utilidade.
     24. A CONTRATADA poderá ser obrigada a revelar os arquivos de configuração específicos, para qualquer sistema associado às funções de suporte (tais como mecanismos de busca ou bases de dados) e detalhes técnicos (linguagens de programação, etc.) sobre o(s) aplicativo(s).
     25. Os equipamentos que hospedem patrimônio de Tecnologia da Informação dos CONTRATANTES deverão estar localizados em uma instalação fisicamente segura. Será requerido, no mínimo, o controle por crachás, para acesso à instalação. O patrimônio de Tecnologia da Informação dos CONTRATANTES deverá estar localizado em um ambiente do tipo sala cofre.
     26. O CONTRATANTE deverá deter o poder de decisão final, a respeito de quem estará autorizado a entrar em qualquer ambiente físico fechado e acessar o patrimônio de Tecnologia da Informação dos CONTRATANTES. A CONTRATADA deverá revelar a lista do pessoal autorizado a acessar o ambiente de hospedagem do patrimônio de Tecnologia da Informação dos CONTRATANTES. Todos os controles de segurança física deverão ser verificados regularmente.
     27. O procedimento de autorização para o processo de colocação em produção deverá respeitar as políticas e procedimentos de tecnologia da informação dos CONTRATANTES. Os Testes de Aceitação do Usuário (que serão responsabilidade e prerrogativa dos CONTRATANTES, independentemente do suporte necessário para realizar estas tarefas) deverão ser realizados antes de qualquer mudança na produção.
     28. O acesso ao código-fonte de programas e itens associados (tais como projetos, especificações, planos de verificação e planos de validação) deverá ser estritamente controlado. Bibliotecas de programas-fonte não deverão ser mantidas em sistemas em operação, e qualquer exceção a esta regra deverá ser aprovada pelos CONTRATANTES. Todas as atualizações de bibliotecas de programas-fonte e itens associados, bem como a emissão de fontes de programas para os programadores, deverão ser executadas somente após a devida autorização haver sido recebida.
     29. Um Acordo de Custódia deverá ser firmado entre CONTRATANTES e Fornecedor com a finalidade de proteger os investimentos de tecnologia dos CONTRATANTES, através da garantia da manutenção do software, ou do acesso ao código-fonte. O Fornecedor deverá propor, discutir e celebrar um Acordo apropriado com os CONTRATANTES definindo explicitamente como: o depósito do código-fonte do software em uma conta mantida por uma terceira parte, como agente depositário; as condições detalhadas, sob as quais o código-fonte será liberado, permitindo os CONTRATANTES acessá-lo caso o licenciador se declare insolvente, ou deixe de manter e atualizar o software, conforme prometido no contrato de licença de software.
     30. A CONTRATADA deverá gerenciar todas as medidas necessárias para assegurar a continuidade do serviço, em conformidade com o SLA [Service Level Agreement / Acordo de Níveis de Serviço] definido, incluindo a aplicação das atualizações e "patches" [correções] necessárias para hardware e software, conforme recomendação de cada Fornecedor de Tecnologia.
     31. A CONTRATADA deverá oferecer regularmente as recomendações necessárias para garantir a compatibilidade com as últimas versões de software, hardware, e software distribuído comercialmente, à medida que tais versões sejam autorizadas no âmbito dos CONTRATANTES e executar as atividades recomendadas, tão logo seja possível, após obtida a aprovação dos CONTRATANTES.
     32. O serviço incluirá gestão de backup e restauração: designadamente, um serviço de planejamento, implantação e testes dos procedimentos de recuperação (incluindo login pelos usuários finais) necessários para restabelecer a funcionalidade do Serviço, Sistema Operacional do sistema, bancos de dados, aplicativos, e dados dos usuários, em caso de uma falha.
     33. Gerenciar todas as medidas necessárias para assegurar a continuidade do serviço objeto deste CONTRATO.
     34. A CONTRATADA deverá informar regularmente as recomendações necessárias para garantir a compatibilidade com as últimas versões de software, hardware, e software distribuído comercialmente, à medida que tais atualizações das versões sejam autorizadas por escrito pelos CONTRATANTES, a CONTRATADA deverá executar as atividades recomendadas, passando os documentos trocados pela PARTES, em razão do disposto neste item serão parte integrante do CONTRATO.
     35. Ao firmar o presente instrumento, a CONTRATADA compromete-se a observar, durante a execução dos serviços de desenvolvimento/manutenção nos Sistemas Aplicativos dos CONTRATANTES, o Anexo IA - Ciclo de Vida de Desenvolvimento de Software - SDLC .
     36. O Guia de Desenvolvimento Seguro poderá ser, a critério dos CONTRATANTES, atualizado de tempos em tempos. Havendo atualizações, no momento da solicitação de proposta comercial, os CONTRATANTES disponibilizarão à CONTRATADA a última versão do mencionado guia.
     37. Eventuais manutenções, aperfeiçoamentos, atualizações e/ou modificações cuja execução seja necessária para garantir que os serviços de desenvolvimento/manutenção estejam em conformidade com o Guia de Desenvolvimento Seguro e, ainda, com a legislação aplicável e/ou às demais normas expedidas por qualquer autoridade governamental competente, serão realizados pela CONTRATADA, sem qualquer ônus os CONTRATANTES. A responsabilidade da CONTRATADA pelo cumprimento das normas bem como da legislação aplicável vigorará por tempo indeterminado.
     38. A CONTRATADA concorda que: (a) deverá entregar os CONTRATANTES, além do Código-Fonte, a Documentação referente a cada desenvolvimento.
     39. A CONTRATADA concorda que: (b) Os Sistemas Aplicativos, incluindo seus programas, aperfeiçoamentos, adaptações, correções e demais funcionalidades desenvolvidas pela CONTRATADA, sob encomenda dos CONTRATANTES, em decorrência do Contrato, assim como a respectiva Documentação são de propriedade intelectual total e definitiva dos CONTRATANTES.
     40. A CONTRATADA concorda que: (c) Os CONTRATANTES é a única legitimada a promover qualquer registro relacionado aos dados, informações, relatórios ou quaisquer outros documentos criados pela CONTRATADA no cumprimento do objeto do Contrato, podendo realizar tais registros da maneira que julgar conveniente, para resguardar ou salvaguardar seus direitos de exclusiva proprietária;
     41. A CONTRATADA concorda que: (d) A CONTRATADA, desde já, compromete-se a fornecer para os CONTRATANTES toda e qualquer informação ou documento necessário para a realização dos registros mencionados no item (b) acima;
     42. A CONTRATADA concorda que: (e) A CONTRATADA somente poderá fazer uso de qualquer Material Pré-Existente para a prestação dos serviços, se obtiver prévia autorização por escrito dos CONTRATANTES. Caso os CONTRATANTES expressamente autorize a utilização de Material Pré-Existente para o desenvolvimento de um determinado Sistema Aplicativo, a CONTRATADA deverá ceder os CONTRATANTES, o direito perpétuo de utilização de referido Material Pré-Existente que não possa ser obtido/licenciado diretamente pelos CONTRATANTES e que seja necessário à absorção da tecnologia e à compilação dos Sistemas Aplicativos desenvolvidos sob o Contrato;