Índice

1. Introdução e Escopo

1.1 Este documento representa a base de requisitos de segurança relevantes para o escopo de trabalho a ser realizado por um Fornecedor. Estes requisitos estão em 3 níveis.

O primeiro nível exigências na seção 2 está relacionado aos Fornecedores que realizarão um trabalho contendo informações limitadas da BT e que podem ter acesso limitado aos Sistemas administrativos e às Redes da BT. Fornecedores que se enquadrem nesta categoria não serão obrigados a cumprir com nenhuma outra obrigação deste documento.

O segundo nível, seções 3-6, são obrigatórios para todos os tipos de trabalho.

Para o terceiro nível, dependendo do escopo do trabalho, uma ou mais obrigações nas seções 7-18 podem se aplicar, seu representante de Contrato BT poderá auxiliá-lo.

Algumas das obrigações podem fazer referência a um Anexo, conforme listado abaixo, que pode fornecer maiores informações:

Anexo 1 - Classificação das informações
Anexo 2 - Treinamento obrigatório
Anexo 3 - Passando perguntas/problemas a um contato de segurança da BT
Anexo 4 - Acesso a unidades e prédios da BT realizado por empresas que não a BT - Apenas no Reino Unido
Anexo 5 - Requisitos de segurança de hospedagem externa

1.2 Estes requisitos de segurança são adicionais, e sem prejuízo a qualquer outra obrigação do Fornecedor no Contrato (inclusive, mas não limitado a, suas obrigações sob as Condições entituladas “Confidencialidade”, “Proteção de dados pessoais” e “Verificações de pré-contratação (PECs).

2. Segurança da informação para acesso limitado

A conformidade com a Seção 2 é a única obrigação aplicável caso o Fornecedor esteja realizando um trabalho que tenha acesso limitado a informações da BT e que possa ter acesso limitado a Sistemas administrativos da BT, ex. iSupplier e redes BT (os tipos de trabalho incluem, mas não estão limitados a, estacionário, gestão de instalações prediais, pesquisas no local, esquemas de vales e produtos com descontos para funcionários, provedores de conteúdo da TV BT e titulares de direitos.)

Sem prejuízo de qualquer obrigação de confidencialidade que possa vir a ter, quando o Fornecedor ou funcionário contratado tiver acesso a informações da BT ou de clientes da BT (inclusive dados pessoais) relacionadas à BT ou a clientes da BT, o Fornecedor deve:
(a) garantir que estas informações (inclusive dados pessoais) não sejam divulgadas ou acessadas por pessoas contratadas não diretamente empregadas pela BT; e
(b) manter (e garantir que todos os funcionários contratados mantenham) estas informações (inclusive dados pessoais) seguras e confidenciais (inclusive, sem limitações, afetando estes sistemas e procedimentos conforme necessário com a finalidade de proteger a segurança de todas as informações pertencentes à BT ou controladas por ela na medida em que estiver de posse ou sob o controle do Fornecedor, de acordo com as melhores práticas da indústria e implementar todos estes sistemas e processos de forma rigorosa).

As seções 3-6, inclusive, se aplicam a todos os engajamentos de fornecedores com a BT (exceto fornecedores que estejam apenas fornecendo Suprimentos de acesso limitado)

3. Segurança de informações gerais

3.1 O fornecedor deve informar imediatamente à BT os dados de contato de segurança do fornecedor e quaisquer alterações ligados a eles.

3.2 No início do Contrato o Fornecedor deve informar ao contato de segurança da BT, por escrito, utilizando o Anexo 3, a localização geográfica em que os principais serviços são prestados, onde seus funcionários contratados estão localizados ou onde as informações da BT são processadas ou armazenadas. Durante o contrato, o Fornecedor também deve informar qualquer alteração de localização geográfica proposta ao contato de segurança da BT através do Anexo 3 para que a BT possa reavaliar quaisquer riscos que possam ser gerados à BT ou às i8nformações do cliente da BT.

3.3 O fornecedor deve garantir que todos os contratos com subcontratadas relevantes incluam termos por escrito que obriguem a subcontratada a cumprir com os requisitos de segurança do fornecedor da BT à medida em que forem aplicáveis. Estes termos devem estar em vigor entre o Fornecedor e sua subcontratada antes que a subcontratada ou um de seus funcionários tenha acesso aos sistemas ou a informações da BT.

3.4 O Fornecedor não deve usar informações da BT para nenhuma finalidade que não aquela para a qual as informações da BT foram fornecidas a ele pela BT e, então, apenas na medida necessária para permitir que o Fornecedor execute o Contrato. O Fornecedor deve lidar ou usar as informações da BT de forma consistente com as obrigações constantes no Anexo 1 deste Requisito de Segurança e de acordo com a legislação aplicável.

3.5 O fornecedor deve informar o contato de segurança da BT através do Anexo 3 caso passe por uma fusão, aquisição ou mudança na propriedade para que possamos reavaliar qualquer risco à BT ou às informações do cliente da BT.

3.6 O Fornecedor deve pelo menos anualmente, ou quando for fornecida alguma alteração ao Suprimento ou conforme estas forem fornecidas, revisar estes Requisitos de Segurança para garantir que estejam em conformidade com todos os Requisitos de Segurança aplicáveis.

3.7 O Fornecedor deve gerenciar de forma segura qualquer Ativo Físico da BT e/ou itens da BT atribuídos a ele pela BT.

- Os ativos físicos e itens da BT devem ser armazenados com segurança quando não estiverem sendo usados. Exemplos disso incluem, mas não se limitam a, o acesso remoto realizado por tokens, laptops da BT, equipamentos de rede, servidores e documentações.
- Ativos físicos da BT não devem ser retirados do local de trabalho sem prévia autorização.

3.8 O Fornecedor deve, em relação aos Suprimentos, ter procedimentos formais de gestão de incidentes de segurança com responsabilidades definidas e todas as informações relacionadas a incidentes de segurança devem ser tratadas como "Confidenciais". O Fornecedor deve informar o contato de segurança da BT através do Anexo 3, dentro de um prazo razoável, após tomar conhecimento de qualquer acidente:

i) que envolva a perda material , adulteração, dano ou mal uso de informações da BT, de ativos físicos da BT, itens da BT ou o acesso impróprio ou não autorizado aos sistemas e informações da BT ou a violação de qualquer obrigação do Fornecedor sob estes Requisitos de Segurança; ou

ii) que envolva qualquer inabilidade de fornecer os Suprimentos de acordo com o contrato;

Iii) qualquer ação que viole os requisitos deste documento de Segurança.

Mediante solicitação, o Fornecedor deve fornecer imediatamente à BT um relatório por escrito com um plano de correção que inclua um cronograma e os passos a serem tomados para evitar que o incidente volte a se repetir.

3.9 O Fornecedor deve se certificar de que os riscos à confidencialidade, integridade ou disponibilidade das informações da BT identificados nos processos ou sistemas do Fornecedor sejam imediatamente tratados

3.10 A BT deve realizar avaliações de risco em qualquer parte relevante do serviço (a qual pode incluir subcontratadas relevantes ao serviço) para identificar riscos adicionais à BT como resultado dos Suprimentos, conforme aplicável. A BT pode então estipular contramedidas adicionais para abordar riscos que possam vir a ocorrer. Quaisquer custos associados à implementação de contramedidas devem ser acordados por ambas as partes.

3.11 O Fornecedor deve ter políticas de segurança e processos e deve manter documentos (as cópias devem ser disponibilizadas em inglês) que comprovem a conformidade com estes Requisitos de Segurança e deve fornecer à BT acesso às provas desta, de acordo com a Seção 7 abaixo.

