Anexo [XX] — Requisitos de segurança para Fornecedores da BT

Índice

PARTE 1: INTRODUÇÃO

1 INTRODUÇÃO

1.1 Este documento estabelece os requisitos de segurança da BT.

1.2 A estes Requisitos de segurança são aplicáveis as definições na Parte 5 intitulada "**Definições**" — porém, caso contrário, serão aplicáveis a estes Requisitos de segurança os termos do Contrato, e todas as palavras e expressões utilizadas terão o significado que lhes é atribuído no Contrato.

1.3 Estes Requisitos de segurança são adicionais a e sem prejuízo de quaisquer outras obrigações do Fornecedor ao abrigo do Contrato (incluindo, sem se limitar, as suas obrigações no âmbito das Condições intituladas "**Confidencialidade**", "**Proteção de dados pessoais**" e "**Conformidade**").

PARTE 2: REQUISITOS DE ACESSO LIMITADO

2 REQUISITOS DE ACESSO LIMITADO

Esta secção será disponibilizada conforme aplicável sempre que o Fornecedor forneça Produtos que envolvam acesso limitado à BT ou a informações de Clientes da BT, ou nos casos em que o Fornecedor tenha acesso aos sistemas administrativos da BT com nível de utilizador. Os Fornecedores que se enquadrem nesta categoria não necessitam de cumprir quaisquer outras partes deste documento.

2.1 Sem prejuízo de quaisquer obrigações de confidencialidade, nos casos em que o Fornecedor ou o Pessoal contratado tenha acesso a Informações da BT, o Fornecedor deve:

2.2 garantir que as informações da BT não são divulgadas a ou acedidas por Pessoal contratado, exceto se necessário para o fornecimento dos Produtos;

2.3 implementar todos os sistemas e processos (técnicos e organizacionais) requeridos em conformidade com as Boas práticas de segurança da indústria para proteção das informações de segurança e confidenciais da BT e dos sistemas BT.

PARTE 3: REQUISITOS GERAIS DE SEGURANÇA

Obrigatórios onde a Parte 2: Requisitos de acesso limitado não for considerada aplicável.

3 SEGURANÇA GERAL DA INFORMAÇÃO

Segurança geral da informação

3.1 O Fornecedor deve implementar sistemas e processos (técnicos e organizacionais) para:

3.1.1 proteger a segurança e confidencialidade das informações da BT e dos sistemas BT, conforme estipulado por estes Requisitos de segurança; e

3.1.2 garantir a disponibilidade, qualidade, integridade e capacidade adequadas para entregar os Produtos sem interrupção, conforme exigido pelas Boas práticas de segurança da indústria.

3.2 O Fornecedor deve implementar um processo de gestão de alterações de TI documentado que garanta que quaisquer alterações aos processos e Sistemas do Fornecedor são implementadas de uma forma que mantenha a conformidade do Fornecedor face a estes Requisitos de segurança.

3.3 O Fornecedor deve disponibilizar à BT, mediante pedido escrito por parte da mesma, cópias de quaisquer certificados de segurança e declarações de conformidade relevantes para os Produtos, que comprovem a conformidade com estes Requisitos de segurança.

3.4 O Fornecedor tomará todas as medidas razoáveis para assegurar a designação do(s) indivíduo(s) apropriado(s) e que atuará(ão) como Ponto de contacto para Riscos de segurança, Gestão de incidentes e Gestão de conformidade. O Fornecedor deve notificar o Contacto de Segurança da BT sobre os dados de contacto do(s) indivíduo(s) e quaisquer alterações correspondentes. Os dados de contacto devem incluir:

nome, responsabilidade, função e endereço de e-mail e/ou número de telefone do grupo.

3.5 O Fornecedor reconhece e concorda que a BT pode efetuar alterações razoáveis periódicas aos Requisitos de segurança da BT nos casos em que:

3.5.1 o Fornecedor seja sujeito a uma fusão, aquisição ou alterações materiais de propriedade ou controlo;

3.5.2 haja uma alteração das normas de segurança de tecnologia ou sector; ou

3.5.3 existam quaisquer alterações materiais aos Produtos ou à forma como são fornecidos,

(individualmente, uma "**Alteração aos Requisitos de segurança**").

Após a receção da notificação escrita da BT sobre a necessidade de uma Alteração aos Requisitos de segurança, o Fornecedor deve atuar prontamente e em conformidade com a alteração aos Requisitos de segurança e, em qualquer caso, dentro de um período razoável (tal período razoável deve considerar a natureza da alteração e o risco para a BT).

3.6 O Fornecedor deve, com periodicidade mínima anual ou quando houver alterações materiais aos Produtos ou à respetiva forma de fornecimento, rever os Requisitos de segurança para garantir que se mantêm compatíveis com todos os Requisitos de segurança aplicáveis.

3.7 Se o Fornecedor subcontratar obrigações ao abrigo do Contrato, deve garantir que todos os Contratos com os Subcontratados relevantes incluem termos por escrito que exijam a conformidade dos subcontratados com os Requisitos de segurança da BT, na medida em que estes sejam aplicáveis. Estes termos devem estar em vigor entre o Fornecedor e respetivo Subcontratado antes de o Subcontratado ou qualquer seu funcionário ter a possibilidade de aceder aos sistemas e Informações da BT.

Uso das Informações da BT

3.8 O Fornecedor não deve usar as informações da BT para quaisquer fins que não os que foram facultados ao Fornecedor, e na medida do necessário para permitir que o Fornecedor desempenhe as suas obrigações contratuais. Nos casos em que o Fornecedor processe Dados pessoais, não deve usar quaisquer dados pessoais que façam parte das Informações da BT para qualquer finalidade que não a especificada no Anexo relativo a processamento.

3.9 As Informações da BT podem ser conservadas durante o tempo necessário para o desempenho do Contrato, após o qual não deverão ser conservadas por mais de dois anos, salvo se for acordado um período de conservação diferente entre a BT e o Fornecedor, ou caso seja necessário ao abrigo de qualquer legislação aplicável. Para que não restem dúvidas, nos casos em que o Fornecedor processe Dados pessoais, não deve conservar quaisquer dados pessoais que façam parte das informações da BT durante um período superior aos períodos especificados no Anexo relativo a processamento ou na Condição intitulada "**Proteção de dados pessoais**".

3.10 O Fornecedor deve respeitar as políticas e normas aplicáveis em:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Caso os Produtos sejam diretamente suportados por um Contrato com o Governo do Reino Unido, o Fornecedor deve cumprir a mais recente versão do Cyber Essentials Plus.

Tratamento de informações

3.12 O Fornecedor deve manter e seguir processos de tratamento de informações materialmente consistentes com a Especificação de classificação e tratamento de informações de terceiros que, no mínimo, garantam que o Fornecedor:

3.12.1 implementa processos adequados para evitar a distribuição não autorizada de Informações da BT em qualquer formato, incluindo por e-mail, fax, redes sociais, impressão ou correio postal (por exemplo, assegurando uma política de secretária e ecrã limpos e garantindo que nenhuma informação estritamente confidencial seja enviada por fax ou e-mail);

3.12.2 não discute quaisquer informações da BT em reuniões, exceto se os participantes: (i) estiverem autorizados a participar na referida reunião; (ii) necessitem de conhecer a informação em discussão; (iii) estejam cientes e considerem as suas obrigações de confidencialidade;

3.12.3 não armazena informações da BT:

3.12.3.1 na nuvem ou com serviços da internet, incluindo, sem se limitar, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin ou Facebook, exceto se acordado por escrito com a BT;

3.12.3.2 em nenhum computador portátil ou outro dispositivo, exceto se protegido com um recurso de encriptação total do disco (como BitLocker) que atenda às normas indicadas no parágrafo 3.15; ou

3.12.3.3 elimina ou armazena as informações da BT, para além do uso das atividades comerciais diárias, de uma forma segura.

Controlo de acessos

3.13 O Fornecedor deve manter controlos de acessos nos respetivos Sistemas que sejam apropriados ao ambiente e à natureza dos Produtos fornecidos à BT, e inclusive, deve garantir que, onde aplicável:

3.13.1 todos os utilizadores, incluindo os utilizadores com nível de administrador, possuem ID únicas;

3.13.2 são exigidas alterações regulares das palavras-passe (no mínimo a cada 90 dias);

3.13.3 são implementadas as proteções adequadas na sequência de tentativas de início de sessão infrutíferas para impedir ataques de força bruta;

3.13.4 as contas não utilizadas são desativadas automaticamente;

3.13.5 as palavras-passe possuem uma força apropriada (com uma exigência mínima de 8 caracteres englobando três das seguintes categorias: (i) maiúsculas; (ii) minúsculas; (iii) caracteres numéricos; e (iv) caracteres não alfanuméricos) utilizados e o histórico de palavras-passe é forçado a proibir a utilização de palavras-passe usadas anteriormente num período de 12 meses;

3.13.6 o acesso aos Sistemas do Fornecedor com base em funções é implementado como controlo de acesso mínimo mais rigoroso para o acesso de administrador; e

3.13.7 são levadas a cabo revisões e auditorias regulares ao acesso dos utilizadores.

Acesso remoto

3.14 O Fornecedor não pode permitir que o Pessoal contratado tenha acesso remoto às informações classificadas como Estritamente confidenciais, salvo se acordado por escrito de outra forma com a BT. Nos casos em que seja permitido o acesso remoto, o Fornecedor deve assegurar que o acesso remoto está sujeito a controlos de segurança dentro da organização do Fornecedor, incluindo, sem se limitar, o acesso remoto por parte dos utilizadores ser sujeito a uma forte autenticação de dois fatores. Caso seja utilizado acesso remoto através de redes públicas para fins de assistência, as ligações deverão ser encriptadas em conformidade com as normas definidas no parágrafo 3.15.

Transmissão de dados

3.15 A transmissão de Registos em massa de rotina das Informações da BT deve ser efetuada via PGP ou por meio de uma plataforma de transferência aprovada no sector.

Encriptação

3.16 O Fornecedor deve garantir que as informações Confidenciais e Estritamente confidenciais da BT são encriptadas, quer se tratem de informações estáticas ou em trânsito, em conformidade com as Boas práticas de segurança da indústria, assegurando que não são utilizadas normas descontinuadas pelo sector. As normas de encriptação atuais aprovadas pela BT na Data de início que cumprem os requisitos deste parágrafo 3.15 são estipuladas na Especificação de classificação e tratamento de informações de terceiros.

Correções

3.17 O Fornecedor deve manter e seguir um processo de gestão de correções documentado que, no mínimo, deve garantir que o Fornecedor:

3.17.1 implementa correções dentro dos seguintes cronogramas:

Tipo de correção	Descrição	Cronograma
Correções críticas	Correções necessárias para abordar vulnerabilidades de zero dias.	Assim que for praticável e, em qualquer caso, no prazo de 14 dias após a disponibilização de uma correção.
Correções importantes	Vulnerabilidades classificadas como Alta 7.0 – 8.9 na escala de classificação de gravidade qualitativa do Sistema de Pontuação de Vulnerabilidade Comum (CVSS).	No prazo de 30 dias a partir da disponibilização de uma correção.
Outras correções	Todas as correções que não sejam importantes ou críticas	No prazo de 8 semanas a partir da disponibilização de uma correção.

3.17.2 monitoriza todos os Fornecedores aplicáveis relativamente à versão das correções;

3.17.3 utiliza correções obtidas de: diretamente de vendedores para sistemas de proprietário e correções (i) assinadas digitalmente ou (ii) verificadas através do uso de um hash do Fornecedor (não devem ser usados hashes MD5) para o pacote de atualização, de forma que a correção possa ser identificada como oriunda de uma comunidade de assistência de software de código aberto fidedigna;

3.17.4 testa todas as correções em sistemas que representam com exatidão a configuração dos sistemas de produção de destino antes da implementação da correção em sistemas de produção. A operação correta do serviço ao qual a correção foi aplicada é verificada após qualquer atividade de aplicação de correções; e

3.17.5 mantém e atualiza Sistemas do Fornecedor que garantam a aplicação das correções de Fornecedores mais atualizadas.

3.18 Caso um sistema não possa ser corrigido pelo Fornecedor com recurso a correções, o Fornecedor deve notificar a BT por escrito. Ao receber a referida notificação, a BT deve analisar o risco associado ao uso continuado do sistema pelo Fornecedor para a BT e para as Informações da BT, e pode ainda requerer que o Fornecedor tome quaisquer medidas razoáveis (a expensas do Fornecedor) para fazer face aos riscos em questão.

Gestão de vulnerabilidades

3.19 O Fornecedor deve manter e seguir um processo de gestão de vulnerabilidades que, no mínimo, deve garantir que o Fornecedor:

3.19.1 toma as medidas necessárias (por exemplo, análise) para identificar as vulnerabilidades;

3.19.2 leva regularmente a cabo os seus próprios testes de penetração; mantém relatórios sobre os referidos testes; e

3.19.3 reage a qualquer notificação de vulnerabilidades e implementa planos de ação para mitigar vulnerabilidades conhecidas em conformidade com os parágrafos 3.22 a 3.27.

Testes de penetração

3.20 O Fornecedor deve:

3.20.1 permitir que a BT (ou subcontratados autorizados pela BT) leve a cabo testes de penetração razoáveis, num prazo razoável; e

3.20.2 fornecer à BT acesso aos relatórios de testes de penetração do Fornecedor existentes relevantes para os Produtos fornecidos.

Auditoria e registo

3.21 O Fornecedor deve manter e seguir um processo de auditoria e registo que, no mínimo, garanta que o Fornecedor regista (conforme apropriado) os seguintes eventos:

3.21.1 os pontos de início e fim do processo alvo de registo;

3.21.2 as alterações ao tipo de eventos registados, conforme exigido pelo registo de auditoria (por exemplo, os parâmetros de arranque e quaisquer alterações aos mesmos);

3.21.3 arranque e encerramento do sistema do Fornecedor;

3.21.4 inícios de sessão bem-sucedidos;

3.21.5 tentativas de início de sessão falhadas (por exemplo, ID ou palavra-passe incorretas);

3.21.6 todas as operações realizadas por utilizadores privilegiados (por exemplo, utilizadores com amplo acesso aos utilitários ou aplicações do sistema);

3.21.7 escalamentos de privilégios bem e malsucedidos;

3.21.8 todos os acessos ou operações efetuadas pelo Fornecedor ou Pessoal contratado do Fornecedor a informação estritamente confidencial; e

3.21.9 criação, modificação e eliminação de contas de utilizador.

3.22 Para cada evento auditável, o Fornecedor deve manter um registo de auditoria à prova de adulterações que permita a reconstrução dos referidos eventos.

3.23 Considerando a criticidade do componente/dados, o Fornecedor deve inspecionar e analisar os registos de auditoria com regularidade a fim de detetar comportamentos suspeitos ou anómalos, tomar as medidas adequadas e/ou lançar um alarme.

3.24 Todos os alarmes devem ser documentados e postos em prática de forma atempada com base na criticidade do alarme.

3.25 O Fornecedor deve manter todos os ficheiros de registo durante 3 meses (exceto se for requerida a sua eliminação no âmbito da Condição intitulada "**Proteção de dados pessoais**") e deve efetuar cópias ou permitir o acesso aos ficheiros de registo a pedido da BT, num formato acordado entre as ambas as Partes.

Gestão de ameaças e tratamento de incidentes

3.26 O Fornecedor deve manter e seguir um processo de gestão de incidentes formal que inclua responsabilidades definidas para lidar com um Incidente de segurança relevante. Qualquer informação relacionada com um Incidente de segurança relevante deve ser tratada como "**Confidencial**".

3.27 O Fornecedor deve informar o Contacto de Segurança da BT e o contacto comercial da BT, dentro de um período razoável, quando tiver conhecimento de qualquer incidente de segurança pertinente e, em qualquer caso, sempre nas doze (12) horas a seguir ao momento em que tomou conhecimento do Incidente de segurança relevante.

3.28 Com a maior brevidade, o Fornecedor deve tomar as medidas corretivas apropriadas atempadamente para mitigar quaisquer riscos e efeitos relacionados com o Incidente de segurança relevante a fim de reduzir a gravidade e a duração do incidente.

3.29 O Fornecedor concorda em fornecer todas as informações razoavelmente solicitadas pela BT relativamente a um Incidente de segurança relevante, incluindo, sem se limitar:

3.29.1 data e hora;

3.29.2 localização;

3.29.3 tipo de incidente;

3.29.4 impacto;

3.29.5 classificação de informações afetadas;

3.29.6 estado; e

3.29.7 resultado (incluindo as recomendações de resolução ou medidas tomadas).

3.30 O Fornecedor deve garantir que os riscos identificados quanto a confidencialidade, integridade ou disponibilidade de informações da BT nos processos ou Sistemas do Fornecedor são resolvidos atempadamente.

3.31 Caso um Incidente de segurança relevante seja simultaneamente uma violação de dados pessoais, o Fornecedor deve também respeitar as disposições da Condição intitulada "**Proteção de dados pessoais**", juntamente com as disposições destes Requisitos de segurança. Para que não restem dúvidas, o Fornecedor deve também respeitar as disposições da Condição intitulada "**Proteção de dados pessoais**" relativamente a todas as violações de dados pessoais, independentemente de a violação constituir ou não um Incidente de segurança relevante.

4 SEGURANÇA DO PESSOAL CONTRATADO

4.1 Não deve ser concedido acesso ao Pessoal contratado até este ter concluído a formação sobre segurança das informações da BT, acessível em https://workingwithbt.extra.bt.com ou através do sistema de aprendizagem da BT, nos casos em que o Pessoal contratado tenha um número de identificação atribuído. A formação sobre Segurança das Informações da BT deve ser alvo de reciclagem periódica, conforme detalhado em https://workingwithbt.extra.bt.com. O Fornecedor deve manter registos da formação e disponibilizá-los para auditoria por parte da BT.

4.2 O Fornecedor deve assegurar que todo o Pessoal contratado assina acordos de confidencialidade que incluam obrigações materialmente similares às impostas pelo Fornecedor na Parte 2 acima, antes de qualquer Pessoal contratado começar a trabalhar em edifícios ou Sistemas da BT ou antes de ter acesso a informações da BT. Estes acordos de confidencialidade devem ser conservados pelo Fornecedor e disponibilizados para auditoria à BT.

4.3 O Fornecedor deve lidar com violações das políticas e procedimentos de segurança do Fornecedor e da BT por meio de processos formais, incluindo medidas disciplinares que podem incluir impedir o indivíduo de:

4.3.1 ter acesso aos Sistemas da BT ou às informações da BT; ou

4.3.2 realizar trabalhos relacionados com o fornecimento dos Produtos.

