Portuguese

Requisitos de Segurança da Informação do Fornecedor

1. Introdução

O fornecedor concorda que ele e terceiros, agindo em seu nome para fornecer serviços e produtos à CWT, devem cumprir com os requisitos de segurança da informação contidos neste documento ("**Requisitos de Segurança da Informação**"), que definem as medidas de segurança da informação necessárias ("**Medidas de Segurança Organizacionais e Técnicas**")

2. Definições

2.1 Salvo indicação explícita em contrário indicada ou ampliada no presente documento, os termos definidos terão o mesmo significado como estabelecido no Acordo principal. Os seguintes termos tal como definidos serão aplicáveis aos Requisitos de Segurança da Informação:

"**Afiliados**", salvo definição em contrário no Contrato, significa, com referência a uma das Partes, qualquer empresa ou outra pessoa jurídica que: (i) controle, de maneira direta ou indireta, uma das Partes; ou (ii) seja controlada, direta ou indiretamente, por uma das Partes; ou (iii) seja controlada direta ou indiretamente por uma empresa ou entidade que controle direta ou indiretamente uma Parte. Para tais fins, "controle" significa o direito de exercer mais de 50% (cinquenta por cento) dos votos ou direito similar de propriedade; mas apenas pelo tempo que tal controle continue a existir.

"Contrato", salvo definição em contrário nos termos principais do contrato, significa o contrato ou outro documento jurídico celebrado pela CWT e o Fornecedor.

"Informação Confidencial" significa qualquer tipo de informação comercialmente sensível, patenteada ou confidencial relacionada com (a) a CWT e suas afiliadas; com (b) um cliente da CWT; (c) funcionários da CWT, (d) parceiros independentes e joint ventures da CWT ou (e) o conteúdo ou objetivos do Contrato, sejam orais, escritos ou que por qualquer outro meio tenha chegado direta ou indiretamente ao Fornecedor ou estiver na posse de funcionário do Fornecedor, agentes, contratados ou subcontratados como resultado ou em conexão com o Acordo. Para que não restem dúvidas, todo produto de trabalho constitui Informação Confidencial.

"CWT", salvo definição em contrário no Contrato, é a entidade indicada no Acordo, bem como suas afiliadas.

"**Zona Desmilitarizada**" ou "**DMZ**" é uma rede ou subrede que fica entre uma rede interna confiável, como uma rede local privada (LAN) da empresa, e uma rede externa não confiável, como a Internet pública. A DMZ ajuda a evitar que usuários externos obtenham acesso direto aos sistemas internos e a outros recursos.

"Processo de Gestão de Incidentes" é um processo e procedimento documentado desenvolvido pelo Fornecedor a ser seguido em caso de ataque real ou suspeito, ingerência, acesso não autorizado, perda e qualquer outro tipo de violação que envolva a confidencialidade, disponibilidade ou integridade das Informações Confidenciais e Dados Pessoais.

"Ocultação" é o processo de cobertura de informação exibida na tela.

"Dispositivos móveis e portáteis" significa computadores, dispositivos, mídia e sistemas móveis e portáteis capazes de serem facilmente transportados, movidos ou enviados que são usados em conexão com o Contrato. Os dispositivos móveis e portáteis incluem: computadores portáteis, tablets, discos rígidos, USB, cartões de memória USB, Personal Digital Assistants (PDAs), telefones celulares ou de dados, assim como

qualquer outro dispositivo ou periférico sem fio com capacidade de armazenar Informações Confidenciais e Dados Pessoais.

"Dados Pessoais", salvo definição em contrário no Contrato, significa conforme é definido na Norma da União Europeia (EU) 2016/679, e em outas leis em vigor sobre segurança global de informação, proteção de dados e leis de privacidade, significa qualquer tipo de informação relativa a uma pessoa física identificada ou identificável, que pode ser identificada direta ou indiretamente, por referência a um número de identificação ou a um ou mais fatores que sejam específicos à sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

"Portal de Segurança" é um conjunto de mecanismos de controle entre duas ou mais redes com diferentes níveis de confiança que filtram e registram o tráfego que passa, ou tenta passar, entre as redes, servidores administrativos e de gestão associados. Exemplos de Portal de Segurança incluem firewalls, servidores de gerenciamento de firewall, hops, controladores de margem de sessão, servidores proxy e dispositivos de prevenção de intrusão.

"Autenticação Forte" significa o uso de mecanismos e metodologias de autenticação mais fortes do que as senhas exigidas. Exemplos de mecanismos e metodologias de Autenticação Forte incluem certificados digitais, duplos fatores de autenticação e senhas descartáveis.

"Criptografia Forte" significa o uso de tecnologias de criptografia com comprimentos mínimos de chave de 256 bits para criptografia simétrica e 1024 bits para criptografia assimétrica cuja força oferece garantia razoável de que irá proteger a informação criptografada contra o acesso não autorizado e é suficiente para proteger a confidencialidade e privacidade das informações criptografadas, e que também incorpora uma política documentada para o gerenciamento das chaves de criptografia e processos associados adequados para proteger a confidencialidade e a privacidade das chaves e senhas usadas como entradas para o algoritmo de criptografia. A Criptografia Forte inclui, entre outros: SSL v3.0+/TLS v1.0+, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (apenas para o governo dos Estados Unidos), RSA 1024 bit, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 ou WPA2.

"Medidas de Segurança de Informação Técnicas e Organizacionais" significa quaisquer atividades inerentes aos Requisitos de Segurança de Informação para acessar, administrar, transferir, processar, armazenar, reter e destruir dados ou informações; divulgar e notificar as Partes afetadas exigidos nos termos do Acordo e nos termos das leis de proteção de dados e de privacidade aplicáveis; e para salvaguardar informações ou dados para assegurar disponibilidade, integridade, confidencialidade e privacidade ou notificar indivíduos sobre qualquer tipo de falha na proteção de tais informações ou dados. As medidas incluem, entre outros, às exigidas ou entendidas como tal pelas Diretivas da União Europeia 94/46/CE e 2006/24/CE, como promulgada pelos países membros, pela lei Gramm-Leach Bliley (GLBA) dos Estados Unidos, pela lei Health Insurance Portability e Accountability (HIPAA - Portabilidade e Responsabilidade dos Seguros de Saúde) dos Estados Unidos, as normas de sigilo de dados da União Europeia e da Suíça e outras leis internacionais e dos EUA, a interpretação jurídica oficial ou a jurisprudência relativa a informações ou aos dados ao abrigo do Acordo.

"**Terceiros",** salvo definição em contrário no Contrato, significa quaisquer subcontratados e cada um dos funcionários temporários, empreiteiras ou fornecedores adicionais do Fornecedor assim como agentes que estejam agindo em nome do Fornecedor, e não inclui qualquer definição de Terceiros em vigor na União Europeia, nos Estados Unidos, ou nos termos de qualquer outra legislação internacional.

" **Fornecedor**" é a entidade contratante indicada no Acordo, juntamente com suas Afiliadas e seus Terceiros.