3.12 O Fornecedor deve se certificar de que os procedimentos e controles estão em vigor para proteger a transferência de informações da BT através da utilização de e-mails, comunicações por meio de voz, fax e vídeo (Ex. quando estiver em vídeo conferências, certifique-se de que todos os participantes estão autorizados a discutir informações da BT). Para maiores informações relacionadas a informações da BT, veja o Anexo 1.

3.13 O Fornecedor deve ter procedimentos implementados que lidem com ameaças à segurança dirigidas ou orientadas à BT ou contra terceiros que estejam trabalhando em nome da BT para que possam proteger as informações da BT de forma adequada.

3.14 O Fornecedor deve se certificar de que as atividades de trabalho remotas ou realizadas na casa dos colaboradores relacionadas às informações e aos sistemas da BT estejam sujeitas aos controles de segurança apropriados dentro das empresa do

Fornecedor, inclusive, mas não limitado a, o acesso remoto realizado por usuários, sujeito a uma autenticação eficaz.

3.15 Em caso de encerramento ou fim do Contrato, o Fornecedor deve, e deve providenciar que qualquer funcionário contratado e subcontratadas, destruir de forma segura, de acordo com o Anexo 1 destes Requisitos de Segurança, toda e qualquer informação da BT detida ou controlada pelo Fornecedor ou por suas subcontratadas, a não ser que especificado pela BT ou exigido por alguma lei ou obrigação legal. As informações arquivadas devem ser colocadas fora de uso durante atividades diárias da empresa.

3.16 O Fornecedor deve manter as informações da BT durante todo o tempo necessário para a realização do serviço, mas não mais do que dois anos, a não ser que um período de retenção diferente deste tenha sido especificado pela BT ou seja necessário para atender aos requisitos legais ou regulatórios.

3.17 O Fornecedor deve garantir a disponibilidade, qualidade, integridade e adequada capacidade para o fornecimento do desempenho do sistema necessário ou dos serviços com disponibilidade sem qualquer interrupção certificando-se de que:-

- Exista um plano B
- Os dados de sistema essenciais estejam protegidos, se aplicável
- Um plano de contingência seja implementado quando for um requisito acordado
- O sistema ou serviço possa ser recuperado após uma grande falha ou desastre
- O plano seja praticado ao menos uma vez por ano
- Cópias de backup das informações e do software sejam feitas, quando aplicável, e testadas regularmente de acordo com uma política de backup acordada para garantir a restauração dos dados sem que haja qualquer alteração.

4. Segurança dos funcionários contratados

4.1 Os funcionários contratados relevantes não devem ter acesso até que tenham finalizado o treinamento de segurança da BT, conforme detalhado no Anexo 2 destes Requisitos de Segurança. O treinamento de Segurança da Informação da BT pode ser substituído por um treinamento de segurança da informação equivalente do próprio fornecedor, desde que aprovado pela segurança da BT. Depois disso, o treinamento obrigatório deve ser atualizado, conforme detalhado no Anexo 2. O fornecedor deve manter os registros do treinamento, os quais deve ser disponibilizados para auditoria realizada pela BT.

4.2 O Fornecedor deve se certificar de que todos os funcionários contratados tenham assinado acordos de confidencialidade do Fornecedor antes de iniciar seus trabalhos nas instalações ou nos sistemas da BT ou que tenham acesso a informações da BT. Estes acordos de confidencialidade devem ser retidos pelo Fornecedor e devem ser disponibilizados para revisão durante a auditoria realizada pela BT.

4.3 O Fornecedor deve lidar com as violações das políticas e procedimentos de segurança através de processos formais que incluam ações disciplinares, conforme apropriado.

4.4 O Fornecedor deve manter uma linha direta confidencial, disponível a todos os seus funcionários, até o limite permitido pela lei, para que seja usado pelos funcionários contratados caso sejam instruídos a agir de forma inconsistente e em violação a estes requisitos de segurança. Os relatórios relevantes devem ser informados ao contato de segurança da BT através do Anexo 3.

4.5 Quando funcionários contratados não forem mais atribuídos aos serviços, o Fornecedor deve se certificar de que o acesso às informações da BT seja revogado e que qualquer ativo, item ou informação da BT de posse do funcionário contratado seja devolvido à equipe operacional competente da BT ou seja destruído de acordo com o Anexo 1 destes Requisitos de Segurança. Quando aplicável, o Fornecedor deve implementar um procedimento de saída controlada que inclua uma solicitação por escrito à BT operacional que peça a remoção dos acessos a BT e à identidade. Os funcionários contratados devem ser avisados de que o contrato de confidencialidade ainda está em vigor e que as informações da BT adquiridas durante o trabalho realizado não devem ser divulgadas.

4.6 Como parte da concessão do acesso, o Fornecedor deve manter e fornecer registros de todos os funcionários contratados que precisarem de acesso ou que estiverem fornecendo serviços à BT, inclusive nome, local de trabalho, endereço comercial de e-mail, número de telefone comercial direto e ramal (se aplicável) e/ou telefone celular, data de solicitação do número de identificação do usuário (UIN) (Caso tenham), data de atribuição do projeto BT, data de conclusão do treinamento obrigatório, data de abandono do projeto BT e declaração de verificação pré-contratação. O contato de segurança do Fornecedor deve se certificar sempre de que todos os funcionários contratados relevantes estejam autorizados.

5. Análise de auditoria e segurança

5.1 O Fornecedor deve, com relação aos serviços prestados e desde que mantendo a confidencialidade das informações relacionadas aos seus outros clientes, permitir mediante uma solicitação sensata (e se certificar de que todos os funcionários contratados permitam) o acesso à BT ou aos seus representantes autorizados às instalações, sistemas e registros do Fornecedor ou de qualquer uma de suas subcontratadas relevantes que contenham informações da BT ou do cliente da BT (inclusive dados pessoais), uma vez que este acesso é necessário para avaliar a conformidade do Fornecedor com os Requisitos de Segurança.

Isso pode incluir avaliações de todos os elementos de controles físicos e lógicos e a validação de sistemas do Fornecedor que contenham informações da BT. O Fornecedor deve facilitar a avaliação, permitindo que a BT colete, retenha e analise informações relacionadas à prestação dos serviços, conforme aplicável, para que identifique riscos de segurança em potencial, forneça estes relatórios à BT e participe destas reuniões, conforme razoavelmente solicitado pela BT.

Caso seja solicitado pela BT, o Fornecedor deverá participar de uma avaliação de saúde online remota para estabelecer a conformidade de segurança básica com as cláusulas de segurança destes Requisitos de Segurança.

6. Investigação

6.1 Se a BT tiver qualquer razão para suspeitar que houve violação por parte do Fornecedor ou de alguma Subcontratada do fornecimento destes Requisitos de Segurança que tenham impacto sobre os sistemas e/ou informações da BT, a BT deve informar o contato de segurança do Fornecedor. O Fornecedor deve cooperar totalmente com a BT em qualquer investigação subsequente realizada pela BT e/ou qualquer agência de aplicação da lei, que possa incluir o acesso a informações da BT nas instalações do Fornecedor, desde que o Fornecedor seja notificado com antecedência.

Durante a investigação, o Fornecedor deve cooperar com a BT fornecendo a assistência e as instalações necessárias para a investigação da violação. A BT pode solicitar que o Fornecedor coloque em quarentena para avaliação algum ativo tangível ou intangível pertencente ao Fornecedor para auxiliar na investigação e o Fornecedor não deve recusar ou atrasar o pedido injustificadamente.

Nas cláusulas 7-18, a descrição de cada seção especifica a qual tipo de serviço cada uma se aplica.

7. Requisitos e política de segurança genéricos

É preciso que o Fornecedor esteja em conformidade com as cláusulas da Seção 7 caso este tenha acesso a "Informações Confidenciais" ou esteja fornecendo desenvolvimento, suporte de funções de rede ou serviços profissionais de TI.

7.1 O Fornecedor deve ter certificação ISO27001 ou deve estar em conformidade com os Requisitos de Segurança da certificação ISO 27001 ou com as políticas de segurança alinhadas à ISO 27001 e/ou esteja trabalhando para adquirir a certificação ISO 27001 dentro de um prazo acordado junto à BT.

7.2 Se necessário, a BT pode atualizar de tempos em tempos as políticas relacionadas a segurança, diretrizes, os requisitos de segurança e outros requisitos. A BT deve incorporar atualizações relevantes dentro de uma versão atualizada destes Requisitos de Segurança através de uma solicitação de alteração de contrato, a qual deve ser informada por escrito pela BT ao Fornecedor. Quaisquer custos associados à implementação de requisitos de segurança devem ser acordados por ambas as partes.

7.3 O Fornecedor deve disponibilizar à BT cópias das certificações de segurança e da declaração de aplicabilidade relevante aos serviços fornecidos para dar suporte às evidências de conformidade com este cronograma.

8. Segurança Física - Instalações da BT

Caso o Fornecedor esteja prestando serviços nas instalações da BT, é necessário que esteja em conformidade com as cláusulas da Seção 8.

8.1 Todos os funcionários contratados que estiverem trabalhando nas instalações da BT devem ter em mãos um cartão de identificação fornecido pela BT ou pelo Fornecedor autorizado. Este cartão deve ser usado como um meio de verificação da identidade do funcionário dentro das instalações da BT a qualquer momento e deve incluir uma imagem fotográfica exibida no cartão clara e ser um verdadeiro retrato do funcionário contratado. O funcionário contratado também deve receber um controle de acesso eletrônico e/ou um carão de visitante com duração limitada que deve ser usado de acordo com as instruções de emissão locais.

8.2 Apenas os build servers aprovados pela BT, Pcs Webtop da BT e dispositivos de confiança da BT podem ser conectados diretamente (ligados a uma porta Lan ou à conexão sem fio) aos domínios da BT. O Fornecedor não deve (e, se for o caso, deve se certificar de que nenhum funcionário contratado deva), sem autorização prévia do contato de segurança da BT por escrito (através do Anexo 3), conectar qualquer equipamento não aprovado pela BT a qualquer domínio da BT. O contato de segurança da BT deve fornecer a autorização por escrito ao iniciar o processo de concessão da política de segurança dentro da BT.

8.3 Nenhuma informação da BT deve ser removida das instalações da BT e nenhum equipamento ou software deve ser removido ou instalado nas instalações da BT sem a autorização prévia da BT.

8.4 Deve-se respeitar a proteção física e diretrizes para trabalhar nas instalações da BT, ex. ser acompanhado ao ir para áreas seguras. Além disso, ordens ou instruções dadas pela BT aos representantes do Fornecedor devem ser consideradas como tendo sido dadas ao Fornecedor.

8.5 Quando o Fornecedor for autorizado a fornecer acesso não acompanhado a áreas dentro do estado da BT aos seus funcionários contratados, o signatário autorizado que não é funcionário da BT e o funcionário contratado devem obedecer as instruções de orientação dadas pela BT. Além disso, o signatário autorizado que não é funcionário da BT e o funcionário contratado devem ter melo menos as verificações pré-contratação de nível 2.

9. Segurança Física - Instalações do Fornecedor

Caso o Fornecedor esteja prestando serviços em instalações fora BT, é necessário que esteja em conformidade com as cláusulas da Seção 9, incluindo todos os funcionários contratados, subcontratadas, funcionários do Fornecedor, subcontratados e agentes.

9.1 O acesso a instalações que não sejam da BT (instalações, prédios ou áreas internas) em que sejam prestados serviços, ou onde informações da BT sejam armazenadas, deve ser realizado através de um cartão de identificação fornecido por um Fornecedor autorizado. Este cartão deve ser usado como um meio de verificação nas instalações aplicáveis a qualquer momento e a imagem fotográfica exibida no cartão clara e ser um verdadeiro retrato do funcionário contratado. Os indivíduos também devem receber um cartão de acesso eletrônico autorizado com a única finalidade de acesso às instalações

aplicáveis ou acesso de segurança por teclado com processos de controle de autorização, disseminação e alteração regular de código/código ad-hoc.

9.2 O Fornecedor deve se certificar de que o acesso às instalações, prédios ou áreas internas em que os serviços são executados, ou que as informações da BT são armazenadas ou processadas, deve ser autorizado e deve estar de acordo com os processos e procedimentos de segurança, inclusive subcontratadas com acesso físico a estas áreas (ex. manutenção de controle ambiental, empresas de alarme).

9.3 Caso seja solicitado pela empresa BT ou pelo proprietário do projeto BT, o Fornecedor deve garantir de que os funcionários contratados relevantes estejam segregados de forma segura de todos os outros funcionários do Fornecedor.

9.4 Áreas seguras nas instalações do Fornecedor (ex. salas de comunicação de rede) devem ser segregadas e protegidas por controles de entrada apropriados, garantindo que apenas funcionários contratados autorizados tenham permissão de acesso a estas áreas seguras. O acesso de funcionários contratados a estas áreas deve ser auditado regularmente e deve ser feita uma nova autorização dos direitos de acesso pelos menos uma vez ao ano.

9.5 Os sistemas de circuito fechado de televisão e seus meios de gravação devem ser usados pelo Fornecedor tanto em resposta a incidentes de segurança como como uma ferramenta de vigilância de segurança, um impedimento ou como uma ferramenta para a possível apreensão de indivíduos pegos em flagrante cometendo um crime. Quando as imagens do sistema de circuito fechado são gravadas (seja em fita de vídeo ou digitalmente), estas imagens devem ficar retidas por pelo menos 20 dias. No entanto, este período pode ser prorrogado nas seguintes situações:-
i) Quando a evidência do sistema de circuito fechado de TV precisar ficar retida devido a um incidente ou uma investigação criminal.
ii) Quando especificado como um requisito necessário para ficar em conformidade com a legislação.

Todas as fitas de vídeo do sistema de circuito fechado de TV utilizadas para a gravação de imagens da câmera devem ser armazenadas em um armário trancado e a chave deve ser mantida e controlada de forma segura. O acesso ao armário deve ser restrito apenas a pessoas autorizadas.
Todos os gravadores do sistema de circuito fechado de TV devem ficar em um local discreto, evitando o acesso não autorizado e a possibilidade da visualização “ocasional” de qualquer tela do sistema de circuito fechado de TV associada.

9.6 A área que circunda as instalações do Fornecedor usada para os produtos e/ou serviços, conforme aplicável, deve ser inspecionada regularmente pelo Fornecedor para verificação de possíveis riscos ou ameaças.

9.7 O cabeamento de energia e telecomunicação que transporta dados ou que dá apoio a serviços de informações ou serviços de rádio/satélite utilizado no fornecimento de Suprimentos deve ser ter seu nível de proteção verificado pelo Fornecedor a fim de evitar a interrupção das operações da empresa. As medidas de proteção de segurança física proporcionais à importância do negócio das operações a que servem devem ser implementadas como segue:
i) Vias críticas do negócio, blindagem do cabo, bueiros, tampas de bueiros contendo cabos essenciais da empresa devem ser protegidos.

ii) Acesso a câmeras de cabos ou armário com tubo vertical para cabos dentro dos prédios operacionais devem ser restritos ao uso dos leitores de controle de acesso eletrônico ou à gestão eficaz de chaves.
iii) Links de comunicação com computadores e equipamentos de comunicação dentro das instalações de computadores devem ser física e ambientalmente protegidos.
iv) Links de comunicações via rádio ou satélite e equipamentos de comunicação devem ser protegidos de forma adequada.