Além disso, o Fornecedor deve garantir que estão implementados os processos relevantes para garantir que qualquer Pessoal contratado que tenha sido desta forma impedido não obtém acesso posterior aos Sistemas da BT, às informações da BT nem é autorizado a trabalhar de alguma forma relacionada com o fornecimento dos Produtos.

4.4 O Fornecedor deve, conforme permitido por lei, manter uma linha telefónica confidencial, disponível a todos os seus funcionários, para ser usada pelo Pessoal contratado caso seja instruído a atuar de forma inconsistente com ou em violação destes Requisitos de segurança. Os relatórios relevantes devem ser transmitidos ao Contacto de Segurança da BT.

4.5 Nos casos em que o Pessoal contratado deixa de estar afeto aos Produtos, o Fornecedor deve assegurar que:

4.5.1 o acesso à informação da BT é revogado; e

4.5.2 a critério da BT, quaisquer ativos físicos ou informações da BT na posse de Pessoal contratado devem ser:

4.5.2.1 entregues à equipa operacional da BT relevante; ou

4.5.2.2 destruídos em conformidade com a versão mais atual da Especificação de classificação e tratamento de informações de terceiros.

4.6 Salvo acordo por escrito em contrário com o Contacto de Segurança da BT, o Fornecedor deve implementar um procedimento de saída controlado para o Pessoal contratado que inclua o pedido por escrito ao Contacto de Segurança da BT para a remoção do acesso aos Sistemas da BT, às informações da BT, e qualquer outro Acesso e acessos. O Pessoal contratado deve ser informado de que o seu acordo de confidencialidade permanecerá em vigor e que as informações da BT adquiridas no decorrer do seu trabalho nos Produtos não devem ser divulgadas.

4.7 Como parte da concessão do acesso, o Fornecedor deve manter e fornecer registos de todo o Pessoal contratado que requeira acesso ou esteja envolvido no fornecimento dos Produtos à BT, incluindo o seu nome, local de trabalho, endereço de e-mail profissional, número de telefone profissional direto e extensão (se aplicável) e/ou número de telemóvel, a data em que o pedido do número de identificação de utilizador (UIN) foi solicitado (se aplicável), data em que foram designados para o fornecimento dos Produtos à BT, data em que completaram a formação obrigatória, data em que deixam de fornecer Produtos e uma declaração de verificação de antecedentes pré-contratação. Será responsabilidade do Contacto de segurança do Fornecedor garantir sempre que apenas o Pessoal contratado relevante possui autorização.

4.8 O Fornecedor deve ter políticas e processos implementados para garantir que o Pessoal contratado não usa as redes sociais para publicar online qualquer declaração, comentário, conteúdo ou imagens que:

4.8.1 possam razoavelmente ser entendidos como as visões da BT;

4.8.2 divulguem qualquer informação da BT que seja informação confidencial, ou assinalada como “Confidencial” ou “Estritamente confidencial”; e

4.8.3 sejam difamatórios para a BT e possam causar danos à marca e reputação da BT.

5 AUDITORIA E AVALIAÇÃO DE SEGURANÇA

5.1 Sem prejuízo de qualquer outro direito de auditoria que a BT eventualmente detenha, a fim de avaliar a conformidade do Fornecedor com estes Requisitos de segurança e onde for aplicável a condição intitulada “**Proteção de informações pessoais**”, a BT e seus representantes designados reservam o direito de realizar uma auditoria de conformidade de segurança, periodicamente, com base em qualquer ou em todos os aspetos das políticas, processos e Sistemas do Fornecedor (sujeito à proteção por parte do Fornecedor da confidencialidade das informações não relacionadas com o fornecimento dos Produtos à BT), por uma análise de segurança documental ou às instalações do Fornecedor e de qualquer Subcontratado que estejam materialmente envolvidos no fornecimento dos Produtos ou na execução do Contrato.

5.2 O Fornecedor deve fornecer à BT, ou aos seus representantes, acesso e assistência conforme necessário e adequado para permitir a realização de análises de segurança documentais ou auditorias às instalações. O Fornecedor deve ser notificado sobre a auditoria de rotina às instalações com uma antecedência mínima de 30 dias úteis, porém, para que não restem dúvidas, em caso de violação efetiva ou suspeita violação de dados pessoais ou violação de segurança relevante, a BT não procederá a essa notificação prévia.

5.3 O Fornecedor deve trabalhar com a BT para implementar as recomendações acordadas e levar a cabo qualquer ação corretiva que a BT considere necessária decorrente de uma análise de segurança documental ou auditoria às instalações no prazo de 30 dias após a notificação das referidas recomendações ou medidas corretivas pela BT, ou após qualquer prazo acordado entre as partes, a expensas do Fornecedor.

5.4 Caso a BT necessite de conduzir uma auditoria independente ao Fornecedor e se determine que o Fornecedor não atua em conformidade com os princípios e práticas da ISO/IEC 27001:2013, então o Fornecedor deve comprometer-se, a expensas suas, a levar a cabo as medidas necessárias a fim de assegurar a conformidade necessária e reembolsar integralmente a BT por todos os custos incorridos na obtenção da referida auditoria.

6 INVESTIGAÇÃO

6.1 Se a BT tiver razões para suspeitar que ocorreu:

6.1.1 uma Violação de dados pessoais;

6.1.2 uma Violação de segurança relevante;

6.1.3 ou uma violação destes Requisitos de segurança;

deverá informar o Contacto de segurança do Fornecedor, e o Fornecedor concorda, a expensas suas:

6.1.4 tomar medidas imediatas para investigar a suspeita de violação e para identificar, prevenir e envidar os esforços razoáveis para mitigar os efeitos de qualquer das referidas violações; e

6.1.5 efetuar quaisquer medidas de recuperação ou outras medidas necessárias para sanar a violação;

6.1.6 fornecer à BT os relatórios que a BT possa razoavelmente exigir sobre os resultados da investigação e as medidas tomadas para remediar ou mitigar a violação.

Em caso de violação grave, o Fornecedor deve cooperar totalmente com a BT em qualquer investigação ou auditoria efetuada pela BT, uma entidade reguladora e/ou as autoridades, que inclua (mediante aviso prévio razoável pela BT ao Fornecedor) acesso às informações da BT contidas nas instalações do Fornecedor ou nos Sistemas do Fornecedor.

Durante qualquer investigação, o Fornecedor deve cooperar com a BT, fornecendo acesso e assistência conforme necessário e adequado para investigar a violação. A BT pode solicitar ao Fornecedor uma quarentena para avaliação de qualquer ativo tangível ou intangível, pertencentes ao Fornecedor, a fim de auxiliar na investigação, e o Fornecedor não deve reter ou atrasar excessivamente o referido pedido.

PARTE 4: REQUISITOS ESPECÍFICOS DE SEGURANÇA

7 REQUISITOS E POLÍTICA DE SEGURANÇA GENÉRICOS

7.1 O Fornecedor garante e declara que os Sistemas do Fornecedor, Produtos, serviços associados, processos e locais físicos do Fornecedor se encontram, e encontrarão permanentemente em conformidade com a norma ISO/IEC 27001:2013 e qualquer versão alterada ou futura da referida norma. Esta conformidade deve ser garantida, a exclusivo critério da BT, por:

7.1.1 certificação do SGSI do Fornecedor por uma entidade de certificação UKAS ou uma entidade de certificação internacional equivalente cujo âmbito e aplicabilidade tenham sido validados pela BT; ou

7.1.2 um processo de auditoria e teste bilateral especificado pela BT.

7.2 O Fornecedor deve enviar um certificado ISO/IEC 27001 válido no início do Contrato e nas futuras renovações da certificação.

7.3 Caso o âmbito do certificado ou declaração de aplicabilidade seja alterado em qualquer momento, o Fornecedor deve enviar essas alterações para revalidação usando o procedimento de controlo de alterações (ou, na ausência de um procedimento de controlo de alterações, através do processo de variação). O Fornecedor deve informar a BT num prazo de 2 dias úteis sobre qualquer inconformidade significativa identificada pela entidade de certificação ou pelo Fornecedor.

8 SEGURANÇA FÍSICA — INSTALAÇÕES DA BT

A conformidade com esta secção é necessária se o fornecimento de Produtos pelo Fornecedor decorrer nas instalações da BT.

8.1 Todo o Pessoal contratado que trabalhe em instalações da BT deve estar na posse de, e usar de forma visível, um cartão de identificação fornecido pelo Fornecedor ou pela BT, comprovando que está autorizado (o "**Cartão de acesso autorizado**"). Os Cartões de acesso autorizado deverão conter uma fotografia que seja nítida e uma representação fiel do Pessoal contratado. Também pode ser fornecido ao Pessoal contratado um cartão de acesso eletrónico e/ou um cartão de visitante de duração limitada que deve ser utilizado em conformidade com as instruções de emissão locais.

8.2 Quando a BT emitir um Cartão de acesso autorizado para o Pessoal contratado, o Fornecedor deve notificar a BT de imediato e em qualquer situação no prazo de 5 dias úteis caso o referido Pessoal contratado deixe de necessitar do acesso às instalações da BT.

8.3 Apenas é permitida a ligação direta (ligar à porta LAN ou ligação sem fio) a domínios da BT de servidores de compilação aprovados pela BT, PC Webtop da BT e dispositivos finais fiáveis. O Fornecedor não deve (e, se for caso disso, deve garantir que qualquer Pessoal contratado não o faça), sem autorização prévia por escrito do Contacto de Segurança da BT, ligar um equipamento não aprovado pela BT a qualquer domínio da BT. O Contacto de Segurança da BT apenas deverá fornecer a autorização por escrito após iniciar o processo de concessões da política de segurança na BT. Em qualquer caso, o Fornecedor deve garantir que nenhum equipamento propriedade do Pessoal contratado ou quaisquer outros funcionários (incluindo empreiteiros, funcionários interinos e trabalhadores temporários) seja usado para armazenar, aceder ou processar quaisquer dados da BT.

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

8.5 A proteção física e orientações para trabalhar nas instalações da BT devem ser respeitadas e devem incluir, sem se limitar, o acompanhamento do Pessoal contratado por um indivíduo designado e a adoção de práticas adequadas de trabalho em áreas seguras.

8.6 Quando o Fornecedor estiver autorizado a fornecer ao seu Pessoal contratado acesso sem vigilância a áreas dentro da propriedade da BT, o signatário e o Pessoal contratado autorizado pela BT devem seguir o documento de orientação "**Acesso do Fornecedor a locais e edifícios da BT**" https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. Além disso, deve proceder-se no mínimo à verificação de antecedentes pré-contratação L2 https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf dos signatários e Pessoal contratado não autorizados pela BT.

9 SEGURANÇA FÍSICA — INSTALAÇÕES DO FORNECEDOR

A conformidade com esta secção é necessária se o fornecimento de Produtos pelo Fornecedor decorrer em instalações que não sejam propriedade da BT. (Por exemplo, Fornecedores terceiros)

9.1 O acesso a instalações que não sejam propriedade da BT (locais, edifícios ou áreas internas) onde os Produtos sejam fornecidos, ou onde as informações da BT sejam armazenadas ou processadas, apenas deve ser admissível mediante a utilização de um cartão de identificação do Fornecedor autorizado. Este cartão deve ser usado como um meio de verificação de identidade no local aplicável, a qualquer momento e, como tal, a fotografia exibida no cartão deve ser nítida e uma representação fiel do indivíduo. Também pode ser fornecido aos indivíduos um cartão de acesso autorizado eletrónico para aceder às instalações aplicáveis ou via teclado numérico de acesso seguro. O Fornecedor deve possuir processos para: a autorização, a divulgação de alterações de código (que deve ocorrer mensalmente, no mínimo); e as alterações de código ad hoc.

9.2 O Fornecedor deve assegurar que o acesso às instalações da BT onde se leva a cabo o fornecimento dos Produtos ou, onde as informações da BT sejam armazenadas ou processadas, tenha de ser autorizado. Além disso, o Fornecedor deve respeitar os processos de segurança e procedimentos de controlo e monitorização do Pessoal contratado, visitantes e outras pessoas externas, incluindo terceiros com acesso físico a estas áreas (por ex.: controlo ambiental, manutenção, empresas de alarmes, empresas de limpeza).

9.3 Se solicitado pela BT, o Fornecedor deve assegurar que o Pessoal contratado se encontra separado, de uma forma segura, de todos os restantes funcionários do Fornecedor. O Fornecedor deve ainda garantir que os sistemas e infraestrutura usados para fornecer os Produtos estão contidos numa rede lógica dedicada. Esta rede deve ser composta apenas pelos sistemas dedicados à entrega de uma instalação de processamento de dados segura.

9.4 As áreas seguras nas instalações do Fornecedor (por ex: salas de comunicações de rede), devem estar separadas e protegidas pelos controlos de entradas apropriados para garantir que apenas é permitido o acesso de Pessoal contratado autorizado a estas áreas seguras. O acesso feito a estas áreas por qualquer Pessoal contratado deve ser controlado, no mínimo, mensalmente, e uma avaliação de reatribuição de autorizações aos direitos de acesso a estas áreas deve ser realizada com uma periodicidade mínima anual.

Devem ser fornecidas provas de avaliação de riscos pelo Fornecedor à BT, se solicitado. Caso tal não seja disponibilizado quando solicitado pela BT, a critério da mesma, deve ser levada a cabo pela BT ou por um seu representante uma avaliação de riscos do ambiente utilizado para a prestação do serviço (tais como centros de dados, áreas de processamento de dados, salas de computadores), antes de início do fornecimento dos Produtos. Além disso, a BT deve ser previamente informada sobre quaisquer trabalhos substanciais em quaisquer instalações que possam comprometer a segurança das Informações da BT.

9.5 Devem ser utilizados pelo Fornecedor sistemas de segurança CCTV e o suporte de gravação associado quer em resposta a incidentes de segurança, quer como uma ferramenta de vigilância de segurança, como elemento dissuasor ou como auxílio para a eventual apreensão de indivíduos apanhados em flagrante delito. No caso em que as imagens de CCTV são gravadas (em cassete ou digitalmente), devem ser conservadas por um período mínimo de 20 dias. Este período pode, no entanto, ser prolongado nas seguintes situações:

9.5.1 quando a prova em vídeo CCTV tiver de ser mantida na sequência de um incidente ou investigação criminal; ou

9.5.2 quando especificado como requisito necessário para cumprir com a legislação.

9.5.3 Todas as gravações de CCTV devem ser armazenadas num armário trancado e a chave deve ser guardada de forma segura e controlada. O acesso ao armário deve ser restrito apenas a pessoal autorizado.

9.6 Todos os gravadores de CCTV devem estar situados em locais seguros para impedir a modificação ou eliminação de imagens e a possibilidade de visualização "casual" de quaisquer ecrãs de CCTV associados e em conformidade com as orientações sobre o uso de CCTV, que podem ser encontradas em:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 Todas as áreas das instalações do Fornecedor utilizadas para a prestação de Serviços e Produtos devem ser inspecionadas pelo Fornecedor em busca de riscos e ameaças, com uma periodicidade mínima mensal. O Fornecedor deve ter considerado e implementado todas as medidas adequadas para garantir a segurança física relativamente aos pontos seguintes:

9.7.1 consciencialização para ameaças locais, incluindo, sem se limitar, potenciais ameaças da indústria local e a proximidade de materiais perigosos armazenados; e

9.7.2 desastres naturais, incluindo riscos de ameaças que incluam, sem se limitar, inundação, desabamento ou condições meteorológicas extremas.

9.8 Cablagem elétrica e de telecomunicações nas instalações do Fornecedor que contenha dados ou suporte os serviços de informações ou serviços de rádio/satélite utilizados no fornecimento de Produtos deve ser avaliada pelo Fornecedor para verificar o nível de proteção a fim de evitar a interrupção das operações comerciais. Medidas de proteção de segurança física avaliadas de acordo com a criticidade das operações comerciais devem ser implementadas da seguinte forma:

9.8.1 vias de rodagem críticas para a atividade, blindagem dos cabos, câmaras de visita ou caixas no pavimento que contenham cablagem crítica para a atividade devem ser protegidos;

9.8.2 o acesso a câmaras de cablagem ou armários para subida de cabos no interior dos edifícios operacionais deve ser reservado com a utilização de leitores de controlo de acesso eletrónicos ou por uma gestão de chaves eficaz;

9.8.3 as ligações de comunicações informáticas e equipamentos de comunicação nas instalações informáticas devem ser física e ambientalmente protegidas; e

9.8.4 as ligações de comunicações de rádio e satélite e o equipamento de comunicação devem ser adequadamente protegidos.

9.9 A BT exigirá, salvo acordo em contrário entre o Fornecedor e o Contacto de Segurança da BT, que sejam implementados pelo Fornecedor serviços de segurança com presença de operador para complementar as medidas de segurança física e eletrónica nas instalações do Fornecedor onde:

9.9.1 a localização seja de importância operacional (por ex.: centros de contacto, centros de dados, principais pontos da rede, etc.);

9.9.2 as informações da BT processadas possam afetar ou prejudicar a reputação e a marca da BT;

9.9.3 seja processado um elevado volume de informações da BT (por ex.: terceirização do processo comercial);

9.9.4 existam requisitos contratuais do Cliente;

9.9.5 haja um risco/ameaça local específico;

9.9.6 o Fornecedor esteja na posse de informações altamente sensíveis da BT.

9.10 Para proteger os equipamentos da BT (como servidores ou interruptores BT) nas instalações do Fornecedor contra ameaças ambientais ou perigos e possibilidade de acesso não autorizado, os equipamentos da BT devem estar situados numa área protegida e separados dos equipamentos utilizados em sistemas de organizações não pertencentes à BT. O nível de separação deve garantir que a segurança do equipamento da BT não pode ser comprometida, deliberada ou acidentalmente, como resultado de acesso concedido a organizações não pertencentes à BT e pode, por exemplo, assumir a forma de partições seguras por meio de paredes, armários com chave ou estruturas de metal.

9.11 O Fornecedor deve ter implementado as medidas adequadas para garantir a segurança física relativamente aos pontos seguintes:

9.11.1 medidas de prevenção de incêndios incluindo, sem se limitar, alarmes e equipamentos de deteção e supressão;

9.11.2 condições climáticas, tendo em conta a temperatura, humidade e eletricidade estática e a gestão, monitorização e resposta associadas a condições extremas (por exemplo, alarmes de encerramento automático);

9.11.3 equipamento de controlo incluindo, sem se limitar, ar condicionado e deteção de água;

9.11.4 localização de reservatórios de água, tubagens, etc. dentro das instalações;

9.11.5 acesso auditável: onde o acesso apropriado aos sistemas por parte do pessoal deva ser auditável; e

9.11.6 supervisão do Pessoal contratado normalmente não associado à gestão de acessos ou ao acesso a Sistemas da BT.

9.12 Perímetros de segurança (barreiras como paredes, vedações, portões de entrada controlada por cartão ou balcões de receção com operador) devem ser usados para proteger áreas que contenham informações confidenciais da BT ou informações de Clientes da BT (incluindo Dados pessoais) e as instalações de processamento associadas.

9.13 Os pontos de acesso, como as áreas de carga e descarga e outros pontos onde possam entrar pessoas não autorizadas nas instalações, devem ser controlados e, se possível, isolados das instalações de processamento das informações para evitar o acesso não autorizado ou ataques deliberados.

9.14 O Fornecedor deve garantir que o acesso físico às áreas que têm acesso às informações da BT ou às informações de Clientes da BT (incluindo Dados pessoais) é efetuado por meio de cartões inteligentes ou cartões de proximidade (ou sistemas de segurança equivalente) e o Fornecedor deve realizar auditorias internas, no mínimo mensalmente, para garantir a conformidade com estas disposições.

9.15 O Fornecedor deve assegurar que a fotografia e/ou a captura de imagem de quaisquer informações da BT ou de informações de Clientes da BT (incluindo Dados pessoais) é proibida. Em circunstâncias excecionais onde possa haver requisitos comerciais sobre a captura dessas imagens, deve ser obtida, por escrito, uma isenção temporária a esta disposição junto do Contacto de Segurança da BT.

9.16 O Fornecedor deve manter uma política de secretária e ecrã limpos para proteger as informações da BT.

10 FORNECIMENTO DE EQUIPAMENTO DE ALOJAMENTO

A conformidade com esta secção é necessária se o Fornecedor oferecer um ambiente de alojamento para equipamento da BT ou de Clientes da BT.

10.1 Caso o Fornecedor ofereça uma área de acesso seguro nas suas instalações para alojamento de equipamentos da BT ou de Clientes da BT ("**Instalações do Fornecedor**"):

10.1.1 garantir que todo o Pessoal contratado com acesso às instalações do Fornecedor está na posse de um cartão de identificação ou de um cartão de controlo de acessos eletrónico. Este cartão deve ser usado apenas como um meio de verificação de identidade nas instalações do Fornecedor, a qualquer momento e, como tal, a fotografia exibida no cartão deve ser nítida e uma representação fiel do Pessoal contratado; e

10.1.2 ter implementado procedimentos para lidar com ameaças de segurança dirigidas contra o equipamento da BT ou de Clientes da BT ou contra terceiros que trabalhem em nome da BT para salvaguardar as informações do Cliente da BT e da BT nas instalações do Fornecedor; e

10.1.3 usar sistemas de segurança CCTV e suporte de gravação associado nas instalações do Fornecedor em resposta a incidentes de segurança, como uma ferramenta de vigilância de segurança, como um elemento dissuasor e como um auxílio para a eventual apreensão de indivíduos apanhados em flagrante delito. O Fornecedor deve assegurar que são gravados 20 dias de CCTV para que constitua um instrumento de investigação eficaz; e

10.1.4 fornecer à BT uma planta do andar onde tenha atribuído um espaço numa área segura das instalações do Fornecedor; e

10.1.5 garantir que os armários da BT e do Cliente da BT nas instalações do Fornecedor se encontram trancados e são acedidos exclusivamente por pessoal autorizado da BT, representantes autorizados da BT e Pessoal contratado relevante; e

10.1.6 implementar um processo de gestão de chaves seguro nas instalações do Fornecedor; e

10.1.7 inspecionar regularmente a área que circunda as instalações do Fornecedor para deteção de riscos e ameaças; e

10.1.8 documentar e manter os procedimentos operacionais (no idioma do país de origem do trabalho da BT) para cumprimento dos Requisitos de segurança detalhados neste parágrafo 10 e, a pedido, fornecer à BT acesso a essa documentação.

10.2 A BT deve facultar ao Fornecedor:

10.2.1 um registo dos ativos físicos do Cliente da BT e/ou da BT armazenados nas instalações do Fornecedor; e

10.2.2 dados dos funcionários da BT, subcontratados e agentes que necessitem de acesso às instalações do Fornecedor (de forma contínua).

11 DESENVOLVIMENTO DOS SERVIÇOS

A conformidade com esta secção é necessária se o Fornecedor lidar com o desenvolvimento de Produtos para utilização pela BT e/ou Clientes da BT. Isto inclui componentes imediatamente disponíveis (off the shelf), configuração de software e componentes de fabrico dos Produtos.

11.1 O Fornecedor deve implementar as medidas de segurança acordadas de uma forma transversal a todos os componentes fornecidos que constituam os Produtos e/ou Serviços de uma forma que proteja a confidencialidade, disponibilidade e integridade dos Produtos, incluindo:

11.1.1 manter a documentação apropriada (no idioma do país de origem do trabalho da BT) em relação à implementação da segurança e assegurar que tanto a documentação como a referida segurança se encontram em conformidade com as melhores práticas da indústria;

11.1.2 minimizar as oportunidades por parte de indivíduos não autorizados (por ex., piratas informáticos) de obter acesso aos Sistemas da BT e às informações da BT, Redes da BT ou Produtos da BT; e

11.1.3 minimizar o risco de utilização abusiva dos Sistemas da BT, Informações da BT, Redes da BT ou serviços que potencialmente possam conduzir à perda de receita ou serviço.

11.2 O Fornecedor deve demonstrar, a pedido, que qualquer software ou compilação de hardware fornecidos (proprietária e imediatamente disponível) entregue à BT é igual ao acordado com a BT. O Fornecedor deve manter a integridade das compilações, incluindo atualizações, sistemas operativos e aplicação desde a criação até à utilização.

11.3 O Fornecedor deve assegurar que o desenvolvimento de sistemas para uso pela BT ou a construção e manutenção de hardware propriedade da BT segue estritamente os Requisitos de segurança da BT se fornecidos pela equipa operacional da BT ou desenvolvidos em conformidade com as melhores práticas da indústria.

11.4 O Fornecedor deve assegurar que os sistemas e processos usados para teste e desenvolvimento de atividades estão separados dos sistemas de produção. Deve ser usado um processo de controlo de alterações para a promoção de qualquer código no ambiente de produção. Os dados de teste fornecidos pela BT devem ser eliminados após um período determinado pelo proprietário dos dados da BT e não podem ser usados dados dinâmicos ou de produção em ambientes de desenvolvimento ou de teste.

11.5 Todas as vulnerabilidades de segurança críticas encontradas nos testes de segurança e classificadas como de risco médio ou superior devem ser corrigidas antes do lançamento. Quaisquer falhas de segurança nos serviços identificados pela BT ou pelo Fornecedor devem ser corrigidas a expensas do Fornecedor dentro dos prazos razoavelmente exigidos pela BT.

11.6 Os Produtos devem ser sujeitos a testes de penetração independentes encomendados pelo Fornecedor antes do lançamento, com periodicidade mínima anual e na sequência de alterações significativas ou incidentes, a expensas do Fornecedor.

11.7 Produtos desenvolvidos para uso por parte da BT ou respetivos Clientes devem ser desenvolvidos com base numa norma do sector documentada e reconhecida de Secure Development LifeCycle (SDLC) para minimizar o risco de introduzir vulnerabilidades de segurança no ambiente de produção e/ou nos Clientes. A SDLC deve incluir as seguintes portas, com artefactos tangíveis resultantes de cada análise e disponíveis para inspeção pela BT no âmbito da auditoria no parágrafo 5 da Parte 3 dos presentes Requisitos de segurança:

11.7.1 análise de segurança dos requisitos comerciais;

11.7.2 análise de segurança da conceção;

11.7.3 análise de segurança do código fonte — automática ou manual; e

11.7.4 auditoria de segurança da solução antes da implementação (incluindo ataques simulados) de acordo com um plano de auditoria documentado, específico para o projeto, com base nos relatórios resultantes de análises de segurança dos requisitos comerciais, de conceção e de código.

Outras orientações podem ser encontradas nas Normas de orientação para terceiros do sector sobre “Codificação Segura”:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 DEPÓSITO DE GARANTIA

Agora contida no Contrato principal.

13 ACESSO AOS SISTEMAS DA BT

A conformidade com esta secção é necessária se o Pessoal contratado necessitar de aceder aos Sistemas da BT para fornecer os Produtos.

13.1 A BT pode permitir, a seu exclusivo critério, o acesso limitado conforme estritamente necessário para o fornecimento de Produtos.

13.2 Em relação ao acesso, o Fornecedor deve comprometer-se a respeitar todas as políticas, normas e instruções relevantes que lhe foram fornecidas pela BT e deve (e irá garantir que todo o Pessoal contratado vai):

13.2.1 assegurar que a identificação de utilizadores, palavras-passe, PIN, tokens e acesso em conferência são de uso individual por parte do Pessoal contratado e não são partilhados. Os dados devem ser armazenados de uma forma segura e separados do dispositivo ao qual permitem aceder. Se uma palavra-passe for do conhecimento de outra pessoa, deve ser imediatamente alterada;

13.2.2 mediante pedido razoável, fornecer à BT os relatórios que a BT razoavelmente possa solicitar relativamente ao acesso de Pessoal contratado autorizado aos Sistemas da BT;

13.2.3 ligações entre domínios aos Sistemas da BT não deverão ser permitidas se não forem especificamente aprovadas e autorizadas pelo Contacto de Segurança da BT;

13.2.4 envidar todos os esforços razoáveis para garantir que nenhum vírus ou código malicioso (da forma como estas expressões são geralmente compreendidas na indústria informática) são introduzidos, a fim de minimizar o risco de corrupção dos Sistemas da BT ou das Informações da BT por quaisquer meios; e

13.2.5 envidar todos os esforços razoáveis para garantir que ficheiros que contenham informação, dados ou meios não relevantes para os Produtos não sejam armazenados em equipamento da BT, servidores da BT, computadores portáteis e de secretária fornecidos pela BT, instalações de armazenamento centralizado da BT ou nos Sistemas da BT.

13.2.6 nos casos em que a BT tenha facultado ao Fornecedor acesso à internet ou intranet da BT, garantir que o Pessoal contratado apenas acede à internet ou intranet da BT de forma apropriada e somente a fim de fornecer os Produtos aplicáveis e que quaisquer sites perigosos ou inaceitáveis estejam bloqueados ao utilizador. É da responsabilidade do Fornecedor garantir orientação sobre o abuso da internet e do e-mail ao Pessoal contratado, com uma periodicidade mínima anual. Esta orientação deve proibir os

13.2.6.1 utilizadores de:

(i) aceder a conteúdo ofensivo, sexual, racista ou politicamente ofensivo;
(ii) levar a cabo atos que possam prejudicar a reputação da BT e de outros indivíduos;
(iii) gerir um negócio privado;
(iv) (d) infringir direitos de autor ou
(v) ignorar ou criar um túnel na firewall da BT ou noutros mecanismos de segurança;

13.2.6.2 O Pessoal contratado não deve contribuir para sites ou publicar declarações online que possam ser entendidas como visões da BT.

13.3 O Fornecedor deve levar a cabo análises regulares para garantir que é necessário acesso para a execução das funções. Deve ser disponibilizada documentação das análises para inspeção por parte da BT nos âmbitos de auditoria descritos no parágrafo 5.1.

13.4 O Fornecedor deve notificar de imediato a BT e em qualquer situação no prazo de 5 dias úteis, quando um funcionário, incluindo empreiteiros, funcionários interinos e trabalhadores temporários, deixe de necessitar de acesso aos Sistemas da BT, por exemplo, se abandonar ou mudar de funções.

14 ACESSO A INFORMAÇÕES DA BT NOS SISTEMAS DO FORNECEDOR

A conformidade com esta secção é necessária se as informações da BT forem armazenadas ou processadas em Sistemas do Fornecedor.

14.1 Se o Pessoal contratado tiver acesso aos Sistemas do Fornecedor com a finalidade de fornecer os Produtos e/ou Serviços, o Fornecedor deve demonstrar responsabilidade por tal acesso (incluindo, sem se limitar, o uso de contas de utilizador únicas, gestão de palavras-passe e um registo de auditoria conciso sobre todas as ações do Pessoal contratado).

14.2 O Fornecedor deve manter sistemas que detetem e registem qualquer tentativa de dano, modificação ou acesso não autorizado às informações da BT nos Sistemas do Fornecedor. Os exemplos incluem, sem se limitar, o sistema de registo e auditoria de processos, IDS e IPS, etc.

14.3 O Fornecedor deve manter controlos para deteção e proteção contra software malicioso, vírus e código malicioso nos Sistemas do Fornecedor e garantir a implementação de procedimentos apropriados de consciencialização dos utilizadores.

14.4 O Fornecedor deve assegurar que qualquer software não autorizado é identificado e removido dos Sistemas do Fornecedor que contenham, processem ou acedam a informações da BT, com uma periodicidade mínima mensal.

14.5 O Fornecedor deve garantir que o acesso a portas de diagnóstico e gestão, bem como a ferramentas de diagnóstico, é controlado de forma segura.

14.6 O Fornecedor deve assegurar que o acesso às ferramentas de auditoria do Fornecedor é restrito ao Pessoal contratado e que o seu uso é monitorizado.

14.7 O Fornecedor deve garantir que as revisões de código e testes de penetração em todo o software criado internamente (incluindo qualquer Software) usado para processar informações da BT sejam realizados por uma equipa independente que não deve incluir os programadores do software.

14.8 Na medida em que alguns servidores são usados para fornecer os Produtos, não devem ser implementados em redes não fiáveis (redes fora do seu perímetro de segurança, que estejam para além do seu controlo administrativo, por ex., com ligação à internet) sem os controlos de segurança adequados.

14.9 O Fornecedor deve assegurar que as alterações aos sistemas individuais do Fornecedor que armazenem e processem informações da BT e/ou que sejam usados para fornecer os Produtos, são controlados e sujeitos a procedimentos formais de controlo de alterações.

14.10 O Fornecedor deve garantir que todos os relógios do sistema e tempos são sincronizados usando a última versão do NTP ou uma tecnologia de sincronização de tempo similar.

14.11 Quando o Fornecedor fornece sistemas que permitem o acesso online a Clientes da BT:

14.11.1 As credenciais online para Clientes da BT devem conter, no mínimo, o seguinte:

14.11.1.1 ID de utilizador;

14.11.1.2 palavra-passe online;

14.11.1.3 três perguntas e respostas de autenticação para apoiar o acesso à conta; e

14.11.1.4 um método alternativo de contacto para fins de autenticação.

14.11.2 O Cliente da BT deve poder escolher uma ID de utilizador única para as suas credenciais online e a palavra-passe online não deve conter a sua ID de utilizador única.

14.11.3 As palavras-passe online dos Clientes da BT devem ter um comprimento mínimo de 8 caracteres e conter pelo menos 1 carácter de 3 dos seguintes conjuntos; (i) número decimal (0-9), (ii) letra maiúscula (A-Z), (iii) letra minúscula (a-z) (iv) caracteres não alfanuméricos.

14.11.4 Para alterar uma palavra-passe online, o Cliente da BT deve fornecer a sua palavra-passe atual, seguida da dupla introdução da nova palavra-passe.

14.11.5 Quando um Cliente da BT se esquecer de uma ID de utilizador ou palavra-passe, o sistema fornecido pelo Fornecedor deve enviar uma mensagem para o endereço de e-mail registado do Cliente da BT que contenha a ID de utilizador ou uma ligação para o pedido de redefinição de palavra-passe após a introdução bem-sucedida da informação seguinte no formulário online:

14.11.5.1 MSISDN ou número de telefone fixo;

14.11.5.2 palavra-passe online;

14.11.5.3 ID de utilizador do Cliente da BT.

14.11.6 A ligação para o pedido de redefinição de palavra-passe deve ter uma validade limitada de 30 minutos, no máximo, antes de expirar e ter de ser efetuado um novo pedido de redefinição de palavra-passe online.

14.11.7 Após a redefinição bem-sucedida da palavra-passe, o Cliente da BT deve ser forçado a mudar para uma nova palavra-passe.

14.11.8 A recuperação das credenciais de utilizador de um Cliente da BT se este se esquecer tanto da ID de utilizador como da palavra-passe online, deve enviar uma mensagem para o endereço de e-mail registado, que contenha a ID de utilizador e uma ligação para o pedido de redefinição de palavra-passe, após introdução bem-sucedida do nome próprio e apelido, número de telefone e endereço de e-mail do Cliente da BT.

14.11.9 Podem ser requeridos níveis adicionais de autenticação de Clientes com base na sensibilidade dos dados e da funcionalidade a ser acedida.

15 FORNECEDOR QUE ALOJA INFORMAÇÕES DA BT

A conformidade com esta secção é necessária quando um Fornecedor aloja externamente informações da BT classificadas como "Confidenciais" ou "Estritamente confidenciais" num ambiente de nuvem ou num ambiente de servidores do próprio Fornecedor ou de Subcontratados.

15.1 O Fornecedor deve assegurar que, no que diz respeito aos Produtos, os ambientes onde as informações da BT estão alojadas se encontram em conformidade com os Requisitos de alojamento de dados em terceiros externos, disponível em:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 SEGURANÇA DE REDE

A conformidade com esta secção é necessária quando o Fornecedor constrói, desenvolve ou presta assistência a redes ou ativos de rede da BT.

16.1 O Fornecedor deve aplicar aos produtos as medidas de segurança acordadas transversalmente a todos os componentes fornecidos, de uma forma que salvaguarde a confidencialidade, disponibilidade e integridade das Redes da BT e/ou ativos 21CN. O Fornecedor deve fornecer à BT toda a documentação relativa à implementação da Segurança de rede relativamente aos Produtos, e deve garantir que:

16.1.1 cumpre e assegura que toda a Segurança de rede pela qual o Fornecedor é responsável atende a todos os requisitos legais e regulamentares; e

16.1.2 envida todos os esforços para evitar que indivíduos não autorizados (por ex.: piratas informáticos) tenham acesso a elementos de gestão da rede e outros elementos acedidos através das Redes da BT e/ou 21CN; e

16.1.3 envida todos os esforços para reduzir o risco de uso indevido das Redes da BT e/ou 21CN por indivíduos autorizados a aceder, que possam potencialmente causar a perda de receita ou serviço; e

16.1.4 envida todos os esforços para detetar quaisquer violações de segurança que possam ocorrer garantindo a rápida retificação de quaisquer violações, juntamente com o resultado e a identificação dos indivíduos que obtiveram acesso e a determinação de como o acesso foi obtido; e

16.1.5 minimiza o risco de erros de configuração de Redes da BT, por exemplo, concedendo as permissões mínimas necessárias para desempenhar a função contratada.

16.2 O Fornecedor deve tomar todas as medidas razoáveis para garantir a segurança de todas as interfaces dos Produtos e/ou Serviços e não deve presumir que os componentes fornecidos serão operados num ambiente seguro.

16.3 O Fornecedor deve fornecer ao Contacto de Segurança da BT os nomes, endereços (e quaisquer outros exigidos pela BT) de todo o Pessoal contratado individual que, periodicamente, esteja envolvido na implementação, manutenção e/ou gestão dos Produtos antes de estar envolvido respetivamente na referida implementação, manutenção e/ou gestão.

16.4 Relativamente às atividades de assistência prestadas no Reino Unido, o Fornecedor deve possuir uma equipa de segurança composta por, pelo menos, um cidadão do Reino Unido que estará disponível para fazer a ligação com o Contacto de Segurança da BT (ou indivíduos designados por ele) e a equipa deverá comparecer nas reuniões periódicas que o Contacto de Segurança da BT possa, razoavelmente, solicitar.

16.5 O Fornecedor deve fornecer ao Contacto de Segurança da BT um cronograma (periodicamente atualizado, conforme necessário) de todos os componentes ativos incluídos nos Produtos e/ou Serviços e a respetiva origem.

16.6 O Fornecedor deve fornecer detalhes dos seus funcionários individuais que mantenham contacto com a equipa de gestão de vulnerabilidades da BT (CERT) relativamente a discussões em torno das vulnerabilidades identificadas pela BT e pelo Fornecedor nos Produtos e/ou Serviços. O Fornecedor deve fornecer à BT informações oportunas sobre as vulnerabilidades e (a expensas do Fornecedor) cumprir os requisitos razoáveis em relação às vulnerabilidades conforme possa ser notificado periodicamente pelo Contacto de Segurança da BT. O Fornecedor deve informar a BT de quaisquer vulnerabilidades de forma suficientemente atempada para permitir a aplicação ou instalação de controlos para as mitigar, antes de o Fornecedor divulgar publicamente essas vulnerabilidades.

16.7 O Fornecedor deve permitir que o Contacto de Segurança da BT e indivíduos designados pelo mesmo acedam periodicamente, na totalidade e sem restrições, a qualquer local onde os Produtos sejam desenvolvidos, fabricados ou criados para realizar testes de conformidade de segurança e/ou avaliações, e o Fornecedor deve cooperar (e deve assegurar que todo o Pessoal contratado relevante coopera) em tais testes de conformidade de segurança.

16.8 O Fornecedor deve garantir que quaisquer componentes relacionados com a segurança compreendidos nos Produtos tal como são identificados pela e à BT sejam, periodicamente e a expensas do Fornecedor, avaliados externamente para satisfação razoável da BT.

16.9 Em relação a qualquer informação fornecida por ou obtida da BT assinalada como "**ESTRITAMENTE CONFIDENCIAL**" ou facilmente interpretada como sendo confidencial, o Fornecedor deve assegurar que:

16.9.1 o acesso é facultado apenas ao Pessoal contratado especificamente autorizado pela BT a visualizar e tratar tal informação e mantendo um registo dos referidos acessos;

16.9.2 a informação é manipulada, usada e armazenada com extremo cuidado e encriptada antes do armazenamento usando PGP ou WinZip 9, e em condições que ofereçam um elevado nível de resistência a quebra deliberada de segurança (isto é, usando o algoritmo de encriptação mais forte disponível/uma palavra-passe forte) e que torne extremamente provável a deteção de qualquer quebra de segurança efetiva ou tentada;

16.9.3 quando a informação é transmitida, a segurança adequada é aplicada, através de encriptação com Secure Email, PGP ou WinZip 9; e

16.9.4 a informação não é exportada, sem permissão por escrito da BT, para fora do Espaço Económico Europeu.

16.10 O Fornecedor deve imediatamente e em qualquer situação, no prazo de 7 dias úteis, fornecer ao Contacto de Segurança da BT todos os detalhes de quaisquer recursos e/ou funcionalidades incluídos em qualquer dos Produtos (ou previstos num plano de fornecimento de Produtos) de que, periodicamente:

16.10.1 o Fornecedor tenha conhecimento; ou

16.10.2 o Contacto de Segurança da BT razoavelmente acredite, e assim informe o Fornecedor, de que são concebidos para, ou poderiam ser usados para, interceção legal ou qualquer outra interceção de tráfego de telecomunicações. Tais detalhes devem incluir todas as informações razoavelmente necessárias para permitir ao Contacto de Segurança da BT compreender plenamente a natureza, a composição e a extensão de tais recursos e/ou funcionalidades.

16.11 A fim de manter o acesso aos sistemas e/ou Redes da BT, o Fornecedor deve comunicar de imediato à BT quaisquer alterações ao seu método de acesso através de firewalls, incluindo o fornecimento de tradução de endereços de rede.

16.12 O Fornecedor não deve usar quaisquer ferramentas de monitorização de rede que possam visualizar a informação da aplicação.

16.13 O Fornecedor deve garantir que a funcionalidade IPv6 incluída nos sistemas operativos é desativada nos anfitriões (por exemplo, dispositivos dos utilizadores finais ou servidores que se liguem à rede e aos domínios da BT devem ser desativados quando não forem necessários).

16.14 O Fornecedor deve garantir e assegurar que todos os Produtos e Serviços se encontram em conformidade com as políticas da BT, onde aplicável, e com os Requisitos de segurança. Qualquer não conformidade deve ser acordada na assinatura do Contrato ou através de um processo de controlo de alterações (ou equivalente).

16.15 O Fornecedor deverá garantir que se proceda a verificações de antecedentes pré-contratação apropriadas ao nível de acesso de todo o Pessoal contratado, conforme estipulado em https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Os Fornecedores que construam, desenvolvam ou prestem assistência às Redes e aos ativos de Rede da BT, devem assegurar que se procede no mínimo à verificação de antecedentes pré-contratação L2 de todo o Pessoal contratado. Será necessária verificação de antecedentes pré-contratação L3 no caso das funções identificadas pelo Contacto de Segurança da BT. Quando o Fornecedor não for capaz de efetuar diretamente as aprovações de segurança do Pessoal contratado como parte das verificações L3, a BT deve prestar auxílio na obtenção de aprovação, a expensas do Fornecedor.

16.16 O Fornecedor deve manter o hardware e software de acordo com as especificações dos fabricantes.

16.17 O Fornecedor não deve usar meios removíveis (discos externos, unidades de memória USB, etc.) para assistência e manutenção ou outros fins.

17 SEGURANÇA DE REDE DO FORNECEDOR

A conformidade com as cláusulas desta secção é necessária nos casos em que a rede do Fornecedor seja utilizada para fornecer os Produtos (inclui redes LAN, WAN, internet, redes sem fios e de rádio).

17.1 O Fornecedor deve aplicar aos produtos as medidas de segurança acordadas transversalmente a todas as suas redes, de uma forma que salvaguarde a confidencialidade, disponibilidade e integridade das informações da BT. As medidas e o Fornecedor devem:

17.1.1 cumprir todos os requisitos legais e regulamentares; e

17.1.2 envidar todos os esforços para evitar que indivíduos não autorizados (por ex., piratas informáticos) obtenham acesso à(s) rede(s) do Fornecedor;

17.1.3 envidar todos os esforços para reduzir o risco de uso indevido da(s) rede(s) do Fornecedor por indivíduos autorizados a aceder, que possam potencialmente causar a perda de receita ou serviço; e

17.1.4 envidar todos os esforços para detetar quaisquer Violações de segurança relevantes e garantir a rápida retificação de quaisquer violações, juntamente com o resultado e a identificação dos indivíduos que obtiveram acesso e a determinação de como o acesso foi obtido.

17.2 Devem estar implementadas as medidas adequadas para garantir a segurança dos componentes incluindo, sem se limitar:

17.2.1 utilização de princípios eficazes de "**defesa em profundidade**";

17.2.2 utilização de controlos implementados para evitar qualquer ataque intencional;

17.2.3 utilização de firewalls, routers, interruptores;

17.2.4 comunicações seguras entre dispositivos e estações de gestão;

17.2.5 comunicações seguras entre dispositivos conforme apropriado; incluindo a encriptação de todos os acessos de administrador não efetuados através da consola;

17.2.6 sólida conceção de arquitetura, escalonada e dividida em zonas com uma identidade de gestão robusta e uma configuração de sistema operativo eficazes, que devem ser devidamente reforçadas e documentadas;

17.2.7 a desativação (quando praticável) dos serviços, aplicações e portas não utilizados;

17.2.8 a desativação ou remoção de contas de convidado;

17.2.9 a instalação das mais recentes correções de segurança na(s) rede(s) e sistema(s) do Fornecedor, logo que praticável após os testes. Quaisquer exceções devem ser comunicadas à BT caso apresentem risco de acesso. A BT reserva o direito de forçar o Fornecedor a instalar correções na sequência da avaliação de riscos;

17.2.10 evitar relações de confiança entre servidores;

17.2.11 usar as melhores práticas do princípio de segurança do "**menor privilégio**" para executar uma função;

17.2.12 garantir que estão implementadas as medidas adequadas para lidar com ataques denial of service;

17.2.13 garantir que estão implementadas as medidas adequadas para deteção e/ou proteção contra intrusões;

17.2.14 monitorizar todos os vendedores aplicáveis e outras fontes de informação relevantes em busca de alertas de vulnerabilidade;

17.2.15 se for o caso, monitorizar a integridade dos ficheiros a fim de detetar quaisquer adições, modificações ou eliminações de ficheiros críticos do sistema ou de dados; e

17.2.16 alterar todas as palavras-passe predefinidas de vendedores antes de colocar os componentes de rede em funcionamento.

18 SEGURANÇA EM NUVEM

A conformidade com as cláusulas desta secção é necessária quando o Fornecedor presta serviços de nuvem à BT.

18.1 O Fornecedor deverá respeitar:

a mais recente versão do Cloud Security Alliance Cloud Controls Matrix (CCM); os Requisitos de segurança para alojamento externo da BT, disponíveis em: https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm Os acordos de nível de serviço de infraestrutura e rede (internos e terceirizados) devem documentar claramente os controlos de segurança documental e os níveis de serviço, além dos requisitos comerciais e do Cliente.

18.2 O Fornecedor deve aplicar as medidas de segurança acordadas transversalmente a todos os componentes fornecidos, de uma forma que salvaguarde a confidencialidade, disponibilidade e integridade dos Produtos, minimizando as oportunidades de indivíduos não autorizados (por ex.: outros Clientes da nuvem) obterem acesso às informações e aos Produtos da BT.

19 CENTRO DE CONTACTO

A conformidade com as cláusulas desta secção é necessária quando o Fornecedor fornece um centro de contacto à BT.

19.1 O Fornecedor deve, em relação aos Produtos, assegurar que os ambientes onde as informações da BT são armazenadas, processadas ou visualizadas se encontram em conformidade com a versão mais atual da Norma sobre centros de contacto de terceiros:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

PARTE 5: DEFINIÇÕES

A estes Requisitos de segurança são aplicáveis as definições que se seguem, caso contrário, serão aplicáveis a estes Requisitos de segurança os termos do Contrato, e todas as palavras e expressões usadas nestes Requisitos de segurança terão o significado que lhes for atribuído no Contrato:

"**Acesso**" — o processamento, tratamento ou armazenamento de informações da BT com base num ou mais dos seguintes métodos:

- interligação com Sistemas da BT;
- fornecidos em papel ou em formato não eletrónico;
- informações da BT em Sistemas do Fornecedor;

- por dados móveis;

e/ou acesso às instalações da BT para o fornecimento dos Produtos (excluindo a entrega de hardware e a comparência a reuniões).

"**Autorizado**" — a BT aprovou o acesso como parte do processo de interligação com o sistema da BT ou foi recebida autorização escrita do contacto da BT Security; "**autorização**" deverá ser interpretado em conformidade. O nível de acesso fornecido será relevante e limitado ao necessário para fornecer os Produtos.

"**Sistemas administrativos da BT**" — refere-se à plataforma de faturação da BT (atualmente iSupplier), ou outros sistemas conforme acordado com a BT, que são puramente administrativos;

"**Cliente da BT**" — inclui para os fins destes Requisitos de segurança, uma empresa ou indivíduo a quem a BT fornece bens ou serviços.

"**Informações da BT**" — todas as informações relacionadas com a BT ou um Cliente da BT facultadas ao Fornecedor e todas as informações processadas ou manipuladas pelo Fornecedor em nome da BT ou de um Cliente da BT no âmbito do Contrato.

"**Redes da BT**" — a rede controlada e administrada pela BT.

"**Ativos físicos da BT**" — todos os ativos físicos (incluindo, sem se limitar, routers, interruptores, chaves de servidores para armários, tokens de computadores portáteis, passes, planos ou documentação) detidos pelo Fornecedor que pertençam à BT.

"**Segurança da BT**" — a organização de segurança no seio da BT.

"**Contacto de Segurança da BT**" — o profissional de garantia de segurança afeto à Segurança da BT ou ao Contacto comercial da BT se transmitido ao Fornecedor ou à Segurança central 0800 321999 [+44 1908 641100] que constituirá o único ponto de contacto para assuntos relacionados com os presentes Requisitos de segurança e qualquer Incidente de segurança relevante.

"**Sistemas da BT**" — os serviços e os componentes de serviços, produtos, redes, servidores, processos, sistemas com base em papel ou informáticos que possam estar alojados nas instalações da BT, incluindo o iSupplier (conforme definido na Condição intitulada "**Pagamento e faturação**").

"**Registos em massa**" — refere-se a mais de 1000 registos individuais das Informações da BT classificados como Confidenciais ou 100 registos individuais das informações da BT classificados como Estritamente confidenciais.

"**CCTV**" — circuito fechado de televisão.

"**Pessoal contratado**", "**Pessoal contratado relevante**" — conforme definido no Contrato.

"**Cyber Essentials Plus**" — refere-se a um esquema com o apoio do Governo do Reino Unido para ajudar as organizações a proteger-se contra ciberataques comuns atualmente disponível em https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

"**Boas práticas de segurança da indústria**" — refere-se, em relação a quaisquer empreendimentos e circunstâncias, à implementação das práticas, políticas, normas e ferramentas de segurança que seriam normal e razoavelmente esperadas de uma pessoa experiente e competente que exerça o mesmo tipo de atividade em circunstâncias idênticas ou semelhantes.

"**Informação**" — informação tangível ou de qualquer outra forma, incluindo, sem se limitar, especificações, relatórios, dados, notas, documentação, desenhos, software, saídas do computador, conceções, esquemas de circuitos, modelos, padrões, amostras, invenções (quer passíveis de patente quer não) e know-how, bem como os meios (se aplicável) nos quais tal informação é fornecida.

"**Interna**", "**Pública**", "**Confidencial**" e "**Estritamente confidencial**" — têm todos o significado que lhes é atribuído na Especificação de classificação e tratamento de informações de terceiros.

"**ISO 27001**" — a versão atual da norma internacional para os sistemas de gestão de segurança internacional definida pela Organização Internacional de Normalização e pela Comissão Eletrotécnica Internacional.

"**Ativos de rede**" — dispositivo ou outro componente da rede BT que suporta as atividades de rede relacionadas.

"**Segurança de rede**" — a segurança dos caminhos e nós de comunicação interligados que ligam logicamente as tecnologias do utilizador final e os sistemas de gestão associados.

"**Processo**", "**Processado**" ou "**Processamento**", "**Anexo sobre processamento**" e "**Dados pessoais**" — terão o significado que lhes é atribuído na Condição intitulada "**Proteção de dados pessoais**".

"**Incidente de segurança relevante**" — uma falha de segurança observada ou suspeita de falha de segurança nos sistemas ou serviços, e eventos de segurança que afetem os Produtos ou o desempenho do Contrato (incluindo, de forma efetiva ou suspeita de perda, danos, roubo ou uso indevido de Informações da BT ou dos Sistemas da BT), incluindo, sem se limitar:

- perda de serviço, equipamentos ou instalações;
- corrupção, danos ou uso indevido de ativos físicos da BT;
- avarias ou sobrecargas do sistema;
- erros humanos;

- não conformidades com os Requisitos de segurança descritos neste documento;
- violações das disposições de segurança física;
- alterações não controladas ao sistema;
- falhas de software ou hardware;
- violações de acesso; e
- perdas conhecidas ou suspeita de perdas relacionadas com os sistemas associados com a BT e ligação(ões) entre a BT e o Fornecedor.

"**Acesso remoto**" — acesso remoto a partir de casa ou de outro local através da rede pública (por ex., Internet) ou acesso remoto da Rede do Fornecedor a um Sistema da BT.
"**Requisitos de segurança**" — refere-se aos presentes Requisitos de segurança da BT conforme devidamente atualizados periodicamente.
"**Produtos**" — refere-se a todos e quaisquer "**Serviços**", "**Produtos**", "**Bens**" e "**Trabalho**" definidos no Contrato e a qualquer desempenho contratual.
"**Sistemas do Fornecedor**" — qualquer computador, aplicação ou sistemas de rede propriedade do Fornecedor usado para aceder, armazenar ou processar as Informações da BT ou envolvidos no fornecimento dos Produtos.
"**Contacto de segurança do Fornecedor**" — a pessoa cuja informação de contacto será transmitida pelo Fornecedor à BT, periodicamente, e que constituirá o único ponto de contacto para questões relacionadas com os presentes Requisitos de segurança e qualquer Incidente de segurança relevante.
"**Transferência**" ou "**Transferido**" — a movimentação das informações na posse do Pessoal contratado (incluindo, sem se limitar, Dados pessoais) de um local ou pessoa para outro, quer por meios físicos, de voz ou eletrónicos; e a concessão de acesso às Informações de BT na posse do Pessoal contratado (incluindo, sem se limitar, Dados pessoais) de um local ou pessoa para outro, quer por meios físicos, de voz ou eletrónicos.
"**Especificação de classificação e tratamento de informações de terceiros**" refere-se aos requisitos sobre a manipulação das informações por parte do Fornecedor conforme estipulado em https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm e periodicamente atualizado.