**Anexo 1b – Cláusulas de Segurança – Condições Gerais**

**APÊNDICE** – Cláusula de Segurança da informação aos seguintes objetos contratuais: Desenvolvimento de Software, Fornecimento de Software (ex.: sistema ERP), SaaS (Software as a Service), Hospedagem, Software distribuído comercialmente (ex.: pacote Office), Fornecimento de Hardware, Fornecimento de Rede e Monitoramento, Operação, Administração ou Suporte de Sistemas e Aplicativos

**I)**             **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 da CONTRATANTE, 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 da CONTRATANTE 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 da CONTRATANTE. A terceira parte será responsável pela segurança do dispositivo, através de antivírus e patches, para proteger o patrimônio de informações da CONTRATANTE. Qualquer dispositivo pertencente a uma terceira parte, e que armazene ativos de informações da CONTRATANTE, deverá ser criptografado.

2.1. Somente usuários autorizados pela CONTRATANTE poderão acessar as informações e dados contidos na infra-estrutura da CONTRATANTE ou na infra-estrutura de terceiros contratados ou utilizados pela CONTRATANTE. A CONTRATANTE deverá deter o poder de decisão final, a respeito de quem estará autorizado a acessar os dados e informações, incluindo o próprio pessoal da CONTRATANTE, 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 da CONTRATANTE.

2.2. Serão concedidas somente autorizações de acessos individuais (login e senha). Contas genéricas ou compartilhadas são absolutamente proibidas.

2.3. Dados ou informações sobre a CONTRATANTE, ou contidos na infraestrutura da CONTRATANTE, 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 da CONTRATANTE.

**II)**            **Visando a SEGURANÇA DA INFORMAÇÃO, caberá a CONTRATADA:**

1.    Obedecer às normas, procedimentos e Políticas de Tecnologia da Informação da CONTRATANTE, 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 da CONTRATANTE.

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.

3.1. As alterações relativas aos aplicativos, arquitetura, procedimentos operacionais, procedimentos de segurança e sua respectiva avaliação de riscos, deverão ser comunicadas antecipadamente.

4.    Oferecer a sua máxima cooperação, para permitir que a CONTRATANTE realize a verificação de conformidade dos produtos fornecidos e/ou serviços prestados.

5.    Atender aos requisitos de governança de tecnologia da informação da CONTRATANTE, 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.

6.    Responsabilizar-se exclusivamente perante o CONTRATANTE sobre todas as considerações de segurança de TI. Sob nenhuma circunstância, a CONTRATANTE assumirá ou aceitará o compartilhamento de responsabilidade entre o Fornecedor e qualquer outra terceira parte, incluindo parceiros de negócios e subcontratados do Fornecedor.

7.    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.

8.    Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE de qualquer responsabilidade.

9.    Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE 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 pela CONTRATANTE.

11. Não deverá estabelecer qualquer tipo de link de comunicação de dados entre as suas redes e sistemas e os da CONTRATANTE, 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 da CONTRATANTE.

12. Garantir que o ambiente de Tecnologia da Informação, em seu lado, assegure a integridade, disponibilidade e confidencialidade do patrimônio de Tecnologia da Informação da CONTRATANTE, incluindo dados, informações e direitos de propriedade intelectual.

12.1.            Somente usuários autenticados e autorizados, com uma data de expiração de usuário pré-definida, deverão ter permissão para acessar sistemas da CONTRATANTE e o prazo de acesso deverá ser restrito.

12.2.            Deverão ser mantidos logs de auditoria completos, nos níveis de conexão, sistema operacional, e aplicativos. A CONTRATANTE se reserva o direito de supervisionar em tempo real, gravar e utilizar os dados armazenados das conexões.

12.3.            Todas as conexões com a CONTRATADA deverão ser criptografadas e serão estabelecidas somente através de firewalls da CONTRATANTE. Somente serão permitidos hosts e protocolos previamente autorizados.

13. Notificar imediatamente a CONTRATANTE, 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 da CONTRATANTE.

13.1.            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 da CONTRATANTE.

13.2.            Todas as informações de propriedade da CONTRATANTE deverão ser enviadas à CONTRATANTE, em duas cópias, sendo em seguida removidas com segurança de todos os dispositivos.

14. Rever a qualquer tempo o acesso de seus empregados ao patrimônio de informações da CONTRATANTE, e prontamente corrigir qualquer discrepância em potencial. Mediante solicitação da CONTRATANTE, a CONTRATADA deverá revelar os resultados da última análise de acessos, bem como as respectivas ações corretivas.

15. Não utilizar qualquer criptografia desenvolvida internamente, para proteger as informações, os aplicativos ou a infra-estrutura da CONTRATANTE. Quaisquer algoritmos simétricos, assimétricos, ou de hashing, utilizado na infra-estrutura da CONTRATANTE, deverá utilizar algoritmos e ferramentas bem conhecidos, publicados, apresentados à comunidade global de criptografia, e adotados como padrão da indústria.