9.8 Serviços de segurança realizados por pessoas são considerados necessários para complementação das medidas de segurança física e eletrônica nas instalações fo Fornecedor, sob as seguintes circunstâncias:

- A localização é de importância operacional
- As informações processadas da BT podem impactar a marca e sua reputação
- Alto volume de informações processadas da BT (ex. Terceirização de processo de negócios)
- Requisitos contratuais do cliente
- Risco/Ameaça específica das instalações
- O fornecedor possui informações da BT com alto nível de confidencialidade.

9.9 Para proteger os equipamentos da BT (como servidores e interruptores da BT) nas instalações do Fornecedor contra ameaças ou perigos ambientais e contra a possibilidade de acesso não autorizado, os equipamentos da BT devem ficar localizados em uma área protegida e segregada de equipamentos usados para qualquer sistema de empresas que não a BT. O nível de segregação deve garantir que o equipamento e segurança da BT não possa ser comprometido seja deliberadamente como acidentalmente como resultado do acesso concedido a empresas que não a BT e que possam por exemplo tomar forma de emparedamento de partição segura, armários trancados ou gaiola de metal.

9.10 A prevenção e detecção de medidas serão implementadas para evitar a falha na instalação causada pela interrupção de serviços essenciais ou outras influencias ambientais.

- Fogo;
- Gás;
- Inundação;
- Falha no fornecimento de energia.

Alarmes devem ser instalados e conectados a uma posição permanentemente tripulada para que seja possível detectar o que segue:

- Fogo;
- Gás;
- Falha no fornecimento de energia;
- Falha no fornecimento de energia ininterrupta (UPS);
- Falha no ar condicionado/controle de temperatura de umidade.

9.11 Perímetros de segurança (barreiras como paredes, cercas. portões de entrada controlada por cartão ou mesas de recepção tripulada) devem ser usados para proteger as áreas que contém informações da BT e instalações de processamento de informações.

9.12 Pontos de acesso como áreas de entrega e de carregamento e outros pontos onde pessoas não autorizadas podem entrar nas instalações devem ser controlados e, se possível, isolados das instalações de processamento de informações com a finalidade de evitar o acesso não autorizado ou ataques deliberados.

9.13 Certifique-se de que o acesso físico a áreas que tenham acesso às informações da BT seja feito apenas com a utilização de cartões inteligentes ou de proximidade (ou sistemas de segurança equivalentes) e que o Fornecedor conduza auditorias internas regulares para garantir a conformidade com estas disposições.

9,4 O Fornecedor deve se certificar de que seja proibido fotografar e/ou capturar a imagem de qualquer informação da BT ou de informações do cliente da BT. Sob circunstâncias excepcionais em que possa haver casos que exijam que estas imagens sejam capturadas, uma exceção temporária a esta cláusula deve ser obtida por escrito pelo contato de segurança da BT, utilizando o Anexo 3.

9.15 O Fornecedor deve manter uma política de mesa e tela limpa para proteger as informações da BT.

10. Fornecimento de ambiente de hospedagem

Se o Fornecedor estiver fornecendo um ambiente de hospedagem para a BT ou para os equipamentos do cliente BT, é necessária estar em conformidade com as cláusulas da Seção 10.

10.1 O Fornecedor deve, quando o Fornecedor estiver fornecendo uma área de acesso seguro em suas instalações para a hospedagem de equipamentos da BT ou do cliente BT ("Instalação do Fornecedor"):

(a) garantir que todos os funcionários contratados que tenham acesso às instalações do Fornecedor possuam um cartão de identificação ou um cartão de controle de acesso eletrônico. Este cartão deve ser usado como um meio de verificação nas instalações do Fornecedor a qualquer momento e a imagem fotográfica exibida no cartão clara e ser um verdadeiro retrato do funcionário contratado; e

(b) deve ter procedimentos implementados que lidem com ameaças à segurança dirigidas à BT ou aos equipamentos do cliente da BT ou contra terceiros que estejam trabalhando em nome da BT para que possam proteger as informações da BT ou do cliente da BT nas instalações do Fornecedor; e

(c) usar sistemas de circuito fechado de televisão e seus meios de gravação nas instalações do Fornecedor em resposta a incidentes de segurança como como uma ferramenta de vigilância de segurança, um impedimento ou como uma ferramenta para a possível apreensão de indivíduos pegos em flagrante cometendo um crime. O Fornecedor deve garantir que 20 dias de sistema de circuito fechado de TV sejam gravados para que as gravações sejam eficazes como uma ferramenta investigativa; e

(d) fornecer à BT uma planta do espaço alocado na área segura das instalações do Fornecedor; e

(e) garantir que os armários da BT e do cliente da BT localizados nas instalações do Fornecedor sejam mantidos trancados e só sejam acessados por pessoas autorizadas pela BT; representantes aprovados pela BT e funcionários contratados relevantes; e

(f) implementar um processo de gerenciamento de chave de segurança nas instalações do Fornecedor; e

(g) inspecionar regularmente a área local que circunda as instalações do Fornecedor para verificação de possíveis riscos ou ameaças; e

(h) documentar e manter procedimentos operacionais (no idioma do país que origina o trabalho da BT) para desempenhar os requisitos de segurança detalhados neste parágrafo 12 e, mediante solicitação, fornecer à BT acesso a estes documentos.

10.2 A BT deve fornecer ao Fornecedor:
(a) um registro dos ativos físicos da BT e do cliente da BT mantidos nas instalações do Fornecedor; e
(b) dados dos funcionários da BT, subcontratadas e agentes que precisem ter acesso às instalações do Fornecedor (em uma base contínua).

11. -Desenvolvimento do fornecimento de Suprimentos

Caso o Fornecedor esteja lindando com o desenvolvimento de Suprimentos para utilização da BT e/ou de clientes da BT, é necessário que esteja em conformidade com as cláusulas contidas na Seção 11. (Isto inclui "componentes fora da prateleira", configurações de software e fabricação de componentes para as prestações de serviços)

11.1 O Fornecedor deve implementar medidas de segurança acordadas em todos os componentes fornecidos. tais como salvaguardar a confidencialidade, a disponibilidade e a integridade dos suprimentos ao:

(i) manter a documentação apropriada (no idioma do país que origina o trabalho da BT) relacionado à implementação da segurança e deve garantir que esta documentação e sua segurança estão de acordo com as melhores práticas da indústria
(ii) minimizar a oportunidade de indivíduos não autorizados (ex. hackers) tenham acesso aos sistemas e informações da BT, às redes ou serviços da BT, e
(iii) minimizar o risco de mal uso dos sistemas e informações da BT, das redes ou serviços da BT que podem eventualmente causar perdas de receita ou de serviços.

11.2 O Fornecedor deve demonstrar, mediante solicitação, que qualquer software ou hardware criado (tanto proprietário como fora da prateleira) entregue à BT seja igual ao acordado com a BT. O Fornecedor deve manter a integridade das criações, inclusive atualizações, sistemas operacionais e aplicativos da fábrica para a mesa.

11.3 garantir que o desenvolvimento de sistemas para utilização da BT ou para a criação e manutenção de hardware de propriedade da BT seja reforçado pelos requisitos de segurança de TI da BT, caso fornecido pela equipe operacional da BT ou pelas melhores práticas da indústria.

11.4 garantir que o desenvolvimento e os ambientes de teste não contenham dados em tempo real e que sejam segregados do ambiente em tempo real. Os dados de teste fornecidos pela BT devem ser excluídos após um período determinado pelo proprietário de dados da BT.

11.5 O Fornecedor garante que todos os esforços razoáveis foram envidados para garantir que o software e/ou o hardware (e os documentos fornecidos em formato eletrônico) estejam livres de, inclusive, mas não limitado a todas as formas de

(i) "posse eletrônica" e "bombas lógicas";
(ii) "vírus" e "worms" que poderiam ter sido detectados com a utilização do mais atual (na data
de expedição) software de detecção de vírus disponível comercialmente; e
(ii) "spyware"; "adware" e outros malwares.

(expressões que devem ter significados conforme normalmente são entendidas dentro da indústria de informática); o Fornecedor garante mediante e após sua aceitação, que o Software e/ou o hardware terão desempenho de acordo com a Especificação funcional durante o Período de Garantia e que o Fornecedor deve empregar apenas materiais de boa qualidade, técnicas e requisitos de segurança durante a execução do Contrato e que, a todo momento, aplicará os Requisitos de Segurança de cuidado, habilidade e diligência das boas práticas de computação e os métodos de codificação seguros.

11.6 O Fornecedor deve trabalhar junto à BT para garantir a conformidade com os requisitos de segurança da(s) estrutura(s) de segurança apropriada(s) às custas do Fornecedor; de tempos em tempos os suprimentos podem precisar ter sua segurança testada de acordo com isso.

11.7 Toda falha de segurança nos Suprimentos identificada pela BT ou pelo Fornecedor deve ser remediada às custas do Fornecedor e dentro do prazo estipulado pela BT.

12. Acesso a informações

Aplicável se especificado nos Requisitos

12.1 Dentro de 14 duas a partir da solicitação por escrito feita pela BT e a critério da BT:
(a) as Partes devem, às suas custas, realizar e entregar à outra parte um contrato de acesso a informações em forma de Contrato de Informações de Acesso, conforme estabelecido no Anexo 3; ou
(b) o Fornecedor deve, às custas do Fornecedor, celebrar um acordo de depósito caução substancialmente na forma de um acordo estabelecido no Anexo 21 relacionado a todas as informações e documentos relacionados aos Suprimentos (inclusive, sem limitação, com relação ao Software, todos os códigos fonte, dados de ligação, listas de softwares, dados técnicos completos, anotações do programador, todas as informações e documentos relacionados ao Software necessários para manter, modificar e corrigir o Software e fornecer todos os níveis de suporte para o Software) ("as informações do depósito caução") e o depósito caução junto ao NCC Escrow International Limited (o "Agente de depósito caução") e uma cópia atualizada das informações do depósito caução. O Fornecedor deve garantir que estas informações de depósito caução possam permitir que a BT e/ou qualquer terceiro competente em nome da BT possam:

(i) preencher todas as notáveis obrigações do Fornecedor nos termos do Contrato, inclusive, sem limitação, as obrigações que teriam existido (inclusive a exigência do cumprimento de qualquer pedido que a BT tenha de outra forma colocado nos termos do Contrato) caso o Contrato não tivesse sido cancelado pela BT (exceto nos termos do parágrafo 4 da Condição entitulada "Cancelamento") antes do fim do prazo natural deste (o qual deve incluir qualquer prazo estendido sob qualquer opção pela BT de estender o prazo inicial); e
(ii) entender prontamente as informações de depósito caução, manter (inclusive a atualização), modificação; melhoria e correção das informações de depósito caução e de Suprimentos.

12.2 O Fornecedor garante que as informações de depósito caução depositadas tanto junto à BT como junto ao agente fiduciário, conforme for o caso, são e serão suficientes para permitir que um programador ou analista razoavelmente habilidoso mantenha ou melhore o Software sem a ajuda de nenhuma outra pessoa ou referência e o Fornecedor ainda se compromete a manter as informações de depósito caução totalmente atualizadas ao longo do período do Contrato.

12.3 Caso ocorra algum evento que permita que a BT ou o Agente Fiduciário, conforme for o caso, use e/ou divulgue as informações do depósito caução, o Fornecedor deve fornecer imediatamente, às suas custas, à BT dentro de um período razoável, tal parecer, suporte, assistência, dados, informações, acesso aos funcionários chave do Fornecedor ou

ao licenciador do Software com a finalidade de entender, manter (inclusive atualizar), melhorar, alterar e corrigir qualquer informação relacionada ao depósito caução e/ou ao Software.

12.4 Sem que afete nenhum outro direito que possa vir a ter, a BT deve automaticamente ter o direito não exclusivo, perpétuo, irrevogável e mundial, a título gratuito, de usar as informações de depósito caução, após sua divulgação com a finalidade de manter e dar suporte aos Suprimentos e, com o direito não exclusivo, perpétuo, irrevogável, mundial e livre de qualquer pagamento de usar, copiar, manter (inclusive atualizar), alterar, adaptar, melhorar e corrigir Suprimentos e qualquer Suprimento alterado, adaptado, melhorado e/ou corrigido, além de licenciar tais Suprimentos a terceiros (sujeito a limitações de licenças do Fornecedor), juntamente com o direito de autorizar terceiros a fazer qualquer uma das atividades supracitadas em nome da BT.

12.5 Esta condição sobreviverá ao término ou cancelamento do Contrato.

12.6 Caso seja necessário para fins de conformidade com assuntos de segurança, o contato de segurança de rede da BT (e/ou pessoas indicadas por ele, as quais devem ser funcionários da BT) deve ter direitos similares (mutatis mutandis) caso solicitado como parte dos fornecimentos, da familiarização e da validação (conforme definido no Contrato de Acesso a Informações) com relação ao material de origem (conforme definido no Contrato de Acesso a Informações).

13. Acesso aos sistemas da BT

Caso os funcionários contratados do Fornecedor precisem ter acesso aos sistemas da BT para o fornecimento de suprimentos, é preciso estar em conformidade com as cláusulas da Seção 13.

13.1 A BT pode permitir, a seu exclusivo critério, na medida em que for determinado por ela, o acesso apenas para o fornecimento de suprimentos, enquanto o fornecedor estiver autorizado a ter acesso.

13.2 Com relação ao acesso, o Fornecedor deve (e, quando relevante, deve garantir que todos os funcionários contratados devam):

a) garantir que a identificação do usuário, senhas, PINs, tokens e acesso a conferências sejam dados apenas a funcionários contratados individuais, e não compartilhados. Os dados devem ser armazenados de forma segura e separados do dispositivo que costumam acessar. Se outra pessoa tomar conhecimento da senha, esta deve ser alterada imediatamente.

b) Mediante um pedido razoável, fornecer relatórios à BT conforme esta solicitar relacionados a funcionários contratados autorizados a ter acesso aos sistemas da BT.

c) Não é permitido realizar ligações entre domínios aos sistemas da BT, a não ser que especificamente aprovadas e autorizadas pelo contato de segurança da BT, usando o Anexo 3.

d) Utilizar todos os meios razoáveis para garantir que nenhum vírus ou código malicioso (expressões normalmente compreendidas na indústria da informática) seja introduzido para minimizar o risco de corrupção nos sistemas da BT ou nas informações da mesma.

e) Utilizar os meios razoáveis para garantir que os arquivos pessoais que contenham informações, dados ou mídia sem relevância para os Suprimentos não sejam armazenados nos servidores da BT, nos laptops e desktops fornecidos pela BT, nas instalações de armazenamento centralizadas da BT ou nos sistemas da BT.