2.2 O Fornecedor declara que cumprirá as seguintes Medidas de Segurança Organizacionais e Técnicas, na medida em que elas são aplicáveis à prestação de serviços estabelecidas no Acordo:

3. Organização da Segurança da Informação

O Fornecedor deverá:

3.1 Estabelecer, implementar e manter, de modo consistente com as práticas do setor, porém de modo algum inferior às políticas razoáveis, assim como um programa de Medidas de Segurança Organizacionais e Técnicas, organizacionais, operacionais, administrativas adequadas para (1) impedir acesso a Informações Confidenciais ou Dados Pessoais que não seja autorizado pelo Contrato ou por esses Requisitos de Segurança da informação e (2) cumprir e atender a todas as normas aplicáveis do setor. O Fornecedor deve garantir também que os seus funcionários têm experiência suficiente em segurança da informação.

3.2 Fornecer um nível adequado de supervisão, orientação e treinamento sobre as Medidas de Segurança Organizacionais e Técnicas para a equipe do fornecedor que necessita ter acesso a Informações Confidenciais e Dados Pessoais. O Fornecedor deve oferecer também treinamento sobre as Medidas de Segurança Organizacionais e Técnicas no momento da contratação e antes de acessar as Informações Confidenciais e os Dados Pessoais. Serão oferecidos cursos de reciclagem pelo menos uma vez por ano e logo que sejam feitas alterações materiais nas Medidas de Segurança Organizacionais e Técnicas do Fornecedor.

3.3 A equipe do Fornecedor que possuam importantes funções de segurança, incluindo, entre outras, funções de recursos humanos ou de tecnologia da informação e qualquer outra função de administrador de tecnologia, também deverão receber treinamento especializado específico para cada uma das suas respectivas funções. O treinamento especializado incluirá, conforme aplicável à função, os procedimentos de segurança da informação, o uso aceitável de recursos de segurança da informação, ameaças atuais aos sistemas de informação, recursos de segurança dos sistemas específicos e procedimentos seguros de acesso.

3.4 Tomar as medidas adequadas para impedir o acesso não autorizado e perda de Informações Confidenciais e de Dados Pessoais, assim como aos serviços, sistemas, dispositivos ou meios que contenham tais informações.

3.5 Empregar processos e procedimentos de avaliação de risco para examinar regularmente os sistemas usados para fornecer serviços ou produtos à CWT. O Fornecedor deve também remediar tais riscos logo que for possível de maneira proporcional ao nível de risco das ameaças contra a Informação Confidencial e Dados Pessoais conhecidos no momento da identificação. Executar o processo necessário para a equipe do Fornecedor a relatar riscos ou incidentes suspeitos à equipe de segurança do Fornecedor.

3.6 Na medida em que o Fornecedor preste serviços nos termos do Contrato nas instalações da CWT ou use serviços, sistemas, dispositivos ou meios que sejam de propriedade, operados ou administrados pela CWT, cumprir com todas as normas da CWT aplicáveis a esse acesso que sejam disponibilizadas ao Fornecedor. O Fornecedor também notificará prontamente a CWT por escrito, quando tal acesso não for mais necessário, incluindo, entre outros, quando um funcionário, empreiteiro, subempreiteiro ou Terceiros de Fornecedor não estiverem mais prestando serviços no âmbito do Acordo ou quando não estiverem mais acessando as Informações Confidenciais e os Dados Pessoais.

3.7 Manter os registros dos recursos do Fornecedor que acessem, transfiram, mantenham, armazenem ou processem Informações Confidenciais e Dados Pessoais.

3.8 Cumprir os requisitos de verificação de antecedentes da CWT, na medida do necessário e do permitido por lei, assim como de outro modo estabelecido em declaração de trabalho/ ordem de serviço/ordem de compra aplicável.

4. Segurança Física e Ambiental

O Fornecedor deverá:

4.1 Garantir que todos os sistemas e outros recursos do Fornecedor que forem ser usados por vários usuários encontram-se em instalações físicas seguras com acesso limitado e restrito apenas a pessoas autorizadas.

4.2 Monitorar e registrar o acesso às instalações físicas que contenham sistemas e outros recursos destinados ao uso de vários usuários, em conexão com o desempenho das obrigações do Fornecedor no âmbito do Contrato.

4.3 Garantir que toda a equipe do Fornecedor assine um acordo de não divulgação ou confidencialidade com o Fornecedor antes de acessar Informações Confidenciais e Dados Pessoais.

4.4 Determinar a todos os seus funcionários que adotem a política de mesas limpas e telas bloqueadas na estação de trabalho, antes de saírem da área de trabalho.

4.5 Recolher todos os ativos da empresa assim que o trabalho tiver sido finalizado ou quando o contrato for rescindido.

4.6 Limitar e monitorar o acesso físico às suas instalações de acordo com os seguintes requisitos:

a. O acesso de visitantes será registrado, sendo tal registro mantido por três (3) meses, incluindo o nome do visitante, da empresa que ele representa e o nome do funcionário que autorizar o seu acesso físico.
b. O acesso é restrito ao pessoal competente, com base no acesso devido à necessidade de saber.
c. Todos os funcionários devem usar o crachá fornecido pela empresa.
d. O acesso será imediatamente revogado após a rescisão do contrato e todos os dispositivos de acesso físico, como chaves, cartões de acesso, etc., serão devolvidos ou desativados.
e. O centro de dados ou sala de informática ficará fechada, ficando a entrada limitada àqueles que precisem ter acesso para executar as suas funções de trabalho.
f. Onde permitido por lei, usar câmeras de vídeo para monitorar o acesso físico individual a áreas sensíveis e analisar tais dados com regularidade. As imagens de vídeo devem ser armazenadas durante um mínimo de 3 (três) meses.

g. Os equipamentos utilizados para armazenar, processar ou transmitir Informações Confidenciais e Dados Pessoais devem ser protegidos fisicamente, como por exemplo, os pontos de acesso wireless, portais, dispositivos portáteis, hardware de redes e de comunicações e linhas de telecomunicações.

4.7 Implementar controles para minimizar o risco e proteger contra ameaças físicas.

4.8 Zelar por todos os equipamentos processando ou manuseando Informações Confidenciais e Dados Pessoais sejam feitos em conformidade com os requisitos de manutenção recomendados pelo prestador de serviços de Terceiros.

4.9 Restringir logicamente a sala de conferências e as outras tomadas de rede acessíveis ao público da rede do Fornecedor, cujo acesso ficará restrito apenas a usuários autenticados ou será desativado por padrão.

4.10 Proteger os dispositivos de captura de dados de cartões de pagamento via interação física direta contra adulteração e substituição. Isto será feito por meio de inspeção periódica das superfícies do dispositivo a fim de detectar adulteração ou substituição. Além disso, oferecerá treinamento para que os funcionários se conscientizem das tentativas de adulteração ou de substituição de dispositivos.

4.11 Separar e fiscalizar os pontos de acesso das áreas de entrega e de carga assim como outros pontos de todos os centros de acesso, gerenciamento, armazenamento e processamento das Informações Confidenciais e Dados Pessoais.

4.12 Deve ter equipamentos de aquecimento, refrigeração, supressão de incêndio, detecção de água, calor e de fumaça.

5. <u>Controle de Acesso</u>

O Fornecedor deverá:

5.1 Tomar todas as medidas necessárias para impedir que as Informações Confidenciais e Dados Pessoais sejam acessadas de qualquer forma e com finalidade diversa dos termos do Contrato e que não tenham sido autorizadas pela CWT. O Fornecedor também deverá limitar o acesso às Informações Confidenciais e Dados Pessoais à equipe do Fornecedor que (1) precisem acessar as Informações Confidenciais e Dados Pessoais para prestar serviços relacionados ao Acordo, e (2) tenham concordado por escrito em proteger a integridade, disponibilidade e confidencialidade das Informações Confidenciais e Dados Pessoais.