15.1.            A resistência dos algoritmos de criptografia deverá ser a mais alta possível, aprovada pelo CSO [Chief Security Officer / Chefe de Segurança] local da CONTRATANTE, e em conformidade com os requisitos de negócios da CONTRATANTE e com a legislação aplicável.

15.2.            Conexões que utilizem a Internet deverão ser protegidas utilizando tecnologias de criptografia, adotados como padrão de mercado.

15.3.            Deverão ser criptografados todos os dispositivos móveis e portáteis utilizados para prover o serviço à CONTRATANTE e que contenham dados confidenciais.

16. Prover a CONTRATANTE uma lista com os nomes e funções dos funcionários que terão acesso aos Locais da CONTRATANTE. Pessoas incluídas na lista acima referida deverão apresentar-se na recepção do Local da CONTRATANTE, onde receberão um cartão de visitante ou crachá, que deverão portar de forma visível, durante todo o tempo de permanência nas instalações da CONTRATANTE.

16.1.            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 da CONTRATANTE, em todos os momentos.

16.2.            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 da CONTRATANTE, em todos os momentos.

16.3.            Se a CONTRATADA necessitar acessar os Locais, fora dos horários de trabalho, a CONTRATANTE deverá informar à CONTRATADA as regras específicas a serem respeitadas.

17. 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 da CONTRATANTE e a posterior notificação por esta à CONTRATADA.

**III)**          **Visando a SEGURANÇA DA INFORMAÇÃO, caberá ao CONTRATANTE:**

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 da CONTRATANTE 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.

4.1. Previamente à remoção dos ativos das instalações da CONTRATANTE, os controles de segurança a estabelecer deverão ser apresentados pela CONTRATADA e aprovados pela CONTRATANTE.

4.2. 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.

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 infra-estrutura ou aplicativos hospedados.

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 da CONTRATANTE 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.

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.

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.

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 a CONTRATANTE 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 à CONTRATANTE e sua aprovação.

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 à CONTRATANTE (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)

Desativar imediatamente a totalidade ou parte da funcionalidade do serviço, caso seja identificado um problema de segurança.

A CONTRATADA deverá apresentar um documento da arquitetura proposta, que inclua um completo diagrama da rede do Ambiente da CONTRATANTE, ilustrando a relação entre o Ambiente da CONTRATANTE e quaisquer outras redes relevantes, com um fluxograma de dados completo, detalhando onde residem os dados da CONTRATANTE, os aplicativos que os manipulam, e a segurança dos mesmos. Quaisquer alterações ou atualizações no modelo de comunicação de dados entre CONTRATADA e CONTRATANTE, mudanças significativas e atualizações nas configurações de segurança, deverão ser previamente comunicadas e aprovadas pela CONTRATANTE.

A rede que hospeda o aplicativo deverá ser fisicamente isolada [air-gapped] de qualquer outra rede ou cliente que a CONTRATADA possa ter.

As instalações de desenvolvimento, testes e operacionais deverão ser isolados uma das outras. A CONTRATADA deverá cumprir as políticas da CONTRATANTE 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.

Qualquer administrador de sistemas com acesso ao ambiente de desenvolvimento não deverá ter acesso ao ambiente de produção, sem autorização da CONTRATANTE

A nenhum desenvolvedor deverá ser concedido acesso ao ambiente de produção. Qualquer exceção ocasionada por uma alteração de emergência deverá ser aprovada pela CONTRATANTE, notificada e devidamente documentada.

O ambiente de testes deverá emular o ambiente operacional do sistema, tanto quanto possível.

Os dados de testes deverão ser protegidos e controlados em conformidade com as políticas da CONTRATANTE. 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 pela CONTRATANTE, registrada, e devidamente sanitizada [depurada] / codificada. O processo a ser usado para sanitização e/ou codificação dos dados deverá ser previamente aprovado pela CONTRATANTE. Logo que os testes sejam concluídos, os dados deverão ser removidos com segurança, do ambiente de testes.

Para todos os ambientes, a CONTRATADA deverá revelar como, e em que medida, os hosts e servidores que compõem a infra-estrutura da CONTRATANTE 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, a CONTRATANTE poderá exigir estas ou quaisquer outras informações. A CONTRATADA deverá revelar os seus processos para monitoramento da integridade e disponibilidade desses hosts.

A CONTRATADA deverá atender à política de senhas da CONTRATANTE, para a infraestrutura da CONTRATANTE (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.

Deverá ser definido um procedimento de acesso de emergência, para o acesso à infra-estrutura da CONTRATANTE. Este processo precisa ser aprovado pela CONTRATANTE.

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.

A CONTRATADA deverá fornecer informações sobre a sua política de logs, incluindo as configurações de logs implementadas, e procedimento de revisão.

Assim que o serviço prestado termine (vencimento do contrato), a CONTRATADA deverá entregar duas cópias das informações da CONTRATANTE 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 da CONTRATANTE.

