Normas do Call Centre

Termos Gerais

(A) Os presentes Requisitos devem ler-se em conjunto com a Matriz de Implementação presente no Anexo 1 deste documento, que visa fornecer detalhes sobre os comportamentos e resultados que a BT considerará aceitáveis no que concerne o cumprimento por parte do Fornecedor.

(B) A BT pode realizar avaliações de risco ao centro de atendimento, estando estas contempladas pela secção 3.10 dos Requisitos de Segurança do Fornecedor ("Requisitos de Segurança"), em qualquer altura, antes ou durante a prestação de serviços. Sem prejuízo de quaisquer outros recursos que possam estar disponíveis à BT, esta pode estipular medidas corretivas, normas de compensação e contramedidas a fim de abordar quaisquer riscos e/ou falhas no cumprimento, ou cumprimento insatisfatório, dos Requisitos identificados, que devem ser implementados pelo Fornecedor e documentados como anexo à presente referência; quaisquer custos associados à implementação dos novos requisitos de segurança devem ser acordados entre ambas as partes.

(C) Deve ser adjudicada à BT a revisão de normas e procedimentos do Fornecedor que impliquem quitação dos requisitos da presente referência pertencentes a avaliações de risco realizadas no centro de atendimento. As normas supracitadas podem incluir (mas não estão limitadas a): Normas de utilização de computadores, descarte de equipamentos TI, Autenticação de Clientes, Verificação de Antecedentes Laborais, Avaliação de Riscos e Gestão de Processos, etc.

1. Segurança Física

1.1 O Fornecedor deve assegurar-se de que as áreas do centro de atendimento (ver: Glossário) usadas para a operação das contas da BT/EE estão Fisicamente Separadas das áreas destinadas a outros negócios por meios físicos e específicos de controlo do acesso.

1.2 O Fornecedor deve possuir um processo de acesso auditável e preparado para requisitos de aprovação de novos métodos de acesso físico, ou de remoção dos mesmos, da área do centro de atendimento. [1]

1.3 O Fornecedor deve assegurar-se de que, a fim avaliar os direitos de acesso físico às áreas do centro de atendimento (incluindo movimentações e alterações internas) e de fazer frente aos despedimentos de pessoal, o processo de acesso auditável é revisto a cada 3 (três) meses, sendo a sua data devidamente registada.

1.4 O Fornecedor deve assegurar-se de que não existe trabalho solitário na área do centro de atendimento. Este requisito aplica-se aos funcionários de limpeza e terceiros.

1.5 O Fornecedor deve possuir um processo auditável que previna o *Tailgating* em áreas controladas. O processo deve ser executório e o seu repetido incumprimento deve ter como consequência ações disciplinares.

2. Acreditações de segurança e Visitantes

2.1 O Fornecedor deve assegurar-se de que os funcionários, aos quais é permitido (como parte das suas funções) o uso de telemóveis, computadores portáteis, iPads e/ou *tablets* nas áreas

[1] Ver: Matriz de Implementação para exemplos de processos de acesso auditáveis.

pertencentes ao centro de atendimento, são facilmente reconhecidos pelos restantes funcionários e supervisores.[2]

2.2 O Fornecedor deve possuir um processo auditável preparado para a emissão de Acreditações de Segurança e Acreditações de Segurança Temporárias aos funcionários do centro de atendimento sempre que necessário, que inclui o cancelamento automático dos direitos de acesso sempre que expira o período de tempo para o qual a acreditação foi requisitada.

2.3 O Fornecedor deve assegurar-se de que as Acreditações de Segurança e as fitas que as suportam não identificam o local de trabalho do funcionário.

2.4 O Fornecedor deve assegurar-se de que existe um processo auditável de controlo de visitas publicado e visível por todos os funcionários. Deve existir um registo de visitas, que deve ser guardado como prova.[3]

2.5 As acreditações de segurança entregues aos visitantes devem distingui-los dos funcionários e devem ser retirados quando o visitante sai do centro de atendimento. Todas as acreditações de segurança que não sejam entregues imediatamente devem ser desativadas na manhã seguinte.

2.6 O Fornecedor deve assegurar-se de que todos os visitantes do centro de atendimento são constantemente escoltados e usam crachás e acreditações visíveis.

3. Funcionários

3.1 O Fornecedor deve assegurar-se de que todos os Artigos Pessoais são armazenados em cacifos pessoais, longe da área do centro de atendimento.

3.2 O Fornecedor deve permitir que quaisquer medicamentos/equipamento médico pessoais como, por exemplo, inaladores, insulina ou medicamentos para a tosse, entrem na área do centro de atendimento.

3.3 Excluindo autorização proveniente de avaliações de risco, os funcionários a desempenhar funções dentro da área do centro de atendimento não podem possuir telemóveis ou quaisquer dispositivos móveis, a menos que devidamente autorizados. O Fornecedor deve implementar revistas regulares a fim de garantir que os funcionários não possuem telemóveis ou outros dispositivos móveis a área do centro de atendimento. Deve também expor sinalética que informe a proibição do uso dos dispositivos supracitados. Para além destas medidas, os funcionários devem frequentar programas de formação que tornem esta norma clara e devem ser aplicados processos disciplinares aos casos de incumprimento.

3.4 O Fornecedor deve assegurar-se de que existem meios de os funcionários serem contactados por partes externas em caso de emergência pessoal.[4]

3.5 Deve existir um processo autidável para a autorização e uso de canetas, lápis e papel dentro da área do centro de atendimento. As canetas, