Índice

1. Introdução

1.1 Os clientes da BT esperam que a BT e a sua cadeia de fornecimento de Terceiros forneçam os seus serviços utilizando Sistemas de Gestão de Segurança da Informação (SGSI) padrão da indústria. Os seus SGSI deverão abranger infraestruturas, redes, equipamentos e sistemas de TI para proteger os serviços prestados e as informações da BT/dos clientes da BT no âmbito dos serviços. Este documento define a política de Requisitos de Segurança da BT e abrange todos os terceiros que trabalham por conta ou em nome do Grupo BT, entre os quais a Openreach, a EE e a Plusnet, doravante designados "BT" no restante do documento. O Terceiro será informado sobre quais conjuntos de controle de segurança são relevantes para o serviço fornecido à BT.

1.2 Estes Requisitos de Segurança são adicionais e sem prejuízo de quaisquer outras obrigações do Terceiro no Contrato. Eles são projetados para garantir que a BT mantenha o controle e a supervisão de sua rede e dos dados do usuário.

2. Requisitos de Acesso Limitado

2.1 Sem prejuízo de quaisquer obrigações de confidencialidade que possa ter, nos casos em que o Funcionário Terceirizado tenha Acesso às Informações da BT, o Terceirizado deverá:

2.2 Garantir que as informações da BT não sejam divulgadas ou acessadas por Funcionários Terceirizados, a menos que necessário para a prestação do Serviço; e

2.3 Estabelecer todos os sistemas e processos, tanto técnicos quanto organizacionais, necessários para proteger as Informações da BT (i) contra destruição acidental ou ilegal e (ii) perda, alteração, divulgação não autorizada ou Acesso às Informações da BT de acordo com as Boas Práticas de Segurança da Indústria.

3. Segurança Geral da Informação

3.1 Mediante solicitação adequada, o Terceiro deverá disponibilizar à BT cópias de certificações de segurança e declarações de conformidade relevantes para o Serviço, a fim de ilustrar evidências de conformidade com tais Requisitos de Segurança.

3.2 Caso haja uma mudança significativa nas normas de segurança da tecnologia ou da indústria; ou se houver alterações relevantes nos Serviços ou na forma como são fornecidos, a BT poderá realizar uma retificação do Contrato durante a vigência, se houver necessidade de uma alteração nos parâmetros de controle de segurança aplicáveis. O Terceiro deverá respeitar a alteração do Contrato acordada dentro de um prazo aceitável, com base na natureza da mudança e no risco para a BT.

3.3 Em caso de alterações significativas nos Serviços ou na forma como eles são prestados, o Terceiro deverá revisar a presente política de Requisitos de Segurança para garantir que ainda estão em conformidade com todos os controles de segurança aplicáveis.

3.4 Se o Terceiro subcontratar obrigações nos termos do Contrato, o Terceiro garantirá que todos os Contratos com os Subcontratados relevantes e os seus Subcontratados incluem termos por escrito exigindo que o Subcontratado respeite as partes aplicáveis de tais Requisitos de Segurança ou requisitos de segurança equivalentes do Terceiro.

3.5 Se uma quarta parte for usada para fornecer o serviço, sempre que esta mantiver ou tratar Informações da BT, o Terceiro deverá obter o consentimento da Parte Interessada da BT sobre quais informações poderão ser compartilhadas. O Terceiro deverá garantir que tem uma relação contratual com a quarta parte e deverá garantir que a quarta parte opera uma estrutura de segurança padrão do setor.

3.6 As Informações da BT poderão ser retidas durante o tempo necessário para a execução do Contrato, após o qual deverão ser retidas por um máximo de dois anos, a menos que tenha sido acordado um período de retenção diferente entre a BT e o Terceiro ou qualquer lei aplicável tenha uma exigência diferente.

3.7 Se os Serviços prestarem suporte direto a um Contrato do Governo do Reino Unido, o Terceiro deverá estar em conformidade com a versão mais atual do Cyber Essentials Plus - https://www.cyberessentials.ncsc.gov.uk/.

3.8 Nos casos em que as informações da BT forem processadas ou armazenadas no exterior, os terceiros devem informar a BT sobre as localizações geográficas; a BT se reserva o direito de descartar locais considerados de alto risco.

Manuseio de Informações da BT

3.9 Salvo indicação em contrário da parte interessada da BT, todas as Informações da BT são classificadas como "Confidenciais". Sempre que dados pessoais ou dados pessoais confidenciais façam parte do âmbito, deverá ser solicitado o parecer da Equipa de Proteção de Dados e Privacidade do Terceiro, caso sejam necessários controles adicionais.

De acordo com os controles de segurança a seguir, os “requisitos de processamento de voz” possuem um âmbito limitado às comunicações verbais.

3.10 Caso seja necessário analisar, mostrar ou compartilhar informações sobre a BT através de uma plataforma de colaboração (por exemplo, o Teams).

- Certifique-se de que apenas os indivíduos que têm necessidade de acessar as informações estejam presentes.
- Caso haja um prestador de serviços terceirizado envolvido, ele deverá formalizar um contrato assinado com o Terceiro ou ter um Acordo de Confidencialidade (NDA) vigente antes do início das tratativas.
- O Terceiro deverá verificar quem está presente na conferência antes de iniciar.

3.11 Caso haja necessidade de discutir Informações da BT com alguém presencialmente, por telefone celular ou através de um telefone fixo convencional.

- As conversas não poderão ocorrer com ou ser ouvidas por alguém que não tenha necessidade de ter acesso a essas informações.
- Caso seja necessário estabelecer uma conversa com um prestador de serviços externo, será necessário que o terceirizado tenha um contrato assinado ou um Acordo de Confidencialidade (NDA) em vigor antes do início das tratativas.
- Informações confidenciais ou altamente confidenciais não devem ser armazenadas em serviços de correio de voz.

Os controles de segurança a seguir são "requisitos de processamento por escrito" e abrangem material mantido em papel. Tal material inclui, mas não se limita a, documentos redigidas à mão, atas, anotações e comunicações oficiais internas. Também inclui material eletrônico impresso, como documentos profissionais e relatórios, uma vez que se encontrem em papel.

3.12 Ao armazenar cópias em papel sobre as Informações da BT nas dependências de Terceiros, caso não estejam em uso, todo o material deve ser protegido em um local que seja possível trancar, de acesso restrito apenas às pessoas que necessitam consultar o material. Os documentos não poderão ser mantidos sem supervisão.

3.13 Caso haja necessidade de realizar impressões, fotocópias ou reimpressões de Informações da BT, os seguintes controles de segurança deverão ser adotados:

- Utilize somente os dispositivos de impressão ou cópia existentes nas próprias instalações do Terceiro.
- As fotocópias ou impressões não poderão ser mantidas sem supervisão no local de impressão e terão que ser recolhidas após serem processadas.
- Caso o equipamento de impressão ou fotocópia tenha capacidade de memória, que permita recuperar e reimprimir o material copiado, ele deverá ser reiniciado imediatamente para a limpeza da memória.

3.14 Caso haja necessidade de retirar cópias das Informações da BT das instalações de Terceiros:

- A menos que já tenha sido acordado como parte do âmbito do trabalho, o Terceiro precisará obter o consentimento comprovado da parte interessada da BT.
- Caso sejam aprovadas, as informações não poderão ser identificáveis durante o transporte e terão de ser mantidas em uma pasta, mala ou em uma caixa comum com dados anonimizados.
- O material não poderá ser mantido sem supervisão e terá de permanecer sob o controle direto do responsável pelo transporte, especialmente nos transportes públicos.

3.15 Caso não sejam mais necessárias, as cópias impressas das Informações da BT precisarão ser descartadas da seguinte forma:

- As cópias em papel não poderão ser descartadas nas lixeiras de resíduo comum.
- Caso utilize um triturador de papel, ele precisará ter no mínimo o padrão P4, conforme a norma DIN66399.
- Caso não existam trituradores de papel aprovados, as informações precisarão ser descartadas em lixeiras de resíduos seguras.

Para "Informações Altamente Confidenciais", as seguintes medidas adicionais precisarão ser cumpridas:

- As informações só poderão ser descartadas em lixeiras de resíduos seguras após o processo de trituração.
- As informações que precisam ser destruídas no local pelo fornecedor terão de receber um certificado que ateste que o fornecedor realizou o processo de destruição.

Os seguintes controles de segurança estão relacionados com as Informações da BT em formato eletrônico.

3.16 Ao armazenar Informações da BT em um computador ou laptop de Terceiros, os seguintes controles estão estabelecidos:

- Só é permitido em dispositivos com criptografia de disco rígido (por exemplo, Bitlocker).
- Todos os documentos precisam estar criptografados individualmente.
- O Gerenciamento de Direitos de Informação (IRM) precisa estar integrado ao documento.
- Se fornecidas, as informações precisarão conter a etiqueta de classificação da BT.

3.17 Ao salvar um documento da BT em um local interno de compartilhamento de arquivos para armazenamento geral, colaboração ou compartilhamento de arquivos, os seguintes controles de segurança serão necessários:

- O local em que o material está sendo armazenado precisará ter permissões de acesso definidas para permitir que somente os usuários necessários possam consultar ou usar o documento.
- Se fornecidas, as informações precisarão conter a etiqueta de classificação da BT.
- Todos os documentos precisam ser criptografados individualmente.
- O Gerenciamento de Direitos de Informação (IRM) precisa estar integrado ao documento.
- Caso esteja no âmbito do serviço a ser fornecido, o material referente ao PCI e aos Cartões de Pagamento não poderão ser salvos em sites específicos de armazenamento de arquivos em nenhum momento.
- Caso seja necessário que as contas para convidados forneçam acesso a um prestador de serviços externo, elas precisarão dispor de um contrato assinado com o Terceiro ou de um Acordo de Confidencialidade (NDA) antes da concessão do acesso.

3.18 Caso seja necessário salvar Informações da BT em mídia removível de Terceiros (por exemplo, um cartão de memória USB), os seguintes controles de segurança serão adotados:

- O dispositivo deve ser criptografado ao mesmo nível que o disco rígido.
- Em caso de perda ou furto, o Terceiro precisará registrar uma ocorrência relacionada à segurança.
- O Terceiro precisará apresentar provas de autorização prévia da Parte Interessada da BT para transferir material “altamente confidencial” para mídia removível.
- Se estiver no âmbito do serviço, o material PCI ou os dados pessoais não poderão ser armazenados em mídia removível.
- Os dispositivos destinados a suporte e manutenção não devem ser utilizados para nenhuma outra finalidade.

3.19 As Informações da BT não poderão ser armazenadas em computadores pessoais, laptops, mídias removíveis ou dispositivos móveis.

3.20 As Informações da BT não poderão ser enviadas ou encaminhadas automaticamente de um endereço de e-mail corporativo de Terceiros para um e-mail pessoal ou uma

conta de e-mail externa, a menos que seja um contratado externo que possua um contrato assinado com Terceiros ou um Acordo de Confidencialidade (NDA) em vigor e seja usado para fornecer o serviço.

3.21 Para reduzir ao mínimo a possibilidade de ataques cibernéticos e as chances para que os invasores consigam manipular o comportamento humano por meio de sua interação com navegadores da Web e sistemas de e-mail, é necessário implementar procedimentos para garantir que apenas navegadores da Web e clientes de e-mail totalmente compatíveis sejam permitidos e desinstalar ou desativar quaisquer plug-ins ou aplicativos complementares não autorizados de navegadores ou clientes de e-mail.

3.22 O Terceiro terá que dispor de medidas de back-up para restaurar as Informações da BT dentro de 3 dias úteis, na eventualidade de corrompimento, perda ou degradação.

3.23 Ao descartar dados/Informações da BT, é necessário manter registros completos sobre a retenção e o descarte de dados que forneçam trilha de auditoria, evidências e rastreamento. Isto precisará incluir:

- Evidência de destruição e/ou descarte (incluindo data de realização e método utilizado).
- Registros de auditoria do sistema para exclusão.
- Certificações sobre o descarte de dados.
- Quem realizou o descarte (inclusive eventuais parceiros/terceiros ou contratados que realizaram o descarte).
- É necessário emitir um relatório sobre a destruição e a verificação para confirmar o êxito ou o insucesso de qualquer processo relacionado à destruição/exclusão (ou seja, para que um processo de substituição ocorra, é necessário fornecer um relatório que detalhe todos os setores que não puderam ser deletados).

3.24 Ao descartar equipamentos com dados/informações da BT, será necessário fornecer uma trilha de auditoria para os seguintes tipos de equipamentos:

- Mídia removível.
- Unidades de disco.
- Fitas de backup.
- Componentes computacionais.