A CONTRATADA deverá revelar a forma pela qual irá autenticar os usuários (por exemplo, LDAP, Netegrity, Certificados de Cliente).

A CONTRATADA deverá fornecer informações sobre a sua política de senhas para a infra-estrutura de aplicativos da CONTRATANTE, incluindo comprimento mínimo de senhas, diretrizes de geração de senhas, e a freqüência com que as senhas serão alteradas.

A CONTRATADA deverá revelar a forma pela qual protege as senhas, quando armazenadas e transmitidas dentro da infra-estrutura de aplicativos da CONTRATANTE, e a forma pela qual destrói as informações, quando não tenham mais utilidade.

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).

Os equipamentos que hospedem patrimônio de Tecnologia da Informação da CONTRATANTE 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 da CONTRATANTE deverá estar localizado em um ambiente do tipo sala cofre.

A 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 da CONTRATANTE. A CONTRATADA deverá revelar a lista do pessoal autorizado a acessar o ambiente de hospedagem do patrimônio de Tecnologia da Informação da CONTRATANTE. Todos os controles de segurança física deverão ser verificados regularmente.

O procedimento de autorização para o processo de colocação em produção deverá respeitar as políticas e procedimentos de tecnologia da informação da CONTRATANTE. Os Testes de Aceitação do Usuário (que serão responsabilidade e prerrogativa da CONTRATANTE, independentemente do suporte necessário para realizar estas tarefas) deverão ser realizados antes de qualquer mudança na produção.

Gestão de Identidades, Acessos e Senhas

Deve ter funcionalidade de política de senha

Qualidade na composição da senha

Expiração de senha

Histórico de senha

Bloqueio de usuário após tentativas de login com senha incorretas

Nomenclatura do login deve seguir padrão definido pela CNI

Transmissão (Comunicação)

Utilização de protocolo seguro para comunicação entre cliente-servidor (HTTPS, SSL, SSH)

Utilização de protocolos seguros para transmissão de arquivos ou informações (SFTP, HTTPS, SCP)

Logs de Auditoria

Deve possuir trilha de auditoria de acessos (logon / logoff / data / ip )

Deve possuir trilha de auditoria e rastreabilidade de TODAS as transações e ações críticas (usuário / ip / hora / data / etc / histórico de alteração)

Controles de Integridade e Confidencialidade

Deve possuir controles que garantam a integridade das informações

Deve possuir solução de criptografia implantada para proteção de arquivos sensíveis ou confidenciais durante o armazenamento

Deve possuir solução de criptografia implantada para proteção de arquivos sensíveis ou confidenciais durante a transmissão

O banco de dados deve utilizar criptografia no armazenamento dos dados sensíveis ou confidenciais

Controle de Acesso Físico

Acesso ao Datacenter restrito a pessoal autorizado

Segurança no Desenvolvimento

O desenvolvimento do sistema deve seguir padrões de segurança, garantindo que não existam ao menos as TOP 10 vulnerabilidades apontadas pela OWASP

Toda a parte web da solução deverá estar protegida por um web application firewall.

Código fonte do Sistema deverá ser entregue a CNI (Caso seja uma solução de mercado, não se aplica)

Testes de intrusão devem ser realizados anualmente (se sistema crítico deve ser realizado semestralmente)

O Sistema deve possuir ambiente de Homologação compatível com o ambiente em produção

O Sistema deve possuir ambiente de desenvolvimento / testes unitários

Os dados utilizados nos ambiente de desenvolvimento e homologação devem ser descaracterizados/mascarados

Os colaboradores da fábrica que desenvolvem não devem ser os mesmos que suportam o ambiente

Os colaboradores da fábrica devem possuir usuários específicos, nominais e nomeados para dar o suporte, sem privilégios especiais em ambiente produtivo

O Fornecedor deverá utilizar ferramenta de Análise de Segurança em Código Fonte e ao final do desenvolvimento entregar relatório da ferramenta que comprovem que não existam riscos CRÍTICOS e ALTOS.

Disponibilidade

Os servidores de Aplicação devem possuir algum tipo de contingência

A política de Backup da aplicação deve ser adequada aos requisitos do negócio quanto à obrigações legais, periodicidade, retenção das informações, tempo de recuperação esperado, ponto de recuperação esperado (por exemplo: ao restaurar o ambiente, ter as informações de 2 horas antes do incidente)

Deve ser definido um calendário de testes periódicos de restore para garantir a integridade das cópias de segurança

CNI

Possuir processo para solicitação formal de concessão de acesso (workflow, formulário, email, etc) \*Responsável por aprovar solicitação não deve ser a mesma equipe responsável por criar o acesso

Possuir processo de workflow de aprovação/criação/solicitação de acesso

Processo de revisão periódica de acessos

Processo de revogação de acessos

Matriz de segregação de função (se necessário)