13.3 Caso a BT tenha concedido ao Fornecedor acesso à Internet/Intranet, o Fornecedor deve, e deve garantir que seus funcionários contratados devam, acessar a Internet/Intranet de forma apropriada para permitir que possa fornecer os Suprimentos, conforme aplicável. É responsabilidade do Fornecedor garantir que a seguinte orientação ao abuso da utilização da Internet e dos E-mail seja comunicada ao funcionário contratado relevante pelo menos uma vez ao ano.
Não deve acessar materiais que possam ser considerados: -

a. Ofensivos, sexuais, sexistas, racistas, politicamente ofensivos;
b. Um ato que possa trazer descrédito à BT ou a indivíduos;
c. Gerenciar uma empresa privada;
d. Uma infração dos diretos autorais;
e. Telefonia pela internet ou envio de mensagens, como o Skype;
f. Ignorar ou fazer o tunelamento do firewall da BT ou de outros mecanismos de segurança;
g. Não deve contribuir com sites ou fazer comentários online que possam ser razoavelmente atribuídos como sendo opinião da BT.
h. Sites inaceitáveis ou perigosos devem ser bloqueados para o usuário.

13.4 O Fornecedor deve informar imediatamente a BT caso qualquer funcionário contratado relevante não precise mais ter direitos de acesso aos sistemas da BT ou mude de função por qualquer motivo com relação ao que consta no Contrato permitindo, assim, que a BT desabilite ou altere os direitos de acesso aos sistemas da BT.

14. Acesso a informações da BT em sistemas do fornecedor

Caso as informações da BT sejam armazenadas ou processadas em sistemas do Fornecedor, é preciso estar em conformidade com as cláusulas da Seção 14.

14.1 Caso os funcionários contratados tenham recebido acesso aos sistemas do Fornecedor devido à entrega de Suprimentos de produtos e/ou serviços para a BT, o Fornecedor deve:

a) garantir que cada indivíduo tenha uma identificação de usuário e senha única (em conformidade com o padrão das melhores práticas da indústria) conhecidos apenas por este indivíduo para sua utilização como parte do processo de login seguro.
b) permitir o acesso aos sistemas de propriedade do Fornecedor que detenha ou acesse as informações da BT ou os sistemas da BT restringindo apenas à medida necessária para permitir que o funcionário contratado realize suas obrigações nos termos do Contrato.
c) manter os procedimentos formais para controlar a alocação, revisão e revocação e/ou cessação dos direitos de acesso.
d) garantir que a alocação e a utilização de privilégios melhorados e o acesso a ferramentas e instalações confidenciais nos sistemas do Fornecedor sejam controladas e limitadas apenas aos usuários que tenham uma necessidade comercial. Os consoles do sistema devem ser acessados e operados em um ambiente seguro

proporcional aos ativos que costumam gerenciar. A segurança física apropriada deve ser posta em prática para garantir que não haja acesso não autorizado.

e) garantir que a alocação das senhas de usuário dos sistemas de propriedade do Fornecedor que detêm ou que acesse as informações da BT sejam controladas através de um processo de gestão auditável formal.

f) conduzir revisões regulares dos direitos de acesso de usuários.

g) garantir que o acesso físico a equipamentos de informática que tenham acesso às informações da BT ou que armazenem as mesmas seja feito apenas com a utilização de cartões inteligentes ou de proximidade (ou sistemas de segurança equivalentes) e que o Fornecedor conduza auditorias internas regulares para garantir a conformidade com estas disposições.

h) demonstrar que os usuários seguem as melhores práticas de segurança na gestão de suas senhas.

i) implementar um sistema de gestão de senhas que fornece uma instalação interativa eficaz e segura que garanta a qualidade das senhas.

j) garantir que as sessões dos usuários sejam finalizadas após um período definido de inatividade.

k) garantir que os registros de auditoria sejam gerados para registrar a atividade do usuário e os eventos relevantes para a segurança e que estes sejam gerenciados de forma segura. Os registros devem ser retidos por um período razoável para facilitar qualquer investigação com nenhuma habilidade por parte do Fornecedor de permitir qualquer acesso não autorizado ou a alteração dos registros de auditoria.

l) garantir que o monitoramento dos registros de auditoria e de eventos e que os relatórios de análises de comportamentos anômalos e/ou a tentativa de acesso não autorizado seja realizado por funcionários do Fornecedor, independente destes usuários estarem sendo monitorados.

14.2 O Fornecedor deve manter sistemas que detectem e registrem qualquer tentativa de dano, alteração ou acesso não autorizado às informações da BT em sistemas em sistemas do fornecedor. Exemplos incluem, mas não se limitam a, o registro do sistema e processos de auditoria, IDS, IPS, etc.

14.3 manter controles para detectar e proteger contra softwares maliciosos e garantir que os procedimentos apropriados de conscientização do usuário sejam implementados.

14.4 garantir que ao menos uma vez ao mês qualquer software não autorizado seja identificado e removido dos sistemas do Fornecedor que detêm, processe ou acesse informações da BT.

14.5 garantir que o acesso a portas de diagnósticos e de gestão, assim como ferramentas de diagnóstico, sejam controladas de forma segura.

14.6 garantir que o acesso às ferramentas de auditoria do Fornecedor seja restrito a funcionários contratados relevantes e que seu uso seja monitorado.

14.7 garantir que a revisão de códigos e a realização de testes de penetração em todos os softwares produzidos no local e utilizados para processar informações da BT sejam realizados por uma equipe independente dos desenvolvedores.

14.8 Na medida que qualquer um dos servidores seja usado para fornecer os Suprimentos, eles não devem ser implementados em redes não confiáveis (redes fora de seu perímetro de segurança, que estejam além de seu controle administrativo, ex. voltado para a internet) sem os controles de segurança apropriados.

14.9 Alterações feitas no sistema individual do Fornecedor que detenha e processe informações da BT e/ou que seja usado para fornecer os Produtos e/ou .Serviços à BT devem ser controladas e estar sujeitas a procedimentos de controle de alteração formal.

14.10 Todos os sistemas devem ser seus relógios internos sincronizados com uma fonte confiável.

15. Fornecedor que hospede informações da BT

Quando o Fornecedor estiver hospedando informações da BT classificadas como Confidenciais ou com classificação mais alta em um ambiente de serviço em nuvem ou em ambientes de servidores de Fornecedores ou subcontratadas deve-se estar em conformidade com as cláusulas da Seção 15.

15.1 O Fornecedor deve, com relação aos Suprimentos, garantir que os ambientes em que as informações da BT são hospedados estejam em conformidade com os requisitos do Anexo 5.

16. Segurança da rede

Quando o Fornecedor estiver criando, desenvolvendo ou dando suporte a redes ou ativos da BT, é necessário estar em conformidade com as cláusulas da Seção 16.

16.1 Com relação aos Suprimentos, o Fornecedor deve implementar medidas de segurança acordadas em todos os componentes fornecidos. tais como salvaguardar a confidencialidade, a disponibilidade e a integridade das redes da BT e/ou dos ativos 21CN: O Fornecedor deve fornecer à BT toda a documentação relacionada à implementação de segurança da rede relacionada aos Suprimentos e deve garantir que ela e sua segurança:

(a) atendam a todos os requisitos regulatórios e legais; e
(b) utilize seus melhores esforços para evitar que indivíduos não autorizados (ex. hackers) obtenham acesso a elementos de gestão da rede e a outros elementos acessados através das redes da BT e/ou do 21CN; e
(c) utilize seus melhores esforços para reduzir o risco de mal uso das redes da BT e/ou do 21CN que podem eventualmente causar perdas de receita ou de serviços por parte de indivíduos que tenham autorização de acesso; e
(d) utilize seus melhores esforços para detectar qualquer violação de segurança que venha a ocorrer, permitindo a rápida retificação de qualquer problema resultante disso e a identificação dos indivíduos que obtiveram acesso e a determinação de como este acesso foi obtido; e
(e) minimizar o risco de má configuração das redes da BT, ex. pode ser realizado ao conceder o número mínimo de concessões necessárias para a realização da função contratada.

16.2 O Fornecedor deve tomar todas as medidas necessárias para proteger todas as interfaces nos componentes fornecidos e não deve supor que os componentes fornecidos sejam operados em um ambiente seguro.

16.3 O Fornecedor deve fornecer ao contato de segurança de rede da BT os nomes, endereços (e demais detalhes, conforme solicitação da BT) de todos os funcionários contratados individuais que periodicamente possam ter envolvimento na implementação, manutenção e/ou gestão de suprimentos antes que estejam respectivamente envolvidos em tal implementação, manutenção e/ou gestão.

16.4 Com relação às suas atividades de suporte baseadas no Reino Unido, o Fornecedor deve reter uma equipe de segurança qualificada composta por pelo menos um cidadão britânico, o qual deve estar disponível para cooperar com o contato de segurança de rede da BT (ou seus indicados) e participar destas reuniões conforme o contato de segurança de rede da BT solicitar de forma razoável de tempos em tempos.

16.5 O Fornecedor deve fornecer um cronograma ao contato de segurança de rede da BT (atualizado conforme necessário) de todos os componentes ativos inclusos no fornecimento e em suas respectivas fontes.

16.6 O Fornecedor deve fornecer dados de seus funcionários individuais que cooperarão com a equipe de gestão de vulnerabilidade da BT (CERT) em conversas ligadas à BT e às vulnerabilidades identificadas pelo Fornecedor com relação aos Suprimentos. O Fornecedor deve fornecer à BT informações oportunas sobre vulnerabilidades e deve estar em conformidade com os requisitos relacionados a estas vulnerabilidades e que possam ser informados pelo contato de segurança de rede da BT de tempos em tempos, às custas do Fornecedor. O Fornecedor deve informar à BT com antecedência qualquer vulnerabilidade apresentada, de forma a permitir a instalação de controles de mitigação antes de o Fornecedor divulgar estas vulnerabilidades publicamente.

16.7 O Fornecedor deve permitir que o contato de segurança de rede da BT e seus indicados tenham de tempos em tempos acesso total e irrestrito a todas as instalações nas quais os Suprimentos são desenvolvidos, manufaturados ou fabricados para que realizem testes e/ou avaliações de conformidade de segurança e o Fornecedor deve cooperar (e deve garantir que todos os funcionários contratados relevantes cooperem) com estes testes de conformidade.

16.8 O Fornecedor deve garantir que todos os componentes relacionados a segurança compreendidos nos Suprimentos, conforme identificados pela ou para a BT de tempos em tempos, sejam, às custas do Fornecedor, avaliados externamente para satisfação da BT.

16.9 Com relação a qualquer uma das informações fornecidas pela BT ou obtidas por ela e que esteja marcada como “ESTRITAMENTE CONFIDENCIAL” ou que sejam consideradas confidenciais, o Fornecedor deve garantir que:

(a) o acesso a ela é concedido apenas a funcionários contratados especificamente autorizados pela BT para que visualizem e lidem com elas e deve ser feito um registro destes acessos;

(b) elas sejam manuseadas, utilizadas e armazenadas com muito cuidado e sejam criptografadas antes de seu armazenamento com a utilização de PGP ou WinZip 9 e sob condições que ofereçam um alto grau de resistência ao comprometer de forma deliberada (ex. usando o algoritmo de criptografia disponível mais forte / usando uma senha forte) e que torne a tentativa ou o real comprometimento muito provável de ser detectado;
(c) quando transmitido, a segurança adequada é aplicada a ele, criptografando fazendo a criptografia com Secure Email, PGP ou WinZip 9; e
(d) não seja, sem a permissão por escrito da BT, exportado para fora do Espaço Econômico Europeu.

16.10 O Fornecedor deve, imediatamente, e, em todo caso, dentro de 7 dias úteis, fornecer ao contato de segurança de rede da BT todos os detalhes de quaisquer recursos e/ou funcionalidades de qualquer fornecimento (ou que esteja planejado no roteiro de qualquer fornecimento) que de tempos em tempos:

(a) o Fornecedor sabe; ou
(b) o contato de segurança de rede acredita e, por isso, informa o Fornecedor que possa ser projetado ou poderia ser usado para interceptação legal ou qualquer outra interceptação de tráfego de telecomunicações. Estes detalhes devem incluir todas as informações necessárias para permitir que o contato de segurança da rede da BT entenda completamente a natureza, a composição e a extensão destes recursos e/ou funcionalidades.

16.11 Para manter o acesso às redes e/ou sistemas da BT o Fornecedor deve informar imediatamente à BT quaisquer alterações relacionadas a seu método de acesso através de firewalls, inclusive o fornecimento da tradução do endereço da rede.

16.12 As ferramentas de monitoramento da rede que podem visualizar informações de aplicativos não podem ser usadas.

16.13 A funcionalidade Ipv6 inclusa nos sistemas operacionais devem estar desabilitadas nas hospedagens (dispositivos de usuário final, servidores) conectados a domínios de rede da BT quando não forem necessárias.

16.14 O Fornecedor deve estar em conformidade e deve garantir que os Suprimentos estejam em conformidade com as políticas, se fornecidas, e com os requisitos de segurança da BT; qualquer não conformidade deve ser acordada no momento de assinatura do contrato ou durante o controle de alterações.

16.15 O Fornecedor deve garantir que todos os funcionários contratados estejam com suas verificações pré-contratação apropriadas de acordo com o nível de acesso http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

Fornecedores que estejam criando, desenvolvendo ou dando suporte às redes da BT ou aos ativos de rede da mesma devem garantir que todos os funcionários contratados tenham realizado pelo menos as verificações pré-contratação de nível 2. As verificações de pré-contratação de nível 3 serão necessárias para funções identificadas pelo contato de segurança de rede da BT. Quando o Fornecedor não puder diretamente conseguir o certificado de segurança do funcionário contratado como parte das verificações de nível 3, a BT ajudará na obtenção da certificação, às custas do Fornecedor.

17. Segurança da rede do Fornecedor

Quando a rede do Fornecedor for ser utilizada para o fornecimento de Suprimentos (isto inclui LAN, WAN, Internet, redes sem fio e de rádio), é preciso estar em conformidade com as cláusulas da Seção 17.