3.25 É necessário haver registros completos para fornecer uma trilha de auditoria que inclua, pelo menos:

- O nome do aplicativo ou serviço que utilizou esse equipamento.
- Tipo de equipamento, por exemplo, desktop, laptop, servidor, fita, roteador, etc.
- Quantidade de discos rígidos que o equipamento contém (se aplicável).
- Equipamento identificado pelo número de série.
- Partes integrantes do equipamento identificadas por número de série.
- Rastreamento completo de ativos de todos os equipamentos e peças de componentes durante todo o ciclo de vida do descarte do equipamento.
- Evidência de destruição e/ou descarte (incluindo data de realização e método utilizado).

- Detalhes de quem realizou o descarte (inclusive quaisquer parceiros de descarte/terceiros/empreiteiros de descarte de resíduos).
- É necessário elaborar um relatório que comprove o êxito ou o insucesso de qualquer processo de reciclagem/sanitização ou destruição. Por exemplo, para que um processo de substituição seja realizado, é necessário fornecer um relatório que detalhe todos os setores que não puderam ser deletados. Estes relatórios devem incluir a capacidade, a marca, o modelo e o número de série da mídia.

Funções e Responsabilidades

3.26 Cada Terceiro precisará ter conhecimento e compreender os requisitos relacionados a esses controles de segurança e será responsável por garantir que todos os indivíduos que estão envolvidos no fornecimento de um serviço para a BT estejam familiarizados e cumpram os requisitos relevantes da presente norma.

Governança

3.27 O Terceiro precisará dispor de uma estrutura de segurança padrão estabelecida e consistente para a governança de segurança cibernética e de informações, que abranja os seguintes componentes:

- Políticas e procedimentos apropriados de segurança da informação e cibernética que sejam aprovados e comunicados.
- Uma estratégia de segurança da informação.
- Requisitos legais e regulamentares relevantes relativos à segurança das Informações e da Cibersegurança (inclusive privacidade) que são compreendidos e gerenciados.
- Processos de Governança e gerenciamento de riscos que abordem os riscos de segurança cibernética e de informações.

3.28 O Terceiro precisará garantir que as funções e responsabilidades apropriadas para a Segurança das Informações e da Cibersegurança sejam definidas e implementadas, o que abrange o seguinte:

- Um Responsável pela Segurança da Informação (ou equivalente) em tempo integral, que seja devidamente qualificado como sênior e que seja responsável pelo programa de segurança da informação.
- Um grupo de trabalho altamente qualificado, comitê ou órgão equivalente que coordene as atividades de segurança da informação em toda a empresa do Terceiro, sob a responsabilidade de um funcionário sênior e que realize reuniões regularmente.
- Uma função de segurança da informação especializada com funções e responsabilidades adequadas e definidas.

3.29 O Terceiro precisará garantir que exista uma responsabilidade individual pelas informações e sistemas, além de assegurar que haja uma propriedade adequada dos ambientes, informações e sistemas críticos de negócios e que tal propriedade seja atribuída a indivíduos capacitados.

3.30 O Terceiro precisará garantir que a BT seja notificada (por escrito), conforme a lei, caso o Terceiro esteja sujeito a uma fusão, aquisição ou qualquer outra mudança de propriedade.

Gerenciamento de Incidentes

3.31 O Terceiro precisará dispor de uma estrutura de gerenciamento de incidentes estabelecida e consistente para garantir que os incidentes sejam adequadamente gerenciados, contidos e mitigados, além de abranger os seguintes componentes:

- Garantir que os funcionários compreendam suas funções e a ordem das operações quando for necessária uma resposta.
- Garantir que os incidentes sejam relatados de acordo com os critérios estabelecidos.
- Garantir que o impacto do incidente seja compreendido.
- Garantir que a perícia seja realizada, quando necessário, internamente ou por um especialista.
- Garantir que as conclusões obtidas com os incidentes sejam incorporadas às práticas recomendadas.
- Garantir que as informações relacionadas a um incidente que afete a BT sejam tratadas como “Confidenciais”.

3.32 O Terceiro tomará todas as medidas cabíveis para garantir que o(s) indivíduo(s) designado(s) e responsável(is) como Ponto de Contato para o risco de segurança, gestão de incidentes e gestão de conformidade. O Terceiro notificará as Partes Interessadas da BT sobre os detalhes de contato do(s) indivíduo(s) e quaisquer alterações realizadas.

3.33 O Terceiro informará a BT através do e-mail security@bt.com ou pelo telefone 0800 321 999, dentro de um prazo aceitável ao tomar conhecimento de qualquer incidente que afete o serviço da BT ou das Informações da BT e, em qualquer caso, no prazo máximo de 24 (vinte e quatro) horas a partir do momento em que o Terceiro tenha conhecimento do Incidente.

3.34 O Terceiro, sem atrasos injustificados, tomará medidas corretivas apropriadas e oportunas para mitigar quaisquer riscos e efeitos relacionados ao incidente, para reduzir a sua gravidade e duração.

3.35 O Terceiro fornecerá, no prazo de 30 dias após um incidente, um relatório às Partes Interessadas da BT, em relação a qualquer incidente que afete o serviço da BT ou das Informações da BT, que deverá incluir, no mínimo:

data e hora, local, tipo de incidente, impacto, status e resultado (inclusive as recomendações de resolução ou ações tomadas).

3.36 O Terceiro precisará realizar uma análise da causa principal de todos os incidentes relacionados à segurança. Os resultados de tal análise devem ser encaminhados para os responsáveis competentes dentro da organização do Terceiro.

Gerenciamento de Mudanças

3.37 O Terceiro precisará garantir que todas as mudanças realizadas no setor de TI sejam aprovadas, registradas e testadas, o que inclui a reversão de alterações malsucedidas, antes da implementação, para evitar interrupções no serviço ou violações de segurança, além de haver um processo para realizar atualizações de emergência de forma adequada.

3.38 O Terceiro precisará garantir que as mudanças sejam aplicadas nos ambientes de Produção e de Recuperação de Desastres (DR).

3.39 O Terceiro precisará garantir que a manutenção e o reparo dos ativos da organização sejam realizados e registrados com ferramentas aprovadas e controladas.

3.40 O Terceiro precisará garantir que a manutenção remota dos ativos da organização seja aprovada, registrada e realizada de forma que o acesso não autorizado seja evitado.

Gerenciamento de Riscos e Ameaças Cibernéticas

3.41 O Terceiro precisará garantir que existe uma estrutura contínua de avaliação de riscos e ameaças relacionadas à Cibersegurança para garantir que o perfil de risco da Cibersegurança para as operações, os ativos, as instalações e os indivíduos da organização seja compreendido e gerenciado por meio de:

- Avaliação das vulnerabilidades dos ativos.
- Identificação de ameaças internas e externas.
- Análise de dados/ informações confidenciais abrangidos.
- Avaliação dos possíveis impactos nos negócios.
- Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar os riscos.
- Garantir que a estrutura de gerenciamento de riscos e ameaças cibernéticas seja acordada em um nível adequado na organização.

3.42 O Terceiro precisará garantir que todos os riscos e ameaças identificados como parte da avaliação de riscos e ameaças à Cibersegurança sejam priorizados e que ações sejam tomadas para minimizar os riscos dentro de um período de tempo apropriado.

3.43 O Terceiro precisará notificar as Partes Interessadas da BT caso não consiga remediar ou reduzir as áreas de risco relevantes que possam afetar o serviço prestado.

Gerenciamento de Identidade e Controle de Acesso

3.44 O Terceiro precisará estabelecer uma estrutura consistente para garantir que as identidades e credenciais sejam gerenciadas com segurança por funcionários autorizados:

- Conceder, reativar, alterar e desativar apenas os direitos de acesso com base em aprovações documentadas e autorizadas.
- Garantir que as contas inativas sejam desativadas.
- Desativar contas de profissionais que não fazem mais parte do quadro de funcionários.

- Implementar processos e ferramentas para rastrear, controlar, prevenir e corrigir o uso, a atribuição e a configuração de privilégios administrativos em computadores, redes e aplicativos.
- Realizar revisões periódicas do acesso para garantir que o acesso seja adequado ao propósito.
- O acesso às contas de usuários é recertificado pelo menos uma vez por ano e o acesso às contas privilegiadas é recertificado trimestralmente.
- Garantir que as credenciais e os sigilos permanentes (por exemplo, acesso de emergência por parte de pessoas sem direitos de acesso) estejam protegidos em um local de armazenamento protegido por hardware e só sejam disponibilizados para a(s) pessoa(s) responsável(is) em caso de emergência.
- Garantir que as credenciais temporárias (por exemplo, autenticação de nome de usuário e senha) sejam armazenadas em um serviço centralizado com controle de acesso adequado baseado em funções, que deverá ser atualizado de acordo com quaisquer alterações relevantes nas funções e responsabilidades dentro da organização.

3.45 O armazenamento central de credenciais permanentes deverá ser protegido através da utilização das ferramentas de hardware. Por exemplo, em um host físico, a unidade pode ser criptografada com o uso de um TPM (Trusted Platform Module). Caso uma máquina virtual (VM) seja usada para fornecer um serviço de armazenamento central, essa VM e os dados nela incluídos também deverão ser criptografados, usar inicialização segura e ser configurados para garantir que só possam ser inicializados em um ambiente apropriado. O Terceiro precisará garantir que o acesso remoto seja gerenciado de modo que somente funcionários autorizados possam se conectar remotamente aos sistemas do Terceiro, de modo que as conexões sejam seguras e evitem o vazamento de dados e que o controle de acesso apropriado esteja em vigor, por exemplo, a autenticação multifator.

A autenticação de dois fatores deverá ser obtida com um ID de usuário, uma senha e um dos seguintes métodos:

- Um gerador de senha de uso exclusivo: que requer um PIN/senha específico do usuário para visualizar a senha de uso exclusivo.
- Um cartão inteligente equipado com um chip compatível com a norma ISO 7816 e um leitor de cartão associado com o respectivo software. Cartões inteligentes sem contato não são permitidos.
- Autenticação baseada em certificados emitida de acordo com a política de certificados Infosec de Terceiros.

A fim de evitar dúvidas, caso o acesso privilegiado ao suporte seja fornecido por meio de acesso remoto, tal acesso precisará ser feito por meio de uma conexão segura e do uso de autenticação de dois fatores.

3.46 O Terceiro precisará garantir que as permissões e autorizações de acesso a todos os sistemas (inclusive ferramentas, aplicativos, bancos de dados, sistemas operacionais, hardware, etc.) sejam gerenciadas conforme os princípios de menor privilégio e separação de tarefas.

3.47 O Terceiro precisará garantir que cada transação possa ser atribuída a um indivíduo identificável exclusivo e, se houver credenciais compartilhadas, que existam controles de compensação adequados (inclusive procedimentos de quebra de sigilo). Credenciais compartilhadas para acesso privilegiado não são permitidas.

3.48 O Terceiro precisará garantir que toda autenticação seja gerenciada de acordo com o risco da transação, ou seja, comprimento e complexidade adequados da senha, frequência de alterações de senhas, autenticação multifator, gerenciamento seguro de credenciais de senha ou demais formas de controle. O acesso privilegiado precisará ser feito através de contas protegidas comautenticação multifator. As contas de usuário com acesso prioritário precisarão dispor de credenciais fortes e exclusivas para cada ponto de acesso do equipamento de rede.

3.49 É necessário haver controles adequados para lidar com autenticações malsucedidas, o que inclui notificações na tela, registro de falhas e bloqueio do usuário.

3.50 Os processos e controles precisarão estar em vigor para gerenciar e autorizar contas de convidados e de serviço.

Classificação e Proteção de Dados

3.51 O Terceiro precisará dispor de uma estrutura/esquema estabelecido e consistente de classificação, identificação e manuseio de informações (alinhado com as Boas Práticas da Indústria/requisitos da BT) que contenha os seguintes componentes:

- Diretrizes sobre o manuseio de informações.
- As informações são protegidas de acordo com seu nível de classificação atribuído.
- Garantir que toda a equipe esteja ciente de que as Informações da BT não devem ser usadas para nenhum outro fim que não seja aquele para o qual foram fornecidas.

Prevenção de Vazamento de Dados

3.52 O Terceiro precisará dispor de uma estrutura estabelecida e consistente para garantir a proteção contra o vazamento inadequado de dados, a fim de garantir que a proteção inclua (mas não se limite a) as seguintes categorias:

- E-mail, Internet/Web gateway (inclusive armazenamento on-line e webmail), USB, fibra óptica e outras formas de portas/armazenamento portátil, etc., computação móvel e BYOD, serviços de acesso remoto, mecanismos de compartilhamento de arquivos e mídia social.
- Os dispositivos não autorizados não poderão ser conectados à rede (seja a rede corporativa do fornecedor ou os sistemas/rede da BT) ou usados para acessar informações não públicas.

Gerenciamento de Vulnerabilidades.

3.53 O Terceiro precisará ter uma estrutura de gerenciamento de vulnerabilidade estabelecida e consistente que inclua os seguintes componentes:

- Processos de políticas e procedimentos.
- Funções e responsabilidades definidas.

- Ferramentas apropriadas, como Sistemas de Detecção de Invasão e sistemas de varredura de vulnerabilidades.

3.54 A estrutura de gerenciamento de vulnerabilidades do Terceiro precisará garantir que os seguintes itens sejam monitorados constantemente para detectar possíveis eventos de cibersegurança:

- Principais sistemas e ativos.
- Acessos não autorizados.
- Software/aplicativos não autorizados.
- Atividade de rede.

3.55 A estrutura de gerenciamento de vulnerabilidades do Terceiro precisará garantir que:

- Existem processos estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas à organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou analistas de segurança).
- Apenas ferramentas, tecnologias e usuários autorizados são permitidos.
- As vulnerabilidades identificadas são atenuadas ou documentadas como riscos aceitos.

Registro e Monitoramento Contínuos de Segurança.

3.56 O Terceiro precisará garantir que haja uma estrutura estabelecida e consistente de auditoria e gerenciamento de registros que assegure que os principais sistemas, entre eles os aplicativos, sejam configurados para registrar os principais eventos (inclusive os de acesso prioritário e atividade de funcionários) com a retenção desses registros por um período mínimo de 13 meses. Os registros de equipamentos de rede em Funções Críticas de Segurança precisarão ser totalmente registrados e disponibilizados para auditoria por 13 meses.

O Terceiro precisará garantir, basicamente, que os registros contemplem os seguintes eventos:

- Inicialização e desligamento do sistema.
- Autenticação bem-sucedida e malsucedida.
- Acesso e saída do sistema.
- Criação, modificação e exclusão de contas.
- Alteração de credenciais.
- Escalonamento de prioridades.
- Bloqueio de conta.
- Anexos e remoções de hardware.
- Alertas de gerenciamento de sistema e rede e mensagens de erro.
- Alterações de administração de eventos relacionados à segurança, o que inclui gerenciamento de grupos e alterações na política de segurança.
- Pontos de início e parada do processo registrado.
- Eventos de ativação ou desativação do registro.

- Alterações no tipo de eventos registrados conforme exigido pela trilha de auditoria (por exemplo, os parâmetros de inicialização e quaisquer alterações realizadas neles).
- Alteração (ou tentativa de alteração) do registro.
- Qualquer forma de acesso ao plano de gerenciamento de sistemas usados em relação a uma rede ou serviço público de comunicações eletrônicas do Reino Unido.

O Terceiro precisará garantir, basicamente, que os seguintes parâmetros de registro sejam obtidos para cada evento:

- Identificação do ativo ao qual o evento se refere.
- Tipo de evento.
- Data e hora do evento.
- Indicação de êxito/falha do evento.
- ID do usuário da conta.
- Identificação da fonte do evento, como localização do usuário/sistemas, endereços IP, ID do terminal ou outros meios de identificação.

3.57 A estrutura de auditoria, registro e monitoramento de Terceiros precisará incluir os seguintes componentes:

- Os registros dos eventos geram alertas em tempo real ou quase real para identificar atividades não autorizadas.
- Os eventos e alertas são monitorados por uma função independente de forma contínua e são investigados, avaliados e recebem uma classificação de nível quanto à gravidade.
- Os alertas avaliados envolvem processos de gerenciamento de incidentes de segurança com base em casos de uso e manuais de monitoramento de proteção estabelecidos, conforme os protocolos de nível de serviço e a gravidade.
- Os registros são tratados conforme uma classificação de informações “Confidencial”, no mínimo, e protegidos contra adulteração, acesso não autorizado e perda.
- A atividade de registro e monitoramento é sincronizada com uma fonte de tempo NTP aprovada.
- Os processos são estabelecidos para identificar e configurar casos de uso de monitoramento de proteção adicional e registros de eventos associados, correlações e alertas necessários para lidar com ameaças e riscos significativos existentes ou que venham a surgir.

4. Segurança de Funcionários do Terceiro

4.1 O Terceiro garantirá que todos os Funcionários do Terceiro tenham acordos de confidencialidade antes de começarem a trabalhar nas instalações da BT ou nos Sistemas da BT ou tenham acesso às Informações da BT. Estes acordos de

confidencialidade precisarão ser mantidos pelo Terceiro e as evidências serão disponibilizadas para auditoria pela BT.

4.2 O Terceiro precisará lidar com as violações do Terceiro e dos controles e padrões de segurança aplicáveis da BT, através de processos formais, inclusive ações disciplinares, que podem incluir o impedimento de o indivíduo:

- ter Acesso aos Sistemas da BT ou Informações da BT; ou
- realizar trabalhos relacionados com a prestação do Serviço.

Além disso, o Terceiro deverá garantir que dispõe de processos relevantes para assegurar que qualquer Funcionário do Terceiro, que tenha sido afastado, não tenha acesso posteriormente aos Sistemas da BT, Informações da BT ou permissão para trabalhar em relação à prestação do Serviço.

4.3 O Terceiro deverá, conforme permitido por lei, manter uma unidade exclusiva e independente, a ser utilizada pelos Funcionários do Terceiro para reportar de forma anônima, caso recebam instruções para agir de forma incompatível ou em caso de violação destes Requisitos de Segurança. As comunicações relevantes devem ser notificadas à BT.

4.4 Assim que os Funcionários do Terceiro não são mais designados para o Serviço, por opção da BT, quaisquer bens físicos da BT ou Informações da BT que estejam em posse dos Funcionários do Terceiro deverão ser: devolvidos à equipe operacional relevante da BT ou destruídos de forma segura, de acordo com os controles de segurança 3.22 e 3.23.

4.5 O Terceiro precisará dispor de uma estrutura estabelecida e consistente sobre o uso aceitável de mídias sociais pessoais e corporativas, que assegure que os funcionários:

- não publiquem conteúdo difamatório, obsceno ou abusivo sobre a organização, seus clientes ou consumidores.
- não usem logotipos de organizações ou clientes sem autorização prévia.
- não divulguem informações confidenciais da organização ou do cliente sem consentimento prévio.
- não publiquem comentários sobre a organização, seus clientes ou clientes que possam ser confundidos ou interpretados como detentores dos comentários oficiais da organização ou de seus clientes.
- não divulguem quaisquer Informações da BT que estejam identificadas como “Gerais”, “Confidenciais” ou “Altamente Confidenciais”.

4.6 O Terceiro precisará garantir que todos os Funcionários do Terceiro que estejam sob seu controle realizem um treinamento obrigatório sobre segurança da informação, o que inclui as práticas recomendadas de Cibersegurança e a proteção de dados pessoais, no prazo de um mês após a admissão e que tal procedimento seja atualizado pelo menos uma vez por ano, inclusive, quando apropriado:

- Usuários prioritários
- Partes interessadas do Terceiro (por exemplo, terceirizados, clientes, parceiros)
- Executivos seniores
- Funcionários responsáveis pela segurança física e pela cibersegurança

4.7 O Terceiro precisará garantir que exista um componente de teste para verificar se o funcionário está ciente do treinamento e da capacitação.

5. Revisão de Auditoria e Segurança

5.1 Sem prejuízo de qualquer outro direito de auditoria que a BT possa ter, a fim de avaliar a conformidade do Terceiro em relação aos controles de segurança nesta política de Requisitos de Segurança, o Terceiro fornecerá à BT, ou aos seus representantes, acesso e assistência, conforme necessário e apropriado para permitir a realização de análises de segurança baseadas em documentos ou auditorias no local. O Terceiro será notificado com um mínimo de 30 dias úteis de antecedência, no caso de uma auditoria de rotina no local.

O objetivo da auditoria será analisar quaisquer ou todos os aspectos das políticas, processos e sistema(s) do Terceiro (desde que o Terceiro proteja a confidencialidade de quaisquer informações não relacionadas à prestação do Serviço à BT), que sejam relevantes para o Serviço prestado.

5.2 O Terceiro trabalhará com a BT para implementar as recomendações acordadas e realizará quaisquer ações corretivas identificadas como necessárias, resultantes de uma revisão de segurança baseada em documentos ou auditoria no local, dentro de 30 dias após a notificação da BT de uma não conformidade maior, 90 dias após a notificação da BT de uma não conformidade menor ou qualquer período acordado entre as partes, com todas as despesas por conta do Terceiro.

6. Direito de Inspeção

6.1 O Terceiro precisará permitir que a BT realize uma inspeção na área de controle onde os serviços são desenvolvidos, fabricados ou fornecidos para realizar testes e/ou avaliações de conformidade de segurança, mediante solicitação adequada (ou imediatamente após um incidente).

6.2 O Terceiro é responsável pelos custos de correção de quaisquer vulnerabilidades de segurança identificadas pela BT, dentro de um prazo acordado por ambas as Partes.

6.3 Na eventualidade de um incidente grave, o Terceiro deverá cooperar plenamente com a BT em qualquer investigação posterior por parte da BT, de uma autoridade reguladora e/ou de qualquer órgão responsável pela aplicação da lei, através da disponibilização de acesso e assistência, conforme necessário e apropriado, para a investigação do incidente. A fim de auxiliar na investigação, a BT poderá solicitar ao Terceiro que proceda com de forma cautelar e realize uma análise de qualquer bem relevante pertencente ao Terceiro, o qual não poderá restringir ou atrasar tal procedimento sem razão justificada.

7. Certificações de Segurança

7.1 Os Sistemas, Serviços, Serviços relacionados, processos e locais físicos do Terceiro devem estar em conformidade com a norma ISO/IEC 27001 (ou certificação(ões) que demonstre(m) controles equivalentes, respaldados por um relatório de auditoria independente) bem como qualquer versão alterada ou futura da norma emitida. Esta conformidade precisará ter a garantia da certificação do SGSI do Terceiro por um Serviço de Credenciamento do Reino Unido (UKAS) ou por um órgão de certificação internacional equivalente aprovado, em que a abrangência e a declaração de

aplicabilidade englobem os serviços prestados a partir dos locais de onde serão prestados.

7.2 O Terceiro precisará apresentar um certificado válido na assinatura do contrato e em futuras recertificações.

7.3 Se a abrangência do certificado ou declaração de aplicabilidade for alterada durante a vigência do contrato, de modo a não cobrir mais todos os serviços prestados nos locais a partir dos quais são prestados, o Terceiro precisará informar a BT dentro de um prazo aceitável. O Terceiro precisará informar a BT dentro de 2 dias úteis sobre qualquer não conformidade importante identificada pelo órgão de certificação ou pelo Terceiro, uma vez que representa um risco para os serviços prestados.

8. Segurança Física – Instalações da BT

8.1 O Terceiro deverá cumprir todas as instruções relevantes que lhe forem fornecidas, relativamente ao acesso às instalações da BT e aos sistemas de entrada nas instalações. Qualquer Funcionário do Terceiro que trabalhe nas instalações da BT precisará dispor de um cartão de identificação fornecido pelo Terceiro ou pela BT, o qual incluirá uma fotografia nítida e autêntica do Funcionário do Terceiro.

8.2 A BT pode também fornecer aos Funcionários do Terceiro um cartão de acesso eletrônico e/ou um cartão de visitante de duração determinada, que deverá ser utilizado de acordo com as instruções de emissão e revogação locais

8.3 O Terceiro é responsável por informar a BT, com 24 horas de antecedência, sempre que um funcionário do Terceiro não necessite mais de acesso às instalações da BT e/ou acesso aos sistemas de acesso da BT.

8.4 Somente funcionários autorizados da BT, PCs Webtop da BT e Dispositivos Finais Confiáveis podem se conectar diretamente (conectar na porta LAN ou conexão sem fio) aos domínios da BT. O Terceiro não poderá, sem a autorização prévia por escrito da BT, conectar qualquer equipamento não aprovado pela BT a nenhum domínio da BT.

8.5 A proteção física e as diretrizes para trabalhar nas instalações da BT deverão ser cumpridas e incluir, entre outras, a escolta do Funcionário do Terceiro e a adoção de práticas de trabalho apropriadas em áreas seguras.

8.6 Nos casos em que o Terceiro esteja autorizado a fornecer aos seus Funcionários Terceirizados acesso não acompanhado a áreas internas de propriedade da BT, o representante autorizado do Terceiro e os Funcionários do Terceiro precisarão cumprir as diretrizes do documento de orientação Acesso do Fornecedor às instalações da BT - Guia de Segurança Obrigatório sobre Relações Comerciais com a BT.