Manter procedimentos adequados para interromper o acesso às Informações Confidenciais e Dados Pessoais fornecidos para a equipe do Fornecedor, quando já não são mais necessárias ou relevantes para o bom desempenho das suas funções antes do fim do trabalho pelo fornecedor ou do contrato com a CWT.

5.2 Separar as informações da CWT que venham de outros clientes ou das próprias aplicações e informações do Fornecedor, por meio de servidores separados fisicamente ou, alternativamente, usando controles de acesso lógico onde a separação física dos servidores não tenha sido implementada.

5.3 Identificar e exigir que os proprietários adequados analisem e aprovem o acesso aos sistemas utilizados para obter, processar, controlar ou armazenar Informações Confidenciais e Dados Pessoais, e manter e acompanhar as aprovações de acesso.

5.4 Remover o acesso a sistemas de gerenciamento das Informações Confidenciais e Dados Pessoais 24 horas após o término da relação de trabalho entre empregado, empreiteiro, subempreiteiro ou Terceiros com o Fornecedor, bem como remover o acesso a tais sistemas no prazo de 3 (três) dias úteis, quando houver mudanças no nível de responsabilidades da função dentro da empresa. Todas as outras IDs de usuário devem ser desativadas ou removidas após 90 dias de inatividade.

5.5 De forma sistemática, rever e aprovar o acesso aos sistemas de gerenciamento de Informações Confidenciais e Dados Pessoais pelo menos a cada trimestre, para remover o acesso não autorizado.

5.6 Li

5.7 Restringir o acesso do administrador do sistema (também conhecido como root, privilegiado, ou superusuário) a sistemas operacionais destinados a ser utilizados por vários usuários apenas àqueles indivíduos que necessitem desse acesso de alto nível para o bom desempenho das suas tarefas. Sempre que possível utilizar IDs de check-out com credenciais de acesso (log-in) e registros de atividades para gerenciar os acessos de alta segurança, além de reduzir o acesso de alto nível a um número bastante limitado de usuários.

5.8 Solicitar aos administradores de aplicativos, banco de dados, rede e sistema que limitem o acesso dos usuários apenas aos comandos, dados, sistemas e outros recursos necessários para a execução das funções autorizadas.

5.9 Exigir Autenticação Forte para qualquer acesso remoto.

5.10 Proibir e empregar Medidas de Segurança Organizacionais e Técnicas a fim de garantir que a equipe do Fornecedor com acesso às Informações Confidenciais e Dados Pessoais não possam copiar, mover ou armazenar Informações Confidenciais e Dados Pessoais em discos rígidos locais, nem cortar e colar ou imprimir as Informações Confidenciais e Dados Pessoais.

5.11 Ativar o uso de recursos de acesso remoto somente quando necessário, monitorar durante o uso e desativar imediatamente após o uso.

5.12 Quando for necessário usar os recursos de fornecedores internos contendo Informações Confidenciais da CWT, exigir que haja, no mínimo, um duplo fator de autenticação.

6. Identificação e Autenticação

O Fornecedor deverá:

6.1 Atribuir IDs de usuário exclusivos para usuários individuais e designar mecanismos de autenticação a cada conta individual.

6.2 Utilizar processo de gerenciamento do ciclo de vida da ID para usuário documentado, incluindo, entre outros, procedimentos para a criação de conta aprovada, remoção da conta em tempo hábil e modificação de conta (por exemplo, alterações de privilégios, prazo de acesso, funções e tarefas) para todos os acessos a Informações Confidenciais e Dados Pessoais e em todos os ambientes (por exemplo, produção, teste, desenvolvimento, etc.). Esse processo incluirá a revisão dos privilégios de acesso e a validade da conta pelo menos a cada trimestre.

6.3 Aplicar a regra do menor privilégio (ou seja, limitar o acesso aos comandos, informações, sistemas e outros recursos necessários para executar as funções autorizadas de acordo com a função exercida pelo funcionário).

6.4 Restringir todos os acessos às Informações Confidenciais e aos Dados Pessoais às pessoas com um ID de usuário e senha válidos e requerer que os IDs de usuário específicos empreguem um dos seguintes procedimentos: senha ou frase de acesso, duplo fator de autenticação ou um valor biométrico.

6.5 Exigir nível de complexidade da senha e preencher os seguintes requisitos de construção da senha: um mínimo de oito (8) caracteres para senhas do sistema e quatro (4) caracteres nas senhas para tablet e smartphones. As senhas do sistema devem conter três (3) dos seguintes pontos: letras maiúsculas e minúsculas, números ou caracteres especiais. As senhas também não devem ser iguais à ID do usuário à qual elas estão associadas. Além disso, tampouco devem incluir uma palavra dicionarizada, números sequenciais ou repetidos e não podem ser idênticos às últimas cinco senhas. Exigir a expiração da senha em intervalos regulares que não ultrapassem 90 (noventa) dias. Ocultar todas as senhas quando exibidas.

6.6 Limitar o número de tentativas frustradas de acesso para, no máximo, (5) cinco tentativas a cada 24 horas, e bloquear a conta de usuário ao atingir esse limite de maneira persistente. O acesso à conta de usuário pode ser reativado posteriormente por processo manual que exija a verificação da identidade do usuário.

6.7 Verificar a identidade do usuário e definir um tempo de uso e de redefinição de senhas num valor exclusivo para cada usuário. Sistematicamente, pedir mudança após a primeira utilização.

6.8 Usar um método seguro para o envio de credenciais de autenticação (senhas) e dos mecanismos de autenticação (p.ex., tokens e cartões inteligentes).

6.9 As senhas da conta de serviço e de proxy devem ter, no mínimo, 12 caracteres, com letras maiúsculas, minúsculas e caracteres numéricos, bem como símbolos especiais. A conta de serviço e as senhas de proxy devem ser alteradas pelo menos uma vez por ano.

6.10 Após um período de inatividade de, no máximo, quinze (15) minutos, encerrar as sessões interativas ou ativar um protetor de bloqueio de tela seguro que requeira autenticação.

6.11 Usar um método de autenticação com base no nível de sensibilidade das Informações Confidenciais ou Dados de Usuário. Sempre que as credenciais de autenticação forem armazenadas, protegê-las com uma Criptografia Forte.

6.12 Configurar sistemas para encerrar automaticamente após um período máximo de inatividade: servidor (15 minutos), estação de trabalho (15 minutos), dispositivo móvel (4 horas), Dynamic Host Configuration Protocol (7 dias), Virtual Private Network (24 horas).

7. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

O Fornecedor deverá:

7.1 Para os produtos ou serviços com a marca CWT, ou para produtos e software desenvolvidos para a CWT, exibir advertência nas telas ou páginas de acesso, conforme especificado por escrito pela CWT.

7.2 Certificar-se de que todo o pessoal, que possa estar executando trabalhos no âmbito do Acordo estejam em conformidade com as Medidas de Segurança Organizacionais e Técnicas, que devem ser comprovadas por um Contrato por escrito no mínimo tão restritivo quanto os presentes Requisitos de Segurança de Informação.

7.3 Retornar todos os dispositivos de propriedade ou de acesso da CWT, assim que possível, no máximo dentro de 15 (quinze) dias após:

(a) o término ou rescisão do Acordo;
(b) O pedido da CWT para o retorno de tais bens; ou
(c) a data em que o Fornecedor não precisar mais de tais dispositivos.