17.1 Com relação aos Suprimentos, o Fornecedor deve implementar medidas de segurança acordadas em todas as suas redes, tais como salvaguardar a confidencialidade, a disponibilidade e a integridade das informações da BT: As medidas devem:-

(a) atender a todos os requisitos regulatórios e legais; e
(b) usar seus melhores esforços para evitar que indivíduos não autorizados (ex. hackers) obtenham acesso à rede; e
(c) usar seus melhores esforços para reduzir o risco de mal uso das redes que podem eventualmente causar perdas de receita ou de serviços por parte de indivíduos que tenham autorização de acesso; e
(d) usar seus melhores esforços para detectar qualquer violação de segurança que venha a ocorrer, permitindo a rápida retificação de qualquer problema resultante disso e a identificação dos indivíduos que obtiveram acesso e a determinação de como este acesso foi obtido; e

18. Segurança nas nuvens

Se o Fornecedor estiver fornecendo serviços relacionados a nuvens para a BT, é necessário estar em conformidade com as cláusulas da Seção 18. A definição de nuvem pode ser encontrada na Publicação NIST http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)

18.1 Os Fornecedores devem fornecer as evidências apropriadas de que os serviços em nuvens fornecidos estão de acordo com a última versão disponível dos requisitos da Matriz de Controles do CSA (CCM), disponível no site https://cloudsecurityalliance.org , além de estar em conformidade com o Anexo 5 destes requisitos de segurança.

18.2 As informações da BT envolvidas em comércio eletrônico e que passe por redes públicas devem estar protegidas de acordo com o Anexo 1, enquanto em trânsito e em repouso (inclusive backups) contra atividades fraudulentas, a divulgação não autorizada, acesso e alterações.

18.3 Os contratos de nível de serviço de rede e infraestrutura (internos ou terceirizados) devem documentar de forma clara os controles de segurança, a capacidade e os níveis de serviço e os requisitos de negócios e do cliente.

18.4 O Fornecedor deve permitir o teste de penetração e/ou o acesso a relatórios de testes de penetração do Fornecedor existentes relevantes para os Suprimentos que estão sendo fornecidos, o escopo e o tempo de duração dos testes, os quais devem ser mutuamente acordados com a BT.

18.5 O Fornecedor deve implementar medidas de segurança acordadas em todos os componentes fornecidos. tais como salvaguardar a confidencialidade, a disponibilidade, a

qualidade e a integridade dos suprimentos ao: minimizar a oportunidade de que indivíduos não autorizados (ex. outros clientes das nuvens) tenham acesso a informações e serviços da BT.

Glossário

Nestes requisitos de segurança, as seguintes definições se aplicam; caso contrário, os termos do contrato devem ser aplicados a estes requisitos de segurança e todas as palavras e expressões usadas nestes requisitos de segurança devem ter o mesmo significado dado a eles no Contrato:

["**Acesso**" – Procedimento, manuseio ou armazenamento de informações da BT realizado através de um ou mais dos métodos a seguir:-

- Pela interconexão com os sistemas da BT
- Fornecido em formato de papel ou não eletrônico
- Informações da BT em sistemas do fornecedor
- por meios móveis

e/ou acesso a prédios da BT para a prestação dos serviços (exceto para a entrega de hardwares e para a participação em reuniões)

[**Autorizado**" - A BT aprovou o acesso tanto como parte do processo de interconexão do sistema da BT ou uma autorização por escrito foi recebida pela empresa BT ou pelo proprietário do projeto BT; a "**autorização**" deve ser interpretada de acordo. O nível de acesso será relevante e limitado ao que for necessário para o fornecimento dos Suprimentos.]

"**Itens BT"** todos os itens fornecidos pela BT ao Fornecedor e todos os itens detidos pelo Fornecedor e que pertençam à BT (ex. chaves de armários, tokens de laptops, cartões de acesso, planos, documentos de processo).

"**Contato de segurança de rede da BT**" - Profissional de garantia da informação da segurança da BT contatado ao preencher e enviar o formulário de solicitação contido no Anexo 3, ou outra pessoa cuja identidade e dados de contato sejam informados ao contato comercial do Fornecedor de quando em quando.

"**Ativos físicos da BT**" - todos os ativos físicos detidos pelo Fornecedor e que pertençam à BT (ex. Roteadores, interruptores, servidores ou documentos)

"**Segurança da BT**" -a organização de segurança baseada dentro da BT.

"**Contato de segurança da BT**" - Profissional de garantia da informação da segurança da BT contatado ao preencher e enviar o formulário de solicitação contido no Anexo 3.

"**Política de Segurança da BT**" - significa a política de segurança de rede da BT, tal como fornecida pela BT.

"**Sistemas da BT**" - serviços e componentes de serviços, produtos, redes, servidores, processos, sistemas baseados em papel ou sistemas de TI (totais ou parciais) de propriedade e/ou operado pela BT ou em nome dela, pelo BT Group plc ou qualquer entidade do BT Group plc; ou quaisquer outros sistemas que possam ser hospedados nas instalações da BT (inclusive o iSupplier, uma uma vez que o "iSupplier" é definido na seção do Contrato entitulada "Pagamento e Faturamento") usados no contexto de "Acesso" (conforme definido acima).

"**Sistema de circuito interno de TV**" - significa o circuito interno de televisão

"**Data de início**" - conforme definido no contrato.

"**Funcionários contratados**", "**Funcionários contratados relevantes"** - conforme definido no contrato.

"**Informações**" – são informações tanto tangíveis como em outra forma, inclusive, sem limitação, especificações, relatórios, dados, anotações, documentos, desenhos, software,

políticas, procedimentos, processos, padrões, informações do computador, projetos, diagramas de circuito, modelos, padrões, exemplos, invenções (sejam elas capazes de ser patenteadas ou não) e conhecimento, e o meio (se houver um) através do qual esta informação é fornecida.

"**ISO 27001**" - um padrão de sistema de segurança internacional fornecido pela Organização Internacional para Padronização (ISO) e pela Comissão Eletrotécnica Internacional (IEC).

"Pedido(s)" - um pedido feito pela BT ao Fornecedor de Suprimentos feito de acordo com o Contrato.

"**Segurança da rede**" - significa a segurança dos caminhos de comunicação de interconexão e os nós que conectam de forma lógica as tecnologias dos usuários finais e os sistemas de gerenciamento associado.

"**Dados pessoais**" - devem ter os significados atribuídos a eles na Diretiva 95/46/EC ou em qualquer legislação subsequente relacionada a ela ("A Diretiva").

"Processo", "Processado" ou "Em Processamento" - significa qualquer operação ou grupo de operações desenvolvida acerca das informações da BT, seja através de meios automáticos ou não, como a coleta, registro, organização, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação através de transmissão, disseminação ou a disponibilização, alinhamento ou combinação, bloqueio, eliminação, devolução ou destruição.

"**Informações confidenciais**" - qualquer informação da BT classificada ou marcada como "Confidencial" ou acima, inclusive dados pessoais.

"**Subcontratada**" - conforme definido no contrato.

"**Sistemas do Fornecedor**" - qualquer computador de propriedade do Fornecedor, aplicação ou sistemas de rede usados para acessar, armazenar ou processar informações da BT ou envolvidos no fornecimento de Suprimentos.

"**Contato de segurança do Fornecedor**" - pessoa cujas informações de contato devem ser informadas pelo Fornecedor à BT de quando em quando e que será o ponto único de contato para problemas relacionados à Segurança.

"**Suprimentos**" - todos os componentes, materiais, plantas, ferramentas, equipamentos de teste, documentos, firmware, software, peças sobressalentes e peças e coisas que devam ser fornecidas à BT nos termos do Contrato juntamente a todas as informações e trabalhos que o Contrato exija que sejam fornecidos ou realizados para a BT.

"**Transferência**" ou "**Transferido**" - significa

(a) a movimentação de informações da BT de posse do funcionário contratado (inclusive, mas sem limitação, dados pessoais) de um local ou pessoa a outro, seja por meio físico, de voz ou eletrônico; e

(a) a concessão de acesso a informações da BT de posse do funcionário contratado (inclusive, mas sem limitação, dados pessoais) de um local ou pessoa a outro, seja por meio físico, de voz ou eletrônico.