9. Segurança Física – Instalações do Terceiro

9.1 O Terceiro precisará dispor de um procedimento de acesso físico que abranja os métodos de acesso e autorização às instalações do Terceiro (locais, instalações ou áreas internas) onde os serviços são prestados ou onde as Informações da BT são armazenadas ou processadas. O método de acesso deverá incluir um ou mais dos seguintes itens:

- Um cartão de identificação do Terceiro autorizado, com uma imagem fotográfica no cartão que seja nítida e que possua uma representação autêntica do funcionário.
- Um cartão de acesso eletrônico autorizado para ter acesso às áreas relevantes das instalações.
- Acesso de segurança com teclado, que precisará conter procedimentos relacionados a: autorização, comunicação sobre alterações da senha (que precisará ocorrer mensalmente, no mínimo) e alterações de código ad-hoc.
- Reconhecimento biométrico.

9.2 O Terceiro precisará dispor de processos e procedimentos para o controle e o monitoramento de visitantes e demais pessoas externas, inclusive funcionários com acesso físico a áreas seguras ou para fins de manutenção de controle ambiental, manutenção de alarmes e limpeza.

9.3 As áreas seguras nas instalações do Terceiro destinadas à prestação do serviço (por exemplo, salas de comunicações de rede) deverão ser separadas das áreas de acesso geral e protegidas por controles de entrada apropriados para garantir que somente indivíduos autorizados tenham permissão de acesso. O acesso a tais áreas precisará passar por auditoria regularmente e uma avaliação da reautorização dos direitos de acesso a essas áreas precisará ser realizada anualmente, no mínimo.

9.4 O Terceiro deverá dispor de sistemas de segurança CCTV nos locais onde as Informações da BT são armazenadas ou manuseadas. As gravações e os gravadores precisarão estar localizados de forma segura para evitar que sejam modificados, excluídos ou visualizados “por acaso” em quaisquer telas de CCTV correspondentes, além de o acesso às gravações ser controlado e restrito apenas a indivíduos autorizados. As gravações de CCTV precisarão ser mantidas por um período mínimo de 20 dias.

9.5 O Terceiro precisará implementar medidas apropriadas para garantir a segurança física com relação ao seguinte:

- Medidas de prevenção de incêndio, as quais estão incluídas, entre outras, alarmes, equipamentos de detecção e extinção.
- Condições climáticas, com a devida atenção à temperatura, umidade e eletricidade estática e ao gerenciamento, monitoramento e resposta associados a condições extremas (como interrupção automática, alarmes).
- Equipamentos de controle, os quais incluem, entre outros, equipamentos de ar condicionado e de detecção de água.
- Prevenção de danos causados pela água, localização de tanques de água, tubulações, etc. dentro das instalações.

9.6 O Terceiro precisará garantir que o acesso físico às áreas nas quais as informações da BT estão armazenadas seja feito por meio de cartões inteligentes ou de proximidade (ou sistemas de segurança equivalentes ou mais eficientes), além de realizar verificações mensais para garantir que apenas os indivíduos autorizados tenham acesso a elas.

9.7 O Terceiro precisará garantir que é terminantemente proibido fotografar e/ou capturar imagens de qualquer informação da BT. Nos casos em que houver uma necessidade comercial de capturar tais imagens, será necessário obter uma confirmação por escrito das Partes Interessadas da BT.

10. Disponibilização de Ambiente de Armazenamento para Equipamentos da BT

10.1 O Terceiro precisará, sempre que este fornecer uma área de acesso seguro em suas instalações para armazenar equipamentos da BT ou de clientes da BT:

- Fornecer à BT uma planta baixa do espaço alocado na área segura das instalações.
- Certificar-se de que os armários da BT e dos clientes da BT, nas instalações, são mantidos trancados e apenas acessados por funcionários autorizados da BT, representantes aprovados pela BT e funcionários pertinentes do Terceiro.
- Implementar um processo seguro de gerenciamento das chaves.

10.2 A BT deverá fornecer ao Terceiro:

- Um registro dos bens físicos da BT e/ou do cliente da BT mantidos nas instalações do Terceiro.
- Dados dos funcionários, terceirizados e representantes da BT que necessitem de acesso às instalações do Terceiro (de forma contínua).

11. Desenvolvimento de Software Seguro

11.1 O Terceiro precisará garantir que os ambientes de produção e de não produção sejam adequadamente controlados, através do cumprimento dos seguintes requisitos:

- Separação de ambientes de produção e de não produção com divisão de tarefas.
- Nenhum dado ativo deve ser usado em testes, a menos que haja acordo prévio dos proprietários dos dados e controles compatíveis com o ambiente de produção.
- Separação de tarefas entre desenvolvimento de produção e não produção.

11.2 O Terceiro precisará dispor de uma estrutura de Desenvolvimento de Sistemas estabelecida e consistente para evitar vulnerabilidades em termos de segurança e violações de Cibersegurança, que contenha os seguintes requisitos:

- Os sistemas são desenvolvidos de acordo com as práticas recomendadas de Desenvolvimento Seguro (por exemplo, OWASP).
- O código está armazenado de forma segura e em conformidade com a Garantia de Qualidade.
- O código está adequadamente protegido contra modificações não autorizadas, uma vez que o teste esteja aprovado e entregue para produção.

12. Garantia

12.1 Nos casos em que seja necessário uma Garantia para proteger todas as partes, tanto para a Organização quanto para o Terceiro (ou seja, para Propriedade Intelectual/ Código-Fonte, etc.), o Terceiro precisará dispor de uma estrutura consistente e estabelecida que inclua os seguintes requisitos:

- Execução do Contrato de Depósito em Garantia independente, neutro e idôneo.
- Entrega e atualizações contínuas do código-fonte e de outros materiais ao terceiro depositário para garantir que as informações necessárias estejam atualizadas.

- Armazenamento seguro do código-fonte e de outros materiais até que as condições de autorização sejam atendidas.
- Condições de autorização apropriadas.
- Atualizações contínuas, pagamentos correspondentes e revisões do contrato de Depósito em Garantia.

13. Acesso aos Sistemas da BT

13.1 O Terceiro deverá cumprir todas as instruções pertinentes que lhe forem fornecidas com relação ao acesso e utilização dos Sistemas da BT.

13.2 O Terceiro é responsável por informar a BT dentro de 24 horas quando um funcionário terceirizado não necessitar mais de acesso.

13.3 O Terceiro precisará garantir que a identificação do usuário, senhas, PINs, tokens e acesso às reuniões sejam para o Funcionário específico do Terceiro e que não sejam compartilhados. Os dados devem ser armazenados de forma segura e separadamente do dispositivo usado para o acesso. Caso outra pessoa tenha conhecimento de uma senha, será necessário alterar as credenciais imediatamente.

Conectividade entre Sistemas

13.4 A criação de vínculos entre domínios com os sistemas da BT não é permitida, a menos que especificamente aprovada e autorizada pela BT.

13.5 O Terceiro precisará realizar todos os esforços necessários para garantir que nenhum malware (como o termo é geralmente usado no setor de computação) seja introduzido nos sistemas da BT.

13.6 Nos casos em que exista conectividade entre o Terceiro e os sistemas da BT, a conectividade será feita através de ligações seguras com dados protegidos por encriptação, em conformidade com os controles de criptografia em 14.9, 14.10, 14.11, 14.12 e 14.13.

13.7 O Terceiro garantirá que os sistemas e a infraestrutura usados estejam contidos em uma rede lógica exclusiva. Esta rede deve consistir apenas nos sistemas destinados ao fornecimento de uma instalação segura de processamento de dados do cliente.

14. Sistemas do Terceiro com Informações da BT

14.1 O Terceiro precisará garantir que as correções de segurança mais recentes sejam aplicadas aos sistemas/ativos/redes/aplicativos, para garantir que:

- O Terceiro implemente as correções assim que possível e empregue o máximo de empenho para implementá-las conforme os seguintes prazos após qualquer atividade de correção:

	Ativamente explorado na natureza	**Alta vulnerabilidade** do EPSS CVSS: > 8,0 (Alto + Crítico) EPSS: >= 70% (Vetor de ataque à rede - consulte a seção de definições)	**Baixa vulnerabilidade** do EPSS CVSS: > 8,0 (Alto + Crítico) EPSS: < 70% (Vetor de ataque à rede - consulte a seção de definições)	**Outro** (vetor de ataque não relacionado à rede)
Interface exposta externamente	7 dias	14 dias	30 dias	90 dias
Interface exposta internamente	7 dias	14 dias	30 dias	90 dias/BAU

- O Terceiro usa correções obtidas de: fornecedores diretos no caso de sistemas exclusivos e correções que são (i) identificadas digitalmente ou (ii) verificadas por meio do uso de um hash de fornecedor (hashes MD5 não poderão ser usados) para o pacote de atualização, de modo que a correção possa ser identificada como proveniente de uma comunidade de suporte confiável para software de código aberto.
- O Terceiro testa todas as correções em sistemas que representam com precisão a configuração dos sistemas de produção de destino antes da implementação da correção nos sistemas de produção e verifica a operação correta do serviço com correção após qualquer atividade de correção.
- O monitoramento de todos os fornecedores pertinentes e de outras fontes de informação relevantes para alertas sobre vulnerabilidades.
- Caso um sistema não possa ser corrigido, será necessário implementar algumas ações corretivas pertinentes.
- O Terceiro instalará correções essenciais quanto à segurança separadamente das versões de funcionalidades para maximizar a velocidade com que a correção pode ser implementada e priorizará as correções essenciais quanto às atualizações de funcionalidade sempre que possível.

14.2 O Terceiro precisará garantir que, no mínimo uma vez por ano, uma avaliação independente de segurança de TI/teste por invasão aprovado pelo Departamento de Segurança da BT seja realizado na infraestrutura de TI do Terceiro e nos aplicativos usados para fornecer serviços, inclusive nos sites de Recuperação de Desastres, para identificar vulnerabilidades que possam ser exploradas através da violação de dados/serviços e para prevenir quaisquer violações de segurança através de ataques cibernéticos. O Terceiro precisará, mediante solicitação cabível, autorizar que a BT tenha acesso aos relatórios de testes de invasão relacionados aos serviços fornecidos.

14.3 O Terceiro precisará garantir que o acesso às portas de diagnóstico e gerenciamento, bem como às ferramentas de diagnóstico, seja controlado com segurança.

14.4 O Terceiro precisará garantir que o acesso às ferramentas de auditoria seja exclusivo aos funcionários competentes do fornecedor e que seu uso seja monitorado.

14.5 O Terceiro precisará garantir que quaisquer servidores usados para fornecer o serviço não sejam implantados em redes não confiáveis (redes que estejam fora do perímetro de segurança do Terceiro, que estejam fora de seu controle administrativo, por exemplo, aplicativos que se conectem à Internet) sem os controles de segurança adequados.

Gestão de Ativos

14.6 O Terceiro precisará manter um inventário de ativos de informações preciso e atualizado de todos os ativos de tecnologia capazes de armazenar ou processar informações, de modo que somente dispositivos autorizados tenham acesso e que dispositivos não autorizados e não gerenciados sejam detectados e bloqueados. Este inventário deverá incluir todos os ativos de hardware, independentemente de estarem ou não conectados à rede da organização. Conforme apropriado, qualquer equipamento da BT hospedado em instalações do Terceiro deverá ser incluído no inventário.

14.7 O Terceiro precisará garantir que o inventário de ativos de informações possua os seguintes componentes inventariados ou catalogados:

- Dispositivos e sistemas físicos, plataformas e aplicativos de software, sistemas de informação externos.
- A priorização dos recursos (por exemplo, hardware, dispositivos, dados, duração e software) é feita com base em sua classificação, relevância e valor comercial.
- Fluxos de dados organizacionais e de comunicação, inclusive fluxos externos/do Terceiro.
- Processos manuais nos quais são gerenciados dados da BT ou dos Clientes da BT.

14.8 O Terceiro precisará manter um inventário de ativos de software atualizado e preciso para todos os softwares na rede, de modo que somente softwares autorizados sejam instalados e possam ser executados, além de detectar e bloquear a instalação ou execução de softwares não autorizados e não gerenciados.

Criptografia

14.9 O Terceiro precisará garantir que as Informações da BT classificadas como Confidenciais ou similares sejam adequadamente criptografadas (seja em trânsito ou em repouso). Todas as criptografias devem ser realizadas com algoritmos criptográficos avançados e modernos e códigos que utilizem mecanismos eficientes de proteção de integridade e que estejam de acordo com os padrões da indústria para a negociação segura de senhas e protocolos e gerenciamento de senhas. Em relação aos dados em trânsito, as seguintes opções de TLS não são permitidas: TLS v1.0, TLS v1.1 e SSL (qualquer versão). As seguintes opções de SSH (SFTP) não são permitidas: SSH v1. As seguintes opções de IPSec não são permitidas: IKE versão 1.

14.10 As chaves criptográficas precisarão corresponder aos seguintes comprimentos mínimos ou excedê-los:

- As chaves simétricas (por exemplo, AES) precisarão ter um comprimento de chave de pelo menos 256 bits.