7.4 Empregar uma metodologia efetiva de gerenciamento de aplicativos que incluam medidas de segurança organizacionais e técnicas no processo de desenvolvimento de software, e garantir que as medidas de segurança organizacionais e técnicas, tal como representado no ciclo de desenvolvimento de software da CWT, ou nas políticas de segurança da informação, padrões e procedimentos, sejam implementados em tempo hábil pelo Fornecedor.

7.5 Seguir os procedimentos padronizados de desenvolvimento, incluindo a separação de acesso e de código entre os ambientes de não-produção e os ambientes de produção e a segregação associada de funções entre tais ambientes.

7.6 Certificar-se de os controles internos de segurança da informação para o desenvolvimento de software sejam avaliados regularmente e que reflitam as melhores práticas da indústria, além de revisar e implementar esses controles em tempo hábil.

7.7 Fazer o gerenciamento da segurança do processo de desenvolvimento e verificar se as práticas de codificação seguras estão sendo implementadas e seguidas, incluindo-se os controles adequados de criptografia, proteção contra códigos maliciosos, e um processo de aferição interpares.

7.8 Realizar testes de penetração em aplicativos funcionalmente completos antes de serem liberados para produção e depois disso, pelo menos uma vez por ano, e após qualquer tipo de modificação significativa no código-fonte ou na configuração que se alinhem com OWASP, CERT, SANS Top 25 e PCI-DSS. Corrigir quaisquer vulnerabilidades exploráveis antes da implantação no ambiente de produção.

7.9 Usar dados anônimos ou ocultos em ambientes de não-produção. Nunca usar dados de produção em texto simples em ambiente de não-produção e jamais usar Informações Confidenciais e Dados Pessoais em ambientes de não produção, por qualquer motivo que seja. Verificar se todos os dados de teste e contas foram removidos antes de lançar a versão completa.

7.10 Verificar se o Fornecedor que esteja usando código de fonte aberto, software, aplicativos ou serviços faz as verificações devidas durante a revisão do código, para determinar se há falhas, erros, ou problemas de segurança que possam afetar a integridade, a disponibilidade ou a confidencialidade dos dados da CWT ou dos seus clientes. O fornecedor também deve notificar a CWT onde é usado o código-fonte aberto e fornecer à CWT o nome e a versão do código-fonte aberto.

7.11 Garantir que o Fornecedor não compartilhará, em qualquer circunstância, qualquer código que tenha sido criado no âmbito do Acordo, qualquer que seja o estágio de desenvolvimento, em ambiente compartilhado ou não privado, como por exemplo um repositório de código de acesso aberto, independentemente do nível de proteção da senha.

8. Software e Integridade de Dados

O Fornecedor deverá:

8.1 Instalar em ambientes em que o programa de antivírus esteja comercialmente disponível software antivírus atualizado e funcionando a fim de procurar e prontamente remover ou colocar em quarentena vírus e outros tipos de malware que sejam encontrados no sistema ou dispositivo.

8.2 Separar as informações e recursos de não-produção dos programas e recursos de produção.

8.3 Verificar se as equipes estão usando um processo de controle de alterações bem documentado em todas as alterações do sistema, incluindo os procedimentos de saída (back-out) em todos os ambientes de produção e processos de mudança de emergência. Incluir testes, documentação e aprovações para todas as alterações do sistema e exigir a aprovação da gerência quando houver mudanças significativas em tais processos.

8.4 Criar e manter uma zona PCI no caso de o Fornecedor processar ou armazenar os dados de titulares do cartão.

8.5 No caso de aplicativos que utilizem banco de dados que permitam modificações a Informações Confidenciais e Dados Pessoais, ter e manter habilitados os recursos de registro de auditoria das transações de banco de dados e os registros de auditoria das transações do banco de dados por um período mínimo de seis (6) meses.

8.6

8.7 Rever o software para buscar e corrigir vulnerabilidades de segurança durante a implementação inicial e após modificações e atualizações significativas.

8.8 Realizar testes de garantia de qualidade para os componentes de segurança (por exemplo, testes de identificação, autenticação e funções de autorização), bem como qualquer outra atividade destinada a validar a arquitetura de segurança, durante a implementação inicial e após modificações e atualizações significativas.

9. Segurança do Sistema

O Fornecedor deverá:

9.1 Regularmente criar e atualizar as versões mais recentes de diagramas de sistema e de fluxo de dados usados para acessar, processar, gerenciar ou armazenar Informações Confidenciais e Dados Pessoais.

9.2 Monitorar de forma ativa os recursos da indústria (p.ex.,, {www.cert.org e as listas de mala direta e websites do fornecedor de software) para notificar de maneira oportuna todos os alertas de segurança aplicáveis referentes aos sistemas do Fornecedor e outros recursos de informação.

9.3 Administrar de maneira eficaz as chaves criptográficas, reduzindo o acesso às chaves ao menor número possível de pessoas, armazenar as chaves criptográficas secretas e privadas por meio de chave de criptografia pelo menos tão forte quanto a chave de criptografia de dados e armazenar em local separado da chave de criptografia de dados em um dispositivo criptográfico, no menor número de locais possíveis. Modificar as chaves de criptografia do padrão na instalação e também, pelo menos, de dois em dois anos, além de eliminar de maneira segura as chaves antigas.

9.4 Verificar os sistemas voltados para o exterior e outros recursos de informação, incluindo, entre outros , redes, servidores e aplicativos, com software padrão da indústria de escaneamento de vulnerabilidades de segurança, a fim de descobrir possíveis vulnerabilidades de segurança no mínimo a cada trimestre e antes da liberação para aplicativos e mudanças significativas e quaisquer atualizações, de acordo com os cronogramas de análises de risco baseados em políticas e normas de TI geralmente aceitas.

9.5 Verificar os sistemas internos e outros recursos de informação, Incluindo, entre outros, redes, servidores, aplicativos e banco de dados, com software padrão da indústria de escaneamento de vulnerabilidades de segurança, a fim de descobrir vulnerabilidades de segurança e verificar que tais sistemas e outros recursos sejam reforçados adequadamente, e identificar as redes sem fio ilegais no mínimo a cada trimestre e antes da liberação para aplicativos e mudanças significativas e ainda atualizações, de acordo com os cronogramas de análises de risco baseados em políticas e normas de TI geralmente aceitas.

9.6 Manter um processo de classificação de risco para as conclusões da avaliação de vulnerabilidade com base nas melhores práticas da indústria e impacto potencial. Todos os resultados da que apresentem pontuação CVSS de 4 ou superior devem ser tratados através de um método formalizado para garantir que a continuidade da avaliação de risco é gerenciada.

9.7 Verificar se todos os sistemas e outros recursos do Fornecedor são e permanecem mais "rígidos", incluindo, entre outros, a remoção e a desativação de rede não utilizada e outros serviços e produtos (por exemplo, finger, rlogin, ftp e serviços e produtos simples de Protocolo de Controle de Transmissão e Protocolo de Internet (TCP/IP) e a instalação de firewall no sistema, wrappers de Protocolo de Controle de Transmissão (TCP) ou tecnologia semelhante.

9.8 Implantar um ou mais Sistemas de Detecção de Intrusão (IDS), Sistemas de Prevenção de Intrusão (IPS) ou Detecção de Intrusão e Sistemas de Prevenção (IDP) em um modo de funcionamento ativo que monitore todo o tráfego de entrada e saída dos sistemas e outros recursos em conjunto com o Acordo em ambientes em que tal tecnologia esteja comercialmente disponível e, na medida do possível,.realizável.

9.9 Manter um processo de classificação de risco para corrigir vulnerabilidades de segurança em qualquer sistema ou em outro recurso, incluindo, entre outros, aqueles que forem descobertos por intermédio de publicações da indústria, escaneamento de vulnerabilidades, detecção de vírus, bem como à análise de registros de segurança e aplicar patches de segurança adequados prontamente relacionado à probabilidade de que tais vulnerabilidades possam estar sendo ou estão em vias de começar a ser exploradas. Patches críticos com pontuação CVSS de 7,5 ou mais devem ser imediatamente instalados após a disponibilidade e em nenhum caso mais de um mês após o lançamento. Patches com uma pontuação CVSS de 4 ou mais devem ser instalados no prazo de 90 dias de lançamento.

9.10 Realizar testes de penetração generalizada, interna e externamente, pelo menos uma vez por ano, sempre que houver atualização ou modificação significativa de infraestrutura e de aplicativos.

9.11 Remover ou desativar software não autorizado descoberto em sistemas do Fornecedor e usar controles padrão de malware no setor, incluindo a instalação, atualização regular e uso rotineiro de programas antimalware em todos os serviços, sistemas e dispositivos que possam ser usados para acesso às Informações Confidenciais e Dados Pessoais. Usar os melhores e mais confiáveis programas de antivírus sempre que possível e verificar que as definições de vírus estejam sempre atualizadas.

9.12 Manter os softwares atualizados em todos os serviços, sistemas e dispositivos que possam ser usados para acessar Informações Confidenciais e Dados Pessoais, inclusive a manutenção adequada do(s) sistema(s) operacional(is) e a instalação correta de patches de segurança atualizados.

9.13 Atribuir responsabilidades de administração de segurança para configurar sistemas operacionais hosts a indivíduos específicos.

9.14 Alterar todos os nomes de conta padrão e as senhas padrão.

10. Monitoramento

O Fornecedor deverá:

10.1 Reter dados de registro de Informações Confidenciais e Dados Pessoais durante pelo menos doze (12) meses e verificar que tais dados estejam disponíveis para a CWT em tempo hábil e sempre que solicitado, a menos que seja especificado em outro item do Contrato.

10.2 Registrar as atividades do sistema primárias nos sistemas que contenham qualquer tipo de Informações Confidenciais e Dados Pessoais.

10.3 Restringir o acesso aos registros de segurança apenas às pessoas autorizadas e protegerá os registros de segurança contra modificações não autorizadas.

10.4 Implementar um mecanismo de detecção de alterações (por exemplo, monitoramento de integridade dos arquivos) a fim de alertar funcionários a respeito de modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo. Configurar o software para realizar comparações semanais de arquivos críticos.

10.5 Rever, pelo menos uma vez por semana, todos os registros de auditoria relativos à segurança em sistemas que contenham Informações Confidenciais e Dados Pessoais buscando anomalias, a fim de documentar e resolver todos os problemas de segurança encontrados no menor tempo possível.

10.6 Rever todos os eventos de segurança, registros de componentes do sistema de armazenamento, processamento e transmissão de dados do titular do cartão, registros de componentes críticos do sistema e registros dos servidores e dos componentes do sistema que executam funções de segurança diariamente.

11. \Portais de segurança

O Fornecedor deverá:

11.1 Exigir Autenticação Forte para acesso administrativo e de gerenciamento aos Portais de Segurança, Incluindo, entre outros, acessos com a finalidade de analisar os arquivos dos registros.

11.2 Implantar e usar controles, políticas, processos e procedimentos documentados a fim de garantir que usuários não autorizados não tenham acesso administrativo ou de gerenciamento aos Portais de Segurança, e que os níveis de autorização do usuário para administrar e gerenciar Portais de Segurança sejam adequados.

11.3 Pelo menos uma vez a cada seis (6) meses, garantir que as configurações do Portal de Segurança sejam mais rígidas, selecionando uma amostra dos Portais de Segurança e verificar que cada uma das regras padrão definidas e o conjunto de parâmetros de configuração garantam o seguinte:

a. Que o roteamento de origem do Protocolo de Internet (IP) esteja desativado,
b. Que o endereço de loopback esteja proibido de entrar na rede interna,
c. Que estejam implementadas os filtros antispoofing (contra falsificação de pacotes),
d. Que os pacotes de transmissão não possam entrar na rede,
e. Que os redirecionamentos de Internet Control Message Protocol (ICMP) estejam desativados.
f. Que todos os conjuntos de regras terminem com uma declaração "DENY ALL", e
g. Que cada regra seja feita com base em um pedido de negócio específico.

11.4 Assegurar-se que as ferramentas de monitoramento são utilizadas para validar que todos os aspectos dos Portais de Segurança (por exemplo, hardware, firmware e software) estejam operacionais de maneira contínua.

11.5 Garantir que todos os Portais de Segurança são configurados e implementados de maneira que todos os Portais de segurança não operacionais devem negar acesso.

11.6 Assegurar que os pacotes de entrada da rede externa não confiável devem terminar dentro da zona desmilitarizada ("**DMZ**"), e não devem fluir diretamente para a rede interna confiável. Todos os pacotes de entrada que fluam para a rede interna confiável devem ser originários apenas da DMZ. A DMZ deve estar separada da rede externa não confiável por intermédio de um Portal de Segurança, e deve ser separada da rede interna confiável por uso:

a. de outro Portal de Segurança, ou
b. do mesmo Portal de Segurança utilizado para separar a DMZ da rede externa não confiável e, neste caso, o Portal de Segurança deve garantir que os pacotes recebidos pela rede externa não confiável sejam excluídos imediatamente, ou quando não excluídos, devem ser encaminhados apenas para a DMZ sem nenhum outro processamento desses pacotes de entrada a não ser a inscrição dos pacotes em um registro.

Os seguintes só devem ser localizados dentro da rede interna confiável:

a. Quaisquer Informações Confidenciais ou Dados Pessoais armazenados sem o uso de criptografia forte,
b. A cópia do registro oficial de informação a ser acessada a partir de solicitações provenientes da rede externa não confiável,
c. A cópia do registro oficial de informação a ser modificada como resultado de solicitações provenientes da rede externa não confiável,
d. Servidores de banco de dados,
e. Todos os registros exportados e
f. Todos os ambientes utilizados para o desenvolvimento, teste, sandbox, produção e outros ambientes semelhantes; além de todas as versões do código-fonte.

11.7 Credenciais de autenticação que não estejam protegidas pelo uso de Criptografia Forte não devem ser localizadas dentro da DMZ.

12. Segurança de Rede

O Fornecedor deverá:

12.1 Mediante solicitação da CWT, fornecer à CWT um diagrama de rede lógica que documente sistemas e ligações a outros recursos, incluindo roteadores, interruptores, firewalls, sistemas de IDS, topologia da rede, pontos de conexão externos, portais, redes sem fio, e quaisquer outros dispositivos que devem dar apoio à CWT.

12.2 Manter um processo formal para aprovar, testar e documentar todas as conexões de rede e alterações às configurações do firewall e do roteador. Configurar firewalls para bloquear e registrar pacotes suspeitos, além de permitir apenas o tráfego adequado e autorizado, negando qualquer outro tráfego por intermédio do firewall. Rever as regras do firewall a cada seis meses.

12.3 Instalar um firewall em cada conexão da Internet e entre qualquer DMZ e a zona da rede interna. Todos os sistemas de armazenamento de Informações Confidenciais e Dados Pessoais devem residir na zona interna da rede, separada da DMZ e de outras redes não confiáveis.

12.4 Monitorar o firewall no perímetro e internamente, para controlar e proteger o fluxo de tráfego de rede entrando ou saindo da fronteira ou divisa, conforme necessário.

12.5 Manter um processo e controles documentados para detectar e lidar com tentativas não autorizadas de acesso às Informações Confidenciais e Dados Pessoais.

12.6 Ao fornecer serviços e produtos baseados na Internet para CWT, proteger as Informações Confidenciais e Dados Pessoais por meio da implementação de uma rede DMZ. Os servidores Web que prestam serviço a CWT devem residir na DMZ. Os recursos de informações ou sistema que armazenem as Informações Confidenciais e Dados Pessoais (tais como servidores de aplicativos e banco de dados) devem residir em uma rede interna confiável. (Serviços e produtos de Internet devem usar DMZ).

12.7 Restringir o tráfego de saída não autorizada do processamento de aplicações, armazenamento ou transmissão de Informações Confidenciais e Dados Pessoais a endereços IP dentro da DMZ e Internet.

12.8 Ao utilizar tecnologias de rede sem fio baseadas em rádio frequência (RF) para executar ou dar suporte a produtos para a CWT, assegurar que todas as Informações Confidenciais e Dados Pessoais transmitidos estão protegidos por tecnologias de criptografia forte que sejam suficientes para salvaguardar a confidencialidade das Informações Confidenciais e os Dados Pessoais. Regularmente verificar, identificar e desativar pontos de acesso sem fio não autorizados.

13. Requisitos de conectividade

O Fornecedor deverá:

13.1 No caso em que já tenha recebido, ou vá receber, conectividade com recursos de Informações Confidenciais e Dados Pessoais juntamente com o Contrato:

a. Utilizar apenas as instalações e metodologias de conexão ajustadas para interligar os recursos de Informações Confidenciais e Dados Pessoais da CWT com os Recursos do Fornecedor.

b. Não estabelecer a interligação com os recursos de Informações Confidenciais e Dados Pessoais da CWT sem o consentimento prévio da CWT.
c. Fornecer à CWT acesso às instalações do Fornecedor durante o horário comercial para manutenção e suporte de equipamentos (p.ex., roteador) fornecido pela CWT no âmbito do Acordo para conectividade aos recursos de Informações Confidenciais e Dados Pessoais da CWT.
d. Utilizar todos os equipamentos fornecidos pela CWT no âmbito do Acordo para conectividade dos recursos de Informações Confidenciais e Dados Pessoais apenas para fornecimento desses serviços e produtos ou para funções expressamente autorizados no Contrato.
e. Se a metodologia de conectividade ajustada exigir que o Fornecedor implemente o Portal de Segurança, deverão ser mantidos registros de todas as sessões que utilizam tal Portal de Segurança. Os registros de sessão devem incluir informações suficientemente detalhadas para identificar o usuário final ou aplicativo, o endereço do IP de origem, endereço IP de destino, protocolos de serviço e portas utilizados e a duração do acesso. Esses registros da sessão devem ser mantidos por um período mínimo de seis (6) meses a partir da criação da sessão.

13.2 No caso em que o Fornecedor tenha, ou venha a receber, conectividade com os recursos de Informações Confidenciais e Dados Pessoais nos termos do Acordo, além dos outros direitos estabelecidos neste documento, autorizações da CWT para:

a. Reunir informações relativas ao acesso, incluindo o acesso do Fornecedor aos recursos de Informações Confidenciais e Dados Pessoais. Esta informação pode ser coletada, mantida e analisada pela CWT para identificar potenciais riscos de segurança sem aviso prévio. Esta informação pode incluir arquivos de rastreamento, estatísticas, endereços de rede e os dados reais ou telas acessados ou transferidos.
b. Imediatamente suspender ou encerrar qualquer interconexão aos recursos de Informações Confidenciais e Dados Pessoais caso a CWT, a seu critério, acreditar que houve uma violação de segurança ou acesso não autorizado ou ainda mau uso dos recursos de dados da CWT ou qualquer informação, sistemas ou outros recursos da CWT.

14. Dispositivos móveis e portáteis

O Fornecedor deverá:

14.1 Usar Criptografia Forte para proteger todas as Informações Confidenciais e Dados Pessoais armazenados em dispositivos móveis e portáteis.

14.2 onfidenciais e Dados Pessoais em dispositivos móveis ou laptops e não armazenar Informações Confidenciais e Dados Pessoais em dispositivos removíveis, a menos que se esteja usando Criptografia Forte.

14.3 Usar Criptografia Forte para proteger as Informações Confidenciais e Dados Pessoais transmitidas por dispositivos móveis e portáteis que sejam rede-cientes.
a. Ao usar dispositivos móveis e portáteis rede-cientes que não sejam computadores portáteis para acesso ou armazenagem de Informações Confidenciais e Dados Pessoais, tais dispositivos devem ser capazes de apagar todas as cópias armazenadas das Informações Confidenciais e Dados Pessoais após o recebimento via rede de um comando corretamente autenticado. (Obs.: Essa capacidade é geralmente chamada de capacidade de eliminação remota.
b. Ter políticas, procedimentos e normas documentadas em vigor de maneira a garantir que a pessoa autorizada que deve estar no controle físico de um dispositivo móvel e portátil rede-ciente que não seja um computador portátil e que esteja armazenando Informações Confidenciais e Dados Pessoais inicie imediatamente a eliminação de todas as Informações Confidenciais e Dados Pessoais quando o dispositivo for perdido ou roubado.

c. Ter políticas, procedimentos e normas documentadas em vigor de maneira a garantir que os dispositivos móveis e portáteis que não sejam laptops computador e que não sejam rede-cientes excluam automaticamente todas as cópias armazenadas das Informações Confidenciais e Dados Pessoais após tentativas consecutivas de acesso sem êxito.

14.4 Implementar políticas, procedimentos e padrões de maneira a garantir que os Dispositivos Móveis e Portáteis usados para acessar e/ou armazenar as Informações Confidenciais e Dados Pessoais:

a. Estejam na posse física de indivíduos autorizados;
b. Estejam fisicamente seguros quando não estiverem na posse física das pessoas autorizadas; ou
c. Tenham os dados armazenados rapidamente excluídos quando não estiverem na posse física de indivíduos autorizados, ou quando não estiverem fisicamente seguros, ou após 10 tentativas de acesso sem sucesso.

14.5 Antes de permitir o acesso às Informações Confidenciais e Dados Pessoais armazenados em ou por intermédio de celulares e dispositivos portáteis, ter e usar um processo para garantir que:

a. O usuário está autorizado para esse acesso; e
b. A identidade do usuário foi autenticada.

14.6 Implementar uma política que proíba o uso de dispositivos móveis e portáteis que não sejam administrados ou geridos pelo Fornecedor ou pela CWT para acessar ou armazenar Informações Confidenciais e Dados Pessoais.

14.7 Rever, no mínimo anualmente, o uso e os controles de todos os dispositivos móveis e portáteis administrados ou gerenciados pelo Fornecedor, para garantir que os dispositivos móveis e portáteis atendam às Medidas de Segurança Técnicas e Organizacionais aplicáveis.

15. Segurança no Trânsito

O Fornecedor deverá:

15.1 Usar criptografia forte para a transferência de Informações Confidenciais e Dados Pessoais para fora das redes controladas pela CWT ou pelo Fornecedor, ou ao transmitir Informações Confidenciais e Dados Pessoais por intermédio de qualquer rede não confiável.

15.2 Para registros contendo Informações Confidenciais e Dados Pessoais em papel, microficha ou meios eletrônicos a serem transferidos fisicamente, transportá-los por mensageiro seguro ou outro método de entrega que possa ser rastreado, embalado de forma segura, de acordo com as especificações do fabricante. As Informações Confidenciais e Dados Pessoais devem ser transportados em contêineres trancados.

16. Segurança em Repouso

O Fornecedor deverá:

16.1 Usar Criptografia Forte para proteger Informações Confidenciais e Dados Pessoais quando armazenados.

16.2 Não armazenar Informações Confidenciais e Dados Pessoais eletronicamente fora do ambiente de rede do Fornecedor (ou da própria rede de computador seguro da CWT), a menos que o dispositivo

de armazenamento (p.ex., fita de backup, laptop, cartão de memória, disco de computador, etc.) seja protegido por Criptografia Forte.

16.3 Não armazenar Informações Confidenciais e Dados Pessoais em mídia removível (p.ex., unidades flash USB, pen drives, cartões de memória, fitas, CDs ou discos rígidos externos), exceto: (a) para backup, continuidade de negócios, recuperação de desastres e para fins de intercâmbio de dados conforme permitido e necessário nos termos do contrato, e (b) usando Criptografia Forte.

16.4 Armazenar de forma adequada e segura os registros contendo Informações Confidenciais e Dados Pessoais em papel ou microfilme em áreas cujo acesso é restrito ao pessoal autorizado.

16.5 A menos que a CWT dê outras instruções, por escrito, ao coletar, gerar ou criar Informações Confidenciais e Dados Pessoais em suporte de papel e mídia de backup para a CWT, por intermédio ou em nome da CWT ou sob a marca CWT, assegurar que tais informações devem ser Informações Confidenciais e Dados Pessoais e, sempre que possível, rotular tais informações da CWT como "Confidenciais". O Fornecedor reconhece que as Informações Confidenciais e Dados Pessoais permanecerão sendo Informações Confidenciais e Dados Pessoais de propriedade da CWT, independentemente de possuir ou não uma etiqueta.

17. Devolução, Destruição e Descarte

O Fornecedor deverá:

17.1 A pedido da CWT e sem custo adicional, providenciar cópias de qualquer uma das Informações Confidenciais e Dados Pessoais para a CWT 30 (trinta) dias após pedido. O Fornecedor também deverá devolver ou, a critério da CWT, destruir todas as Informações Confidenciais e Dados Pessoais da CWT, incluindo cópias eletrônicas e impressas, conforme definido no Contrato, ou caso não seja especificado no Contrato, dentro de 90 (noventa) dias, imediatamente após o que ocorrer primeiro: (a) término ou rescisão do acordo, (b) pedido da CWT para devolução das Informações Confidenciais e Dados Pessoais ou (c) a data em que o Fornecedor não mais necessitar das Informações Confidenciais e Dados Pessoais para fornecer serviços e produtos no âmbito do Acordo.

17.2 Caso a CWT aprove a destruição como alternativa à devolução das Informações Confidenciais e dos Dados Pessoais, certificar por escrito a destruição como equivalente a tornar irrecuperáveis as Informações Confidenciais e Dados Pessoais. Destruir completamente todas as cópias das Informações Confidenciais e Dados Pessoais da CWT em todos os locais e em todos os sistemas onde as Informações Confidenciais e Dados Pessoais estiverem armazenadas, incluindo, entre outros, os Terceiros do Fornecedor previamente aprovados. Essas informações devem ser destruídas de acordo com as normas para destruição completa DOD 5220.22M ou da Publicação Especial NIST 800-88, ou ainda usando-se um produto de desmagnetização recomendado pelo fabricante para o sistema afetado. Antes da destruição, manter todas as Medidas de Segurança Técnicas e Organizacionais aplicáveis para proteger a segurança, a privacidade e a confidencialidade das Informações Confidenciais e Dados Pessoais.

17.3 Proceder à eliminação das Informações Confidenciais e Dados Pessoais de forma a assegurar que a informação não possa ser reconstruída em formato utilizável. Papéis, slides, microfilmes, microfichas e fotografias devem ser eliminados por trituração cruzada ou incineração. Materiais que contenham Informações Confidenciais e Dados Pessoais aguardando destruição devem ser armazenados em recipientes seguros e ser transportados por um Terceiro seguro.

18. Retenção

O Fornecedor deverá:

18.1 Validar os requisitos adequados de retenção com os contatos da CWT, antes de obter qualquer Informação Confidencial e Dados Pessoais e de maneira condizente com qualquer declaração de trabalho ou ordem de compra.

18.2 Proteger cópias de segurança das Informações Confidenciais e Dados Pessoais criadas automaticamente pelos serviços, sistemas, dispositivos ou mídia do Fornecedor ("**Cópias de Arquivo**"). Salvo disposição em contrário do Contrato, em 90 (noventa) dias corridos a contar da expiração ou do término do Contrato ou antes desse prazo, caso solicitado de maneira justificada pela CWT, destruir de forma segura todas as cópias de arquivo de Informações Confidenciais e Dados Pessoais, seguindo um procedimento padrão da indústria que seja, pelo menos, tão restritivo quanto o DOD 5220.22M ou o NIST Publicação Especial 800- 88.

19. Resposta a Incidentes e Notificação

O Fornecedor deverá:

19.1 Possuir e fazer uso de Processo de Gerenciamento de Incidentes e procedimentos conexos e equipar os Processos de Gerenciamento de Incidentes e procedimentos com recursos especializados. Avisar a CWT, de preferência imediatamente, ou no máximo em 24 (vinte e quatro) horas, sempre que houver ataque, invasão, acesso não autorizado, perda e qualquer outro incidente suspeito ou confirmado relacionado à informação, sistemas ou outros recursos da CWT.

19.2 Depois de notificar a CWT, fazer atualizações regulares da situação durante o incidente, informando as medidas que forem sendo tomadas em resposta ao incidente, em intervalos ajustados mutuamente e, assim que possível após o fim do incidente, apresentar à CWT um relatório por escrito descrevendo o incidente, as ações tomadas pelo Fornecedor durante a sua resposta e quais as ações futuras planejadas a fim de evitar que ocorra outro incidente semelhante.

Não relatar ou divulgar publicamente a violação da informação, dos sistemas ou de outros recursos da CWT sem primeiro notificar a CWT. Trabalhar diretamente em conjunto com a CWT para notificar os serviços pertinentes em nível regional, nacional, estadual e os representantes do governo e serviços locais de monitoramento de crédito, as pessoas afetadas pela violação e outros meios de comunicação, conforme exigido por lei.

a. Implementar um processo para identificar imediatamente as pessoas da sua equipe que foram responsáveis pelas violações de controles de segurança, incluindo os controles determinados nos Requisitos de Segurança das Informações.. As pessoas da equipe do Fornecedor que forem identificadas estarão sujeitas às ações disciplinares apropriadas, tal como determinado por lei. Não obstante o indicado acima, a equipe do Fornecedor permanecerá sob a autoridade do Fornecedor. A CWT não deverá ser considerada como empregadora do pessoal do Fornecedor.

20. Gerenciamento da Continuidade dos Negócios e Recuperação de Desastres

O Fornecedor deverá:

20.1 Desenvolver, operar, gerenciar e revisar a continuidade dos negócios e os planos de recuperação de desastres, a fim de minimizar o impacto dos serviços ou produtos do Fornecedor para a CWT. Os planos devem incluir: recursos específicos para a Continuidade dos Negócios e as funções de Recuperação de Desastres, os objetivos determinados de prazo de recuperação e de ponto de recuperação, back-up diário de dados e sistemas, armazenamento fora do local do backup dos

registros e da mídia, proteção dos registros e planos de contingência proporcionais aos requisitos do Acordo,. armazenar esses planos de forma segura fora do local e garantir que esses planos estejam disponíveis para o Fornecedor conforme necessário.

20.2 Mediante solicitação da CWT, fornecer à CWT um plano de continuidade de negócio documentado que garanta que o Fornecedor poderá cumprir com as suas obrigações contratuais no âmbito do Acordo, incluindo os requisitos das declarações de trabalho ou acordo de nível de serviço. Esses planos devem colocar em andamento a recuperação e, ao mesmo tempo, proteger a integridade e a confidencialidade das Informações Confidenciais e Dados Pessoais.

20.3 Ter procedimentos documentados para backup e recuperação seguros das Informações Confidenciais e Dados Pessoais que devem incluir, no mínimo, procedimentos para o transporte, armazenamento e eliminação das cópias de backup das Informações Confidenciais e Dados Pessoais e, a pedido da CWT, fornecer tais procedimentos documentados para a CWT.

20.4 Garantir que os backups de todas as Informações Confidenciais e Dados Pessoais armazenados ou o software e as configurações para sistemas utilizados pela CWT sejam criados, no mínimo, uma vez por semana.

20.5 Pelo menos uma vez por ano ou após qualquer mudança significativa nos planos de Continuidade dos Negócios ou de Recuperação de Desastres, aplicar tais planos de maneira ampla, por conta e risco exclusivo do Fornecedor. Esses exercícios devem assegurar o bom funcionamento das tecnologias impactadas e a conscientização interna de tais planos.

20.6 Prontamente rever o seu Plano de Continuidade dos Negócios para abordar os cenários e as fontes de ameaças adicionais ou emergentes e fornecer à CWT um resumo de alto nível dos planos e testes em tempo hábil, mediante solicitação.

20.7 Garantir que todos os locais de armazenagem ou processamento das Informações Confidenciais e Dados Pessoais de propriedade do Fornecedor ou por ele contratados sejam monitorados 24 horas por dia, 7 (sete) dias por semana contra a invasão, fogo, água e outros perigos ambientais.

21. Conformidade e Credenciamentos

O Fornecedor deverá:

21.1 Manter registros completos e precisos referentes ao desempenho das suas obrigações decorrentes dos Requisitos de Segurança da Informação e a conformidade do Fornecedor em formato a permitir uma avaliação ou auditoria por um período mínimo de três (3) anos, como exigido nos termos de uma ordem judicial ou processo civil ou regulamentar. Não obstante o indicado acima, só será exigido do Fornecedor que mantenha os registros de segurança por um período mínimo de seis (6) meses de desempenho contínuo Acordo.

21.2 A CWT poderá, sem custo adicional a si própria e mediante antecedência razoável, realizar avaliações periódicas de segurança ou auditorias da Medida de segurança técnica e organizacional utilizada pelo Fornecedor durante a qual a CWT deve fornecer o Fornecedor questionários escritos e solicitações de documentação. A todos os pedidos, o Fornecedor também deverá apresentar resposta escrita e provas, se for o caso, imediatamente ou mediante acordo mútuo. Mediante solicitação da CWT de auditoria, o Fornecedor deverá agendar uma auditoria de segurança a ser iniciada 10 (dez) dias úteis após tal pedido. A CWT poderá requisitar o acesso às instalações, sistemas, processos ou procedimentos para avaliar o ambiente de controle de segurança do Fornecedor.

21.3 Mediante solicitação da CWT, certificar que o Fornecedor está em conformidade com este documento, bem como com as certificações das versões mais recentes do PCI-DSS, ISO 27001/27002, SOC 2 ou avaliação semelhante para o Fornecedor. Se o Fornecedor não puder certificar a conformidade, ele deve fornecer um relatório escrito detalhando onde não há conformidade e o seu plano de remediação se tornar conforme.

21.4 No caso em que a CWT, a seu exclusivo critério, considere que uma falha de segurança ocorreu, e que não foi relatada à CWT em conformidade com o documento e com o Processo de Gerenciamento de Incidentes do Fornecedor, agendar a auditoria ou avaliação para iniciar no prazo de vinte e quatro (24) horas após o aviso prévio da CWT pedindo avaliação ou auditoria.

21.5 No prazo de 30 (trinta) dias a contar do recebimento dos resultados de avaliação ou do relatório da auditoria, fornecer à CWT um relatório escrito sobre as ações corretivas que implementou ou se propõe a implementar, com o cronograma e status atual de cada ação corretiva. A cada 30 (trinta) dias corridos, atualizar este relatório à CWT, indicando o status de todas as ações corretivas até a data da implementação. Implementar todas as medidas corretivas no prazo de 90 (noventa) dias a contar da recepção do relatório de avaliação ou auditoria ou dentro de um período de tempo alternativo, desde que esse período de tempo alternativo tenha sido mutuamente ajustado, por escrito pelas partes, no prazo máximo de 30 (trinta) dias após recepção pelo Fornecedor do relatório de avaliação ou auditoria.

21.6 Estar em dia e continuar em dia com todas as normas impostas pelo governo e com a ISO 27001/27002. Se o Fornecedor lidar com números de conta de pagamento ou com outras informações relativas a pagamentos, manter a conformidade com a versão atualizada da Padrões de Segurança de Dados da Indústria de Cartões de Pagamento (PCI-DSS) para toda a gama de sistemas que manuseiam esse tipo de informação. Caso deixe de estar conforme com o PCI-DSS em parte ou no todo, o Fornecedor notificará imediatamente a CWT e fará o necessário para, imediatamente, remediar a situação, mantendo informada a CWT, sempre que esta o solicitar.

22. Padrões, melhores práticas, regulamentos e leis

O Fornecedor deverá:

Caso o Fornecedor processe, acesse, veja, armazene ou administre as Informações Pessoais e Dados Pessoais pertencentes à equipe, parceiros, afiliados da CWT; aos clientes da CWT; ou aos funcionários dos clientes, empreiteiros, ou subcontratados da CWT; empregar Medidas de Segurança Organizacionais e Técnicas tão rigorosas quanto as exigidas por diretrizes, regulamentos, normas e leis globais, regionais, nacionais, estaduais e locais.

23. Modificação

CWT reserva-se o direito de atualizar e de modificar estes Requisitos de Segurança da Informação de tempos em tempos, colocando a versão mais recente no site da CWT.

Versão 2.0

Data: 15 de Dezembro de 2017