- As chaves assimétricas (por exemplo, RSA) precisarão ter um comprimento de chave de pelo menos 3072 bits.
- As chaves de curva elíptica precisarão ter um comprimento de chave de pelo menos 384 bits.

14.11 Se o NIST indicar que um algoritmo de criptografia não é mais seguro, ele não poderá ser usado em novas implementações. As implementações existentes precisarão considerar o uso contínuo de algoritmos de criptografia obsoletos e fornecer um plano de migração para substituir os algoritmos de criptografia obsoletos por uma alternativa mais segura.

14.12 Para criptografia simétrica, os seguintes algoritmos não são permitidos: 3DES-168 (a menos que seja exigido por uma norma internacional), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed e ARIA.

14.13 O uso de salted hashes será necessário para proteger os dados armazenados, por exemplo, senhas. Os hashes também podem ser usados para anonimizar dados antes do processamento, por exemplo, MSISDNs ou pagamentos. Os seguintes algoritmos de hash não são permitidos: MD2, MD4, MD5 e SHA-1.

Configuração do Sistema

14.14 O Terceiro precisará ter uma estrutura estabelecida e consistente para garantir que os sistemas sejam configurados adequadamente, o que inclui os seguintes requisitos:

- Sistemas e dispositivos de rede são configurados para funcionar de acordo com os princípios de segurança (por exemplo, o conceito de menor funcionalidade e nenhum software não autorizado).
- Garantia de que os dispositivos tenham o horário correto e consistente.
- Os sistemas estejam livres de qualquer software malicioso.
- Existam verificações e monitoramento adequados para garantir que a integridade das versões/dispositivos seja mantida.

Proteção contra malware

14.15 O Terceiro precisará garantir que a proteção contra malware mais atualizada seja aplicada em todos os ativos de TI pertinentes para evitar interrupções de serviço ou violações de segurança e garantir que os procedimentos adequados de conscientização do usuário sejam implementados.

A proteção contra malware precisará incluir a detecção de (mas não se limitará a) ransomware, código móvel não autorizado, vírus, spyware, software de registro de chaves, botnets, worms, cavalos de Troia, etc.

Mitigações de Negação de Serviço.

14.16 O Terceiro precisará garantir que os principais sistemas estejam protegidos contra ataques de negação de serviço (DoS) e negação de serviço distribuída (DDoS).

15. Sistemas do Terceiro Responsáveis pelo Armazenamento das Informações da BT

15.1 Em complementação aos registros da Seção 14. Sistemas do Terceiro que detêm as Informações da BT, onde o Terceiro é o responsável pelo armazenamento das Informações da BT em um centro de dados ou solução em nuvem, as instalações precisarão ter um certificado ISO/IEC 27001 válido para a gestão de segurança (ou certificação(ões) que demonstre(m) controles equivalentes, respaldados por um relatório de auditoria independente).

16. Segurança de Rede – Rede própria da BT

Caso o Terceiro instale equipamentos, configure, realize a manutenção, gerencie, repare ou monitore a rede da própria BT, os seguintes registros serão aplicados:

16.1 Mediante solicitação, o Terceiro fornecerá à BT os nomes, endereços e demais detalhes que a BT solicite de forma pertinente, de todo os Funcionários do Terceiro que:

- deverão, periodicamente, estar diretamente envolvidos na implementação, manutenção e/ou gerenciamento do(s) Serviço(s), antes de serem contratados.
- deverão estabelecer relações com a BT, através de discussões sobre as vulnerabilidades identificadas pela BT e/ou pelo Terceiro, em relação ao(s) Serviço(s).

16.2 No que diz respeito às suas atividades de apoio estabelecidas no Reino Unido, o Terceiro manterá uma equipe de segurança qualificada, composta por pelo menos um cidadão do Reino Unido, o qual estará disponível para estabelecer contatos com a BT, além disso, a equipe participará das reuniões que a BT, periodicamente, solicitar.

16.3 O Terceiro fornecerá à BT um cronograma (atualizado de forma periódica, conforme necessário) de todos os componentes ativos incluídos no(s) Serviço(s) e suas respectivas procedências.

16.4 O Terceiro precisará garantir que a instalação de novos sistemas, equipamento ou software na própria rede da BT, utilize a versão de software e correção mais recente.

16.5 O Terceiro deverá assegurar que todos os registros relevantes à segurança sejam habilitados em todos os equipamentos de rede instalados pelo Terceiro e enviados para os sistemas de registro de rede da BT.

16.6 O Terceiro fornecerá à BT informações pontuais (ou seja, o mais brevemente possível para permitir a reparação antes da publicação oficial) em relação a quaisquer vulnerabilidades no(s) Serviço(s) e cumprir (com os custos por conta do Terceiro) com os requisitos pertinentes em relação às vulnerabilidades, conforme notificação da BT.

16.7 O Terceiro deverá assegurar que quaisquer elementos relacionados com a segurança, incluídos no(s) Serviço(s), que sejam identificados pela ou para a BT, de forma periódica, sejam, por conta do Terceiro, avaliados externamente de forma satisfatória pela BT.

16.8 O Terceiro fornecerá prontamente à BT, dentro de 7 Dias Úteis, todos os detalhes de quaisquer recursos e/ou funcionalidades no(s) Serviço(s) ou que estejam planeados no Plano para o(s) Serviço(s) que, periodicamente:

- o Terceiro tenha conhecimento; ou

- a BT acredita de forma plausível e, deste modo, informa o Terceiro, que foram concebidos ou possam ser usados para a interrupção legal ou qualquer outra interrupção do tráfego de telecomunicações. Tais detalhes deverão incluir todas as Informações que sejam devidamente necessárias para permitir à BT compreender totalmente a natureza, composição e extensão de tais características e/ou funcionalidades.

16.9 O Terceiro não poderá usar nenhuma ferramenta de monitoramento de rede que possa exibir informações dos aplicativos.

16.10 A construção, desenvolvimento e/ou apoio à rede própria da BT por parte dos Funcionários do Terceiro deverá ter, no mínimo, uma verificação de pré-contratação L2. As verificações de pré-contratação L3 serão necessárias para funções identificadas pela BT.

16.11 O Terceiro permitirá que a BT instale software de segurança de acordo com as especificações da BT, em qualquer infraestrutura virtual do Terceiro (que inclui, mas não se limita a máquinas virtuais e mecanismos operacionais) ou sistema operacional instalado pelo Terceiro, em execução nas Redes da BT.

16.12 O Terceiro precisará garantir que as correções de segurança mais recentes sejam aplicadas aos sistemas/ativos/redes/aplicativos, para garantir que:

- O Terceiro implemente as correções assim que possível e empregue o máximo de empenho para implementá-las conforme os seguintes prazos após qualquer atividade de correção:

	Ativamente explorado na natureza	**Alta vulnerabilidade** do EPSS CVSS: > 8,0 (Alto + Crítico) EPSS: >= 70% (Vetor de ataque à rede - consulte a seção de definições)	**Baixa vulnerabilidade** do EPSS CVSS: > 8,0 (Alto + Crítico) EPSS: < 70% (Vetor de ataque à rede - consulte a seção de definições)	**Outro** (vetor de ataque não relacionado à rede)
Interface exposta externamente	7 dias	14 dias	30 dias	90 dias
Interface exposta internamente	7 dias	14 dias	30 dias	90 dias/BAU

- O Terceiro usa correções obtidas de: fornecedores diretos no caso de sistemas exclusivos e correções que são (i) identificadas digitalmente ou (ii) verificadas por meio do uso de um hash de fornecedor (hashes MD5 não poderão ser usados) para o pacote de atualização, de modo que a correção possa ser identificada como proveniente de uma comunidade de suporte confiável para software de código aberto.

- O Terceiro testa todas as correções em sistemas que representam com precisão a configuração dos sistemas de produção de destino antes da implementação da correção nos sistemas de produção e verifica a operação correta do serviço com correção após qualquer atividade de correção.
- O monitoramento de todos os fornecedores pertinentes e de outras fontes de informação relevantes para alertas sobre vulnerabilidades.
- Caso um sistema não possa ser corrigido, será necessário implementar algumas ações corretivas pertinentes.
- O Terceiro fornecerá correções essenciais quanto à segurança separadamente das versões das funcionalidades para maximizar a agilidade com que a correção pode ser implementada e priorizará as correções importantes quanto à segurança em relação às atualizações de funcionalidade conforme possível.

Lei (da Segurança) das Telecomunicações de 2021 (TSA)

Nos casos em que o Terceiro forneça ou disponibilize bens, serviços ou recursos para uso em associação a uma rede ou serviço público de comunicações eletrônicas do Reino Unido, os seguintes controles de segurança serão adotados.

16.13 Nos casos em que o Terceiro ofereça suporte a mais de um operador, serão implementados controles para evitar que um operador ou sua rede afetem negativamente qualquer outro operador ou sua rede.

16.14 Nos casos em que o Terceiro atue como Administrador do Terceiro para mais de um operador, os seguintes controles serão adotados:

- Implementar a separação lógica dentro da rede do Terceiro para separar os dados e as redes dos clientes.
- Implementar a separação entre os ambientes de gerenciamento do Terceiro usados para redes de operadoras diferentes.
- Implementar e aplicar funções que garantam a segurança no limite entre a rede do Terceiro e a rede do operador.
- Implementar controles técnicos para limitar a possibilidade de usuários ou sistemas afetarem negativamente mais de um operador.
- Implementar estações de trabalho de acesso prioritário física e logicamente independentes por operador.
- Implementar domínios administrativos e contas independentes por operador.

16.15 Ao fornecer equipamento de rede, os Terceiros precisarão fornecer à BT uma “declaração de segurança” sobre a forma como o equipamento seguro é produzido e como a segurança do equipamento é garantida ao longo da sua vida útil. Esta declaração de segurança deverá abranger os requisitos da Avaliação de Segurança do Fornecedor, publicada no Anexo B do Código de Conduta para a Segurança das Telecomunicações, bem como deverá ser aprovada em nível apropriado de hierarquia acordado com a BT.

16.16 Nos casos em que o Terceiro forneça equipamentos de rede, os seguintes controles são necessários:

- O Terceiro garante que respeitará uma norma não inferior à publicada na “declaração de segurança”.

- O Terceiro fornecerá orientações atualizadas sobre como o equipamento deve ser implantado de forma segura.
- O Terceiro fornecerá suporte a todos os equipamentos e a todos os subcomponentes de software e hardware durante a vigência do contrato.
- O Terceiro fornecerá detalhes de todas as suas principais dependências e componentes como, por exemplo, produto e versão, componentes de código aberto, nível e período de assistência.
- O Terceiro corrigirá todos os problemas de segurança que representem um risco de segurança para a rede ou serviço da BT, detectados nos seus produtos, dentro de um período de tempo adequado após a notificação, através de atualizações regulares sobre o andamento do processo - esse período será acordado entre a BT e o Terceiro, ambos agirão com base em critérios plausíveis. Tal medida deverá incluir todos os produtos impactados de acordo com a vulnerabilidade, não apenas o produto para o qual foi reportada a vulnerabilidade.
- O Terceiro removerá ou alterará as senhas e contas padrão ou codificadas ou assegurará que o equipamento de rede esteja configurado para permitir que a BT o faça.
- O Terceiro, sempre que possível, desabilitará os protocolos de gerenciamento não criptografados e, quando não for possível, identificará a presença de tais protocolos à BT para permitir que seu uso seja mitigado.

16.17 Se o Terceiro tiver obtido avaliações ou certificações de segurança internacionalmente reconhecidas para o equipamento (por exemplo, Common Criteria ou NESAS), deverá compartilhar com a BT os resultados completos que evidenciam esta avaliação ou certificação.

16.18 Quando a própria rede do Terceiro possui potencial para impactar as Redes da BT, o Terceiro irá, conforme orientação da BT, submeter-se ao mesmo nível de testes que a BT aplica às Redes da BT e irá corrigir as vulnerabilidades identificadas, conforme acordado por ambas as partes.

16.19 O Terceiro autoriza a BT a compartilhar detalhes sobre problemas de segurança, conforme apropriado, quando necessário para fins de segurança da rede.

16.20 A infraestrutura e os sistemas utilizados para manter as Redes da BT devem estar localizados no Reino Unido.

16.21 Nos casos em que o Terceiro executa as Funções de Supervisão de Rede da BT, o equipamento utilizado para esta função deverá estar localizado no Reino Unido e ser operado por funcionários localizados no Reino Unido.

16.22 Se o Terceiro for responsável pela segurança da rede e pelos registros de auditoria, estes deverão ser armazenados no Reino Unido e protegidos de acordo com a lei do Reino Unido.

16.23 Nos casos em que o Terceiro esteja atuando como um Administrador do Terceiro, a BT terá o direito de determinar as permissões das contas utilizadas pelo Terceiro para acessar a sua rede, bem como de exigir todos os registros relacionados à segurança da rede do Terceiro, na medida em que tais registros estejam relacionados ao acesso à rede da BT. O Terceiro deverá monitorar e auditar as atividades de sua equipe ao acessar a rede da BT.

17. Segurança da Rede do Terceiro

17.1 O Terceiro precisará garantir que a integridade da rede seja estabelecida e mantida, ao assegurar que os seguintes componentes sejam adequadamente controlados, além de notificar a BT sobre quaisquer ocorrências em que tal procedimento não seja tecnicamente possível:

- As conexões externas à rede são devidamente identificadas, roteadas por meio de um firewall e verificadas e aprovadas antes do estabelecimento das conexões para evitar violações da segurança dos dados.
- A rede foi projetada adequadamente através dos princípios de "defesa em profundidade" para garantir que as violações de Cibersegurança sejam minimizadas, com a garantia de que haja controles apropriados que impeçam qualquer ataque intencional, como a "segmentação de rede".
- O projeto e a implementação da rede são revisados no mínimo uma vez por ano.
- Todo o acesso sem fio à rede está sujeito a protocolos de autorização, autenticação, segmentação e criptografia para evitar violações de segurança.
- Utilização de comunicações seguras entre dispositivos e estações de gerenciamento.
- Utilização de comunicações seguras entre dispositivos, conforme apropriado, o que inclui a criptografia de todos os acessos de administrador que não sejam pelo console.
- Utilização de um projeto arquitetônico sólido, em camadas e zonas, com gerenciamento eficaz de identidade e configuração do sistema operacional, de modo que seja devidamente reforçado e documentado.
- Por meio da desativação (quando possível) de serviços, aplicativos e portas que não serão usados.
- Por meio da desativação ou remoção de contas de convidados.
- Por meio da prevenção de relações de confiança entre servidores.
- Utilização do princípio de segurança de práticas recomendadas de "menos privilégio" para executar uma função.
- Garantia de que medidas apropriadas estejam em vigor para detecção e/ou proteção contra invasões.
- Conforme apropriado, monitoramento da integridade do arquivo para detectar quaisquer integrações, modificações ou exclusões de arquivos ou dados críticos do sistema.
- Alteração de todas as senhas padrão e fornecidas pelo fornecedor antes que os componentes da rede entrem em operação.
- Desativação de protocolos de gerenciamento não criptografados sempre que tecnicamente possível.

17.2 A Rede do Terceiro deverá atender a todos os requisitos legais e regulamentares e:

- Iniciativas de prevenção contra o acesso de indivíduos não autorizados (por exemplo, hackers) à(s) Rede(s) do Terceiro.

- Iniciativas para reduzir o risco de uso indevido da(s) Rede(s) do Terceiro por funcionários autorizados a acessá-la(s).
- Iniciativas para detectar quaisquer violações de segurança e garantir a rápida retificação de quaisquer violações, juntamente com a identificação dos indivíduos que obtiveram acesso e a determinação de como eles obtiveram esse acesso.

Lei (da Segurança) das Telecomunicações de 2021

17.3 Nos casos em que o Terceiro estiver fornecendo ou disponibilizando itens, serviços ou recursos para uso relacionado a uma rede ou serviço público de comunicações eletrônicas do Reino Unido, os seguintes controles de segurança adicionais deverão ser implementados:

- Os sistemas voltados para o exterior, exceto os Equipamentos nas Instalações do Cliente (CPE), são testados quanto à segurança a cada dois anos ou quando ocorrer uma alteração significativa.
- Os conjuntos de dados confidenciais e as funções confidenciais ou essenciais não são armazenados em equipamentos na Borda Exposta da rede.
- Caso não sejam protegidos por criptografia, deverá ser implementada uma separação física e lógica entre a Borda Exposta e as funções essenciais ou confidenciais.
- Deverá ser implementada uma separação de segurança através de recursos que reforçam a segurança entre a Borda Exposta e as funções essenciais ou confidenciais.

18. Segurança na Nuvem

18.1 O Terceiro precisará obter a certificação da versão mais recente da ISO27017 ou dispor de uma estrutura estabelecida e consistente para garantir que toda a finalidade de utilização da tecnologia de nuvem e dos dados não públicos armazenados na nuvem seja aprovada e submetida a controles adequados equivalentes à versão mais recente da Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Os acordos de nível de serviço de rede e infraestrutura (internos ou terceirizados) deverão documentar claramente as responsabilidades compartilhadas, os controles de segurança, os níveis de capacidade e serviço e os requisitos comerciais ou de clientes.

18.3 O Terceiro precisará implementar medidas de segurança em todos os aspectos do serviço a ser fornecido, de forma a proteger a confidencialidade, disponibilidade, qualidade e integridade, ao minimizar a possibilidade de indivíduos não autorizados (por exemplo, outros clientes da nuvem) terem acesso às Informações da BT e aos serviços utilizados pela BT.

18.4 Na medida em que o Terceiro forneça serviços ou aplicativos armazenados com a BT, de locatário único ou de múltiplos locatários, o que inclui software como serviço, plataforma como serviço, infraestrutura como serviço e ofertas semelhantes, para recolher, transmitir, armazenar ou processar Dados Confidenciais, o Terceiro deverá fornecer à BT a opção de:

- isolar logicamente tais Dados Confidenciais dos dados dos demais clientes do Terceiro;

- restringir, registrar e monitorar o acesso a esses Dados Confidenciais a qualquer momento, inclusive o acesso por parte de Funcionários do Terceiro;
- criar, habilitar, desabilitar e excluir a chave de criptografia mais alta (conhecida como Chave Gerenciada pelo Cliente) usada para criptografar e descriptografar chaves subsequentes, inclusive a chave de criptografia de dados mais baixa;
- restringir, registrar e monitorar o acesso à Chave Gerenciada pelo Cliente de forma permanente; e, em nenhum momento, qualquer chave de criptografia subsequente, uma chave de criptografia em uma hierarquia de chaves inferior à Chave Gerenciada pelo Cliente, será armazenada no mesmo sistema que os Dados Confidenciais, a menos que seja criptografada pela Chave Gerenciada pelo Cliente, também conhecida como "wrapped" pela Chave Gerenciada pelo Cliente.

19. Serviços Móveis

19.1 Nos casos em que o Terceiro fornecer Cartões SIM, os seguintes controles deverão ser implementados:

- Para cartões SIM convencionais, o Terceiro deverá garantir que os dados confidenciais do cartão SIM sejam devidamente protegidos pelo fabricante do cartão SIM.
- Para cartões SIM convencionais, o Terceiro deverá garantir que a confidencialidade, a integridade e a disponibilidade dos dados confidenciais do cartão SIM compartilhados com o fabricante do cartão SIM sejam protegidas em todos os estágios de seu ciclo de vida.

20. Informações classificadas como OFICIAIS ou superiores pela HMG

20.1 Os Requisitos de Segurança adicionais estabelecidos no Anexo 1 destes Requisitos de Segurança serão implementados para cada Terceiro que armazenar, processar ou transmitir informações classificadas como OFICIAIS de acordo com o Esquema de Classificações de Segurança do Governo de Sua Majestade, conforme atualização periódica.

21. Definição e Interpretação de Termos

21.1 A menos que definido de outra forma abaixo, as palavras e expressões usadas nestes Requisitos de Segurança terão o mesmo significado que no Contrato:

"**Acesso**" e **"Acessado"** "Acesso" e "Acessado" correspondem ao Processamento, manuseio ou armazenamento de Informações da BT por um ou mais dos seguintes métodos:

a. através de interconexão com os Sistemas da BT;

b. fornecidas em papel ou em formato que não seja eletrônico;

c. Informações da BT nos Sistemas de Fornecedores; ou

d. por mídias móveis.

e/ou Acesso às instalações da BT para o fornecimento dos Suprimentos, exceto a entrega de hardware e a participação em reuniões.

"**Informação da BT**" corresponde a todas as informações relacionadas com a BT ou com um Cliente da BT, disponibilizadas ao Fornecedor e todas as informações que são processadas ou tratadas pelo Fornecedor em nome da BT ou de um Cliente da BT, nos termos do Contrato.

"Partes Interessadas da BT" corresponde aos representantes da BT, os quais têm a responsabilidade pelos assuntos relacionados à execução das atividades desempenhadas pelo Terceiro.

"**Redes da BT**" corresponde aos Serviços e componentes de Serviços, produtos, redes, servidores, processos, sistemas baseados em papel ou sistemas de TI (no todo ou em parte) pertencentes e/ou operados pela BT ou outros sistemas que possam ser armazenados nas instalações da BT.

"BT's Networks" corresponde a qualquer Rede Pública de Comunicações Eletrônicas operada pela BT, conforme definido pela seção 32 da Lei de Comunicações de 2003.

"BYOD" corresponde a "traga seu próprio dispositivo".

"**Contrato**" corresponde ao Contrato celebrado entre as Partes para o fornecimento de bens, software ou Serviços relacionados a estes Requisitos de Segurança.

"Equipamento nas Instalações do Cliente" corresponde ao equipamento fornecido aos clientes pelo fornecedor e gerenciado pelo fornecedor, que é utilizado, ou que se pretende utilizar, como componente da rede ou do serviço. Exceto dispositivos eletrônicos de consumo, como telefones celulares e tablets, mas que incluem dispositivos como firewalls de perímetro, equipamentos SD-WAN e kit de acesso fixo sem fios. **""**

"**Cyber Essentials Plus**" corresponde ao programa promovido pelo governo do Reino Unido para auxiliar as organizações a se protegerem contra ataques cibernéticos comuns.

"Cibersegurança" corresponde à forma como indivíduos e organizações reduzem o risco de ataques cibernéticos. O principal objetivo da Cibersegurança é proteger os dispositivos que todos nós usamos (smartphones, laptops, tablets e computadores) e os serviços que acessamos, tanto on-line quanto no trabalho, contra furtos ou danos.

"EPSS" corresponde ao Sistema de Pontuação de Previsão de Exploração.

"**Garantia**" corresponde ao acordo de depósito de código-fonte celebrado de acordo com o Contrato, para usar, copiar, manter e modificar tal código-fonte para os fins comerciais da BT (inclusive o direito de compilar tal código-fonte).

"**Borda Exposta**" corresponde ao Equipamento localizado nas instalações do cliente, que pode ser acessado diretamente pelo equipamento do cliente/usuário, ou que seja fisicamente vulnerável. Os equipamentos fisicamente vulneráveis incluem equipamentos em gabinetes localizados em vias públicas ou que estejam instalados em mobiliário urbano. A Borda Exposta inclui CPEs, equipamentos de estações de base, equipamentos OLT e equipamentos MSAN/DSLAM.

"**Boas Práticas de Segurança da Indústria**" corresponde à implementação de práticas, políticas, normas e ferramentas de segurança em relação a qualquer atividade e em quaisquer circunstâncias, o que se espera de maneira adequada e normal que um profissional qualificado e experiente esteja envolvido no mesmo tipo de atividade em circunstâncias iguais ou semelhantes.

"NDA" corresponde a um Acordo de Confidencialidade, um contrato vinculativo entre duas ou mais partes que impede que informações confidenciais sejam compartilhadas com outras pessoas/entidades.

"NESAS" corresponde ao Programa de Garantia de Segurança de Equipamentos de Rede da Associação GSM.

"Ativo de Rede" corresponde a um item integrante de um conjunto de componentes interconectados, como computadores, roteadores, hubs, cabeamento e controladores de telecomunicações que compõem uma rede.

"Vetor de Ataque de Rede" corresponde ao fato de que o componente vulnerável está vinculado à pilha de rede e o conjunto de possíveis invasores vai além das demais opções listadas abaixo, ou seja, inclui toda a Internet. Tal vulnerabilidade é geralmente chamada de "explorável remotamente" e pode ser considerada como um ataque que pode ser explorado no nível do protocolo entre um ou mais hops de rede remota (por exemplo, através de um ou mais roteadores). Entre os exemplos de um ataque à rede podemos citar um invasor que provoca uma negação de serviço (DoS) ao enviar um pacote TCP especialmente criado em uma rede remota (por exemplo, CVE 2004 0230).

"Funções de Supervisão da Rede" corresponde aos componentes da Rede da BT que supervisionam e controlam as funções essenciais de segurança, o que as torna extremamente importantes para a segurança total da rede. São essenciais para que a BT possa ter uma percepção abrangente da rede, a fim de protegê-la ou recuperá-la.

"**Segurança de Rede**" corresponde aos sistemas de segurança dos caminhos e nós de comunicação interconectados que conectam logicamente as tecnologias do usuário final e os sistemas de gerenciamento associados.

"NIST" corresponde ao Instituto Nacional de Padrões e Tecnologia, uma agência do Departamento de Comércio dos EUA. Anteriormente conhecido como Departamento Nacional de Normas, o NIST promove e mantém padrões de avaliação. Há também programas ativos para incentivar e auxiliar o setor e a ciência no desenvolvimento e uso de tais normas.

"**Declaração de Caráter Confidencial e Oficial**" corresponde à declaração por escrito a ser fornecida pelo Fornecedor com relação às funções identificadas pelo Fornecedor com acesso a informações classificadas como "Confidenciais e Oficiais" ou que possuem permissões especiais para a infraestrutura que armazena, processa ou transmite informações classificadas como "Confidenciais e Oficiais", cujo modelo está estabelecido no Anexo 1.

"Estação de Trabalho com Acesso Privilegiado (PAW)" corresponde às estações de trabalho por meio das quais o Acesso Privilegiado é possível.

"Funções Essenciais de Segurança" corresponde a quaisquer funções da Rede da BT ou do Serviço, cuja operação poderá ter um impacto significativo na operação adequada de toda a rede ou serviço ou de parte relevante que a compõe.

"**Requisitos de Segurança**" corresponde a este documento, conforme atualizado periodicamente.

"SIM" corresponde a um componente de hardware ou token exclusivo e ao software associado, usado para autenticar o acesso do usuário à rede. Conforme mencionado neste documento, o SIM engloba o hardware UICC/eUICC, os aplicativos SIM/USIM/ISIM, a funcionalidade eSIM e RSP e eventuais miniaplicativos SIM.

"**Subcontratado**" corresponde a um Subcontratado do Fornecedor que executa ou está envolvido no fornecimento dos Insumos ou que emprega ou contrata profissionais envolvidos no fornecimento dos Insumos.

"**Serviço**" corresponde todos e quaisquer "**Bens**", "**Software**" ou "**Serviços**" conforme definido no Contrato.

"Transação" corresponde aos dados/informações operacionais que são obtidos a partir de transações, ou seja, dados gerados por vários aplicativos durante a execução ou o suporte aos procedimentos comerciais diários.

"Módulo de Plataforma Confiável (TPM)" corresponde à tecnologia projetada para fornecer funções relacionadas à segurança baseadas em hardware. Um chip de Módulo de Plataforma Confiável (TPM) consiste em um processador de criptografia seguro projetado para realizar operações criptográficas. O chip inclui vários mecanismos de segurança física para torná-lo resistente a violações, de forma que um software mal-intencionado não conseguirá violar as funções de segurança do TPM. As funções mais comuns do TPM são usadas para avaliações de integridade do sistema e para criação e uso de chaves. Durante o processo de inicialização de um sistema, o código de inicialização que é carregado (o que inclui o firmware e os componentes do sistema operacional) pode ser avaliado e registrado no TPM. As avaliações de integridade podem ser usadas como evidência de como um sistema foi iniciado e para garantir que uma chave baseada no TPM foi usada exclusivamente quando o software correto foi usado para inicializar o sistema.

"Terceiro" corresponde a um Fornecedor da BT.

"Administrador do Terceiro" corresponde a um fornecedor de serviços gerenciados, fornecedor de funções de grupo ou suporte externo para equipamentos pertencentes a fornecedores terceirizados (por exemplo, função referente ao suporte de terceiro nível).

"**Funcionários do Terceiro**" corresponde aos funcionários contratados pelo Fornecedor ou por seus Subcontratados no desempenho das obrigações do Fornecedor previstas no Contrato.

"Rede do Terceiro" corresponde a qualquer rede do Fornecedor.

"**Sistema do Terceiro**" corresponde a qualquer computador, aplicativo ou sistema de rede de propriedade do Fornecedor, usado para acessar, armazenar ou processar as Informações da BT ou que esteja envolvido no fornecimento dos Insumos.

Interpretação

21.2 Quaisquer palavras após os termos "inclusive", "incluir", "em particular", "por exemplo" ou qualquer termo semelhante serão interpretados como ilustrativos e não limitarão o sentido das palavras, da descrição, da definição, da frase ou do período anterior a esses termos.

21.3 Nas situações em que o direito ou a obrigação de uma Parte for expresso como algo que ela "**poderá**" exercer ou executar, a opção de exercer ou executar esse direito ou obrigação ficará a critério exclusivo da Parte.

21.4 Nos casos em que houver referência a qualquer hiperlink ("**URL**"), tal referência será feita ao recurso on-line acessível por meio desse URL ou a outro URL substituto, conforme notificado à Parte pertinente periodicamente.

Versão	Descrição	Autor:	Data
5.0	Legislação relacionada à Lei (de Segurança) das Telecomunicações de 2021 (TSA) e a adoção do CIS pela BT	Jemma Turner	25/10/22
5.1	Alteração da versão 14.9 do Protocolo de Segurança TLS	Jemma Turner	17/04/23
5.2	Alterações em várias cláusulas para incorporar a TSA e as vulnerabilidades	Jemma Turner	30/11/23

ANEXO 1 - Requisitos Adicionais de Segurança

Nos casos em que o Terceiro necessite acessar, armazenar, processar ou transmitir informações classificadas como OFICIAIS ou similares, o Terceiro cumprirá os Requisitos de Segurança da BT e, além disso, os requisitos estabelecidos neste Anexo 1. Em todos os casos, o controle de nível mais elevado prevalecerá sobre os requisitos documentados em outras partes destes Requisitos de Segurança.

1. FUNCIONÁRIOS

1.1 Todas os Funcionários do Terceiro envolvidos que tenham acesso a informações classificadas como OFICIAIS ou similares e que possuam acesso exclusivo à infraestrutura que armazena, processa ou transmite informações classificadas como OFICIAIS ou similares:

1.1.1 precisarão realizar uma triagem antes de serem contratados, de acordo com a Norma Básica sobre Segurança de Funcionários (BPSS);

1.1.2 precisarão assinar uma declaração da Lei de Segredos Oficiais; e

1.1.3. não poderão acessar informações ou sistemas, a menos que tenham as autorizações de segurança necessárias, conforme especificado no respectivo contrato.

2. TREINAMENTOS SOBRE QUESTÕES RELACIONADAS À SEGURANÇA

2.1. O Terceiro exigirá treinamentos de segurança no momento da contratação e, de preferência, anualmente, para todos os funcionários que tenham acesso a informações classificadas como OFICIAIS ou similares, bem como para aqueles que tenham permissões especiais para acessar a infraestrutura que armazena, processa ou transmite informações classificadas como OFICIAIS ou similares. Este treinamento deverá abranger os requisitos de processamento de informações de acordo com os requisitos do Esquema de Classificação de Segurança Governamental de Sua Majestade, conforme detalhado na Orientação sobre Proteção de Informações do HMG da BT para Terceiros, a qual deverá ser fornecida ao Terceiro pela BT.

2.2. O Terceiro atualizará as descrições dos cargos de todos os funcionários que tenham acesso a informações classificadas como OFICIAIS ou similares ou que tenham permissões especiais para acessar a infraestrutura que armazena, processa ou transmite informações classificadas como OFICIAIS ou similares, a fim de incentivar a participação no treinamento descrito no parágrafo 2.1 acima. O Terceiro manterá um registro do treinamento, que deverá ser disponibilizado à BT mediante solicitação.

3. CONTROLE DE ACESSO

3.1. Nos casos em que os funcionários são desligados ou mudam de função, seus direitos de acesso precisarão ser excluídos dos Sistemas do Terceiro em até 1 dia útil.

3.2. Nos casos em que os funcionários do Terceiro, inclusive terceirizados, funcionários temporários e trabalhadores de agências, tenham permissões especiais para acessar a infraestrutura da BT, o Terceiro precisará notificar a BT por escrito dentro de 1 dia útil, a partir do momento em que um funcionário não precisar mais acessar os sistemas da BT (por exemplo, funcionários que são desligados ou mudam de função).

3.3. Nos casos em que os funcionários do Terceiro, inclusive terceirizados, funcionários temporários e trabalhadores de agências, recebam cartões de acesso permanente às instalações da BT, o Terceiro precisará notificar a BT por escrito, no prazo de 1 dia útil,

quando um funcionário não precisar mais de acesso às instalações da BT (por exemplo, funcionários que são desligados ou mudam de função).

4. AVALIAÇÃO E CLASSIFICAÇÃO DE ATIVOS

4.1. O Terceiro implementará procedimentos adicionais de processamento de informações para atender aos requisitos de gerenciamento de acordo com as exigências do Esquema de Classificação de Segurança Governamental de Sua Majestade, conforme atualizado periodicamente.

5. RESPOSTA E NOTIFICAÇÃO DE INCIDENTES - ACORDOS DE NÍVEL DE SERVIÇO

5.1. O Terceiro será orientado sobre acordos de nível de Serviço específicos para oferecer suporte ao processo de resposta a incidentes. Tais acordos podem substituir eventuais acordos anteriores descritos nestes Requisitos de Segurança.

6. AUDITORIA, TESTES E MONITORAMENTO

6.1. O Terceiro implementará monitoramento de segurança 24 horas por dia, 7 dias por semana, conforme especificado pela BT, para garantir que a infraestrutura do Terceiro suporte o processamento, armazenamento ou transmissão de informações classificadas como OFICIAIS ou similares.

7. CONTINUIDADE OPERACIONAL E RECUPERAÇÃO DE DESASTRES

7.1. O Terceiro desenvolverá um plano de continuidade de negócios e recuperação de desastres de acordo com a norma BS ISO 22301 em até 30 dias após a assinatura do Contrato.

8. LOCALIZAÇÃO

8.1. A menos que especificado de outra forma pela BT, o Serviço precisará estar fisicamente localizado no Reino Unido ou, se aplicável, no EEE. Qualquer suporte remoto e/ou gerenciamento do Serviço pelo Fornecedor, a partir de uma localização no exterior, só poderá ser realizado de acordo com o processo de aprovação estabelecido no contrato vigente entre a BT e o departamento governamental competente.

9. REQUISITOS ADICIONAIS PARA FUNCIONÁRIOS DETENTORES DE AUTORIZAÇÕES DE NATUREZA CONFIDENCIAL OU ESPECIAL

9.1 Todas as funções identificadas pelo Terceiro com Acesso a informações classificadas como de NATUREZA CONFIDENCIAL ou especial, bem como detentoras de permissões específicas para acessar a infraestrutura que armazena, processa ou transmite informações classificadas como de NATUREZA CONFIDENCIAL ou especial, precisarão ser documentadas na Declaração de NATUREZA CONFIDENCIAL e fornecer à BT a Declaração de NATUREZA CONFIDENCIAL preenchida antes da assinatura do Contrato.

9.2 Nos casos em que o fornecedor precisar acessar, armazenar, processar ou transmitir informações classificadas como de NATUREZA CONFIDENCIAL do HMG ou equivalente, o fornecedor precisará realizar uma avaliação de risco de segurança dos funcionários em todas as funções identificadas no parágrafo 2 da declaração de NATUREZA CONFIDENCIAL, conforme os requisitos definidos no documento sobre Avaliação de Riscos de Segurança de Funcionários da Autoridade Nacional de Segurança Protetora (NPSA) - Guia (4ª edição - junho de 2013 ou versão posterior).

ANEXO 1, APÊNDICE 1 - MODELO DE DECLARAÇÃO DE NATUREZA CONFIDENCIAL

1. Sistemas/Serviços Abrangidos

Liste os sistemas e Serviços que são fornecidos para auxiliar o cliente HMG.

Sistema	Serviço

2. Funções do Terceiro que requerem um nível de autorização de segurança.

Função	Nível de Autorização de Segurança Necessário
* Por exemplo DBA	SC

3. Gerenciamento de Vulnerabilidade

Sistema	Avaliação do tipo de Vulnerabilidade	Frequência

4. Auditoria, Testes e Monitoramento

Os sistemas precisam ser monitorados 24 horas por dia, 7 dias por semana, conforme orientação da BT

ANEXO 2, Lei (de Segurança) das Telecomunicações de 2021 - Código de Conduta dos Requisitos de Segurança para conversão

Numeração do Código	Requisito	Cláusula do Requisito de Segurança da BT
M1.02	Os testes de segurança em sistemas destinados ao exterior, exceto CPE, normalmente são realizados pelo menos a cada dois anos e, em geral, logo após a ocorrência de uma alteração significativa.	17.3
M1.03	Os equipamentos na borda exposta não deverão armazenar dados confidenciais ou funções essenciais relativas à segurança.	17.3
M1.04	É necessário implementar uma separação física e lógica entre a borda exposta e as funções essenciais relativas à segurança. É importante observar que tal medida pode não ser necessária caso os conjuntos de dados e as funções possam ser protegidos por criptografia contra ataques.	17.3
M1.05	É necessário haver limites de segurança entre a borda exposta e as funções essenciais ou confidenciais que implementam medidas de proteção.	17.3
M2.02	Todo acesso prioritário precisará ser registrado.	3.56, 3.57
M2.06	A infraestrutura usada para prestar suporte à rede de determinado fornecedor deve ser de responsabilidade do fornecedor ou de outra entidade que cumpra os regulamentos, além das medidas e da supervisão aplicáveis ao fornecedor (como um fornecedor terceirizado com o qual o fornecedor tenha uma relação contratual). Nos casos em que o fornecedor ou outra entidade responsável cumprir os regulamentos, tal responsabilidade precisará incluir a manutenção da supervisão do gerenciamento dessa infraestrutura (inclusive a verificação das atividades de gerenciamento, dos funcionários com acesso ao gerenciamento e dos processos de gerenciamento).	3.56, 3.57 e 4, 14
M5.05	Os fornecedores deverão realizar uma análise do motivo principal de todos os incidentes relacionados à segurança. Os resultados desta análise devem ser encaminhados a um responsável competente, que pode incluir a direção do fornecedor.	3.36
M6.01	As credenciais não permanentes (por exemplo, autenticação de nome de usuário e senha) devem ser armazenadas em um serviço centralizado com controle de acesso baseado em funções apropriado, o qual precisará estar atualizado de acordo com todas as alterações relevantes nas funções e responsabilidades dentro da organização.	3.44

M6.02	O acesso com privilégio deve ser feito por meio de contas com ID de usuário exclusivo e credenciais de autenticação para cada usuário, que não devem ser compartilhadas.	3.47
M6.04	Todas as contas de usuário com privilégios de acesso devem ter credenciais exclusivas e sólidas por equipamento de rede particular.	3.48
M6.05	As contas padrão e codificadas deverão ser desabilitadas.	16.16
M8.05	Os fornecedores precisarão registrar todos os equipamentos implementados em suas redes e avaliar ativamente, pelo menos uma vez por ano, sua exposição caso o fornecedor terceirizado não possa continuar a prestar suporte a esses equipamentos.	16.16, 16.5
M8.06	Os fornecedores precisarão remover ou alterar as senhas e contas padrão de todos os dispositivos da rede e desativar os protocolos de gerenciamento não criptografados. Nos casos em que os protocolos de gerenciamento não criptografados não puderem ser desabilitados, os fornecedores precisarão restringir e limitar o uso desses protocolos o máximo possível.	16.16 e 17.1
M8.07	Os fornecedores precisarão garantir que todos os registros relevantes relacionados à segurança sejam habilitados em todos os equipamentos de rede e enviados para os sistemas de registro de rede.	16.5
M8.08	Os fornecedores precisarão priorizar as correções essenciais de segurança em detrimento das atualizações de funcionalidade sempre que possível.	14.1 e 16.12
M8.12	Para os cartões SIM convencionais, o fornecedor precisará garantir que os dados confidenciais do SIM sejam protegidos adequadamente durante toda a sua vida útil, tanto pelo fornecedor do cartão SIM quanto pela rede da operadora, uma vez que há risco quanto ao desempenho e a confidencialidade da rede caso essas informações sejam perdidas.	19.1
M8.13	Para cartões SIM convencionais, a confidencialidade, a integridade e a disponibilidade dos dados confidenciais do cartão SIM compartilhados com o fornecedor do cartão SIM precisarão ser protegidas em todos as etapas de sua vida útil.	19.1
M10.04	O processo de gerenciamento de incidentes do fornecedor e o de seus prestadores de serviços terceirizados precisarão prestar auxílio recíproco para a resolução de incidentes.	3.31-3.36
M10.06	O fornecedor precisará definir quais informações serão disponibilizadas a um fornecedor terceirizado, para garantir que seja o mínimo necessário para cumprir sua função. Os fornecedores precisarão controlar essas informações e limitar o acesso de terceiros ao mínimo necessário para cumprir a função profissional.	3.44

M10.09	Nos casos em que os dados da rede ou do usuário deixarem de ser controlados pelo fornecedor, este deverá exigir contratualmente e verificar se os dados estão devidamente protegidos de forma adequada. Tal exigência deverá incluir a avaliação dos controles do fornecedor terceirizado para garantir que os dados do fornecedor estejam visíveis ou acessíveis apenas aos funcionários competentes e em locais adequados.	3.44-3.50 e 14, 15, 17 e 18
M10.11	Os fornecedores precisarão exigir contratualmente que os fornecedores terceirizados notifiquem o fornecedor dentro de 48 horas após tomarem conhecimento de qualquer incidente de segurança que possa ter causado ou contribuído para a ocorrência de um comprometimento da segurança, bem como no caso de identificarem um risco maior de ocorrência de tal problema. Tal notificação inclui, entre outras coisas, incidentes na rede de desenvolvimento do fornecedor ou em sua rede corporativa.	3.33
M10.12	Os fornecedores precisarão exigir contratualmente que os fornecedores terceirizados prestem suporte ao fornecedor durante as investigações de incidentes que possam causar ou contribuir para a ocorrência de um comprometimento da segurança em relação ao fornecedor principal, bem como de um risco maior de ocorrência de tal comprometimento.	3.31-3.36
M10.13	Os fornecedores precisarão exigir contratualmente que os fornecedores terceirizados encontrem e informem a causa raiz de qualquer incidente de segurança que possa resultar em um comprometimento da segurança no Reino Unido no prazo de 30 dias e que corrijam todas as falhas de segurança encontradas.	3.35
M10.16	Os fornecedores precisarão exigir contratualmente que os fornecedores terceirizados auxiliem, conforme apropriado, em quaisquer auditorias, avaliações ou testes de segurança exigidos pelo fornecedor em relação à segurança da própria rede do fornecedor, inclusive aqueles necessários para avaliar os requisitos de segurança deste documento.	5.1-5.2, 6.1-6.3
M10.18	O fornecedor terá o direito de definir as permissões das contas usadas para acessar sua rede por administradores terceirizados.	16.23
M10.21	Os fornecedores precisarão ter o direito previsto em contrato de controlar os membros da equipe do administrador terceirizado que estejam envolvidos na prestação dos serviços do administrador terceirizado, inclusive para exigir que o administrador terceirizado garanta que nenhum membro da equipe tenha mais acesso à rede.	13.1
M10.24	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem controles técnicos para evitar que um fornecedor ou sua rede afetem negativamente qualquer outro fornecedor ou sua rede.	16.13
M10.25	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem uma separação	16.14

	lógica dentro da rede de administradores terceirizados para separar os dados e as redes dos clientes.	
M10.26	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem a separação entre os ambientes de gerenciamento de administradores terceirizados usados para diferentes redes de fornecedores.	16.14
M10.27	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem e executem funções de reforço de segurança no limite entre a rede do administrador terceirizado e a rede do provedor.	16.14
M10.28	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem controles técnicos para diminuir a possibilidade de usuários ou sistemas afetarem negativamente mais de um fornecedor.	16.14
M10.29	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem estações de trabalho de acesso privilegiado que sejam logicamente independentes por fornecedor.	16.14
M10.30	Os fornecedores precisarão exigir contratualmente que os administradores terceirizados implementem domínios e contas administrativas independentes por fornecedor.	16.14
M10.33	O fornecedor precisará exigir contratualmente que o administrador terceirizado monitore e audite as atividades da equipe do administrador terceirizado ao acessar a rede do fornecedor.	3.56, 3.57
M10.34	O fornecedor precisará exigir contratualmente do administrador terceirizado todos os registros relacionados à segurança da rede do administrador terceirizado, conforme esses registros estejam relacionados ao acesso à rede do fornecedor.	3.56, 3.57 e 16.23
M10.35	Os fornecedores precisarão exigir que as redes do administrador terceirizado que possam afetar o fornecedor sejam submetidas ao mesmo nível de testes que o fornecedor realiza internamente (por exemplo, testes TBEST, conforme definido para o provedor pelo Ofcom de forma periódica).	16.18
M10.36	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede compartilhem com eles uma “declaração de segurança” sobre como produzem equipamentos com segurança e como garantem a manutenção da segurança do equipamento durante toda a sua vida útil. Recomenda-se que essa declaração abranja todos os aspectos descritos na Avaliação de Segurança do Fornecedor (VSA) (consulte o Anexo B), na qual os fornecedores devem ser incentivados a publicar uma resposta à VSA.	16.15
M10.38	Os fornecedores precisão garantir, por meio de acordos contratuais, que a declaração de segurança do fornecedor de	16.15

	equipamentos de rede seja assinada de acordo com o nível de governança adequado.	
M10.39	Nos casos em que o fornecedor de equipamentos de rede alegar ter obtido avaliações ou certificações de segurança internacionalmente reconhecidas de seus equipamentos (como Common Criteria ou NESAS), os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos compartilhem com eles os resultados completos que comprovem tal avaliação ou certificação.	16.17
M10.40	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede sigam um padrão não inferior ao da declaração de segurança do fornecedor de equipamentos de rede.	16.16
M10.41	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede forneçam orientações atualizadas sobre como o equipamento deve ser implantado com segurança.	16.16
M10.42	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede ofereçam suporte a todos os equipamentos e a todos os subcomponentes de software e hardware durante a vigência do contrato. Operíodo de suporte do hardware e do software deverá constar no contrato.	16.16
M10.43	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede forneçam detalhes (produto e versão) dos principais componentes e dependências do Terceiro, bem como componentes de código aberto e o período e nível de suporte.	16.16
M10.44	Nos casos em que seja relevante para o uso específico de equipamentos de um fornecedor, os fornecedores precisarão exigir contratualmente que os fornecedores terceirizados corrijam todos os problemas de segurança que representem um risco à segurança da rede ou do serviço de um fornecedor detectados em seus produtos em um prazo considerável após a notificação, além de fornecer atualizações regulares sobre o andamento dos procedimentos realizados até então. Tal medida deverá incluir todos os produtos impactados de acordo com a vulnerabilidade, não apenas o produto para o qual foi reportada a vulnerabilidade.	16.16
M10.46	Os fornecedores precisarão garantir que seus contratos permitam que os detalhes dos problemas de segurança sejam compartilhados, conforme apropriado, para auxiliar na identificação e na redução dos riscos de comprometimento da segurança da rede pública de comunicações eletrônicas ou do serviço público de comunicações eletrônicas como resultado de ações ou omissões de fornecedores terceirizados.	3.33 e 16.19

M10.47	Os fornecedores precisarão exigir contratualmente que os fornecedores de equipamentos de rede forneçam as correções essenciais de segurança separadamente das versões de recursos, para maximizar a velocidade com que a correção pode ser implementada.	14.1 e 16.12
M11.02	Quaisquer credenciais e informações confidenciais existentes (por exemplo, acesso de emergência por parte de pessoas sem direitos de acesso) precisarão ser protegidas e não devem ser disponibilizadas para ninguém, exceto para a(s) pessoa(s) responsável(is) em uma emergência.	3.44
M11.03	O armazenamento central de credenciais permanentes deverá ser protegido através da utilização das ferramentas de hardware. Por exemplo, em um host físico, a unidade pode ser criptografada com o uso de um TPM. Caso uma máquina virtual (VM) seja usada para fornecer um serviço de armazenamento central, essa VM e os dados nela incluídos também deverão ser criptografados, usar inicialização segura e ser configurados para garantir que só possam ser inicializados em um ambiente apropriado. Tal medida visa garantir que os dados não possam ser removidos do ambiente operacional e posteriormente acessados.	3.45
M16.12	Os registros de equipamentos de rede em funções essenciais para a segurança precisarão ser completamente registrados e disponibilizados para auditoria por 13 meses.	3.56, 3.57
M16.21	As indicações de possíveis atividades anômalas devem ser prontamente avaliadas, investigadas e tratadas.	3.56, 3.57
M21.02	As medidas a serem tomadas pelo fornecedor nos termos do Regulamento 3(3)(f) normalmente devem incluir a garantia, até onde seja possível, de que o equipamento que executa as funções de supervisão da rede do fornecedor esteja localizado no Reino Unido e seja operado por uma equipe estabelecida no Reino Unido.	16.21
M21.03	O fornecedor precisará manter uma equipe técnica localizada no Reino Unido para fornecer informações especializadas sobre a operação das redes do fornecedor no Reino Unido e os riscos para as redes do fornecedor no Reino Unido.	16.2, 16.20-16.22
M21.04	Nos casos em que os dados forem armazenados no exterior, o fornecedor precisará manter uma lista dos locais onde os dados são mantidos. O risco decorrente da manutenção dos dados nesses locais, inclusive qualquer risco associado à lei local de proteção de dados, precisará ser gerenciado como parte dos processos de gerenciamento de riscos do fornecedor.	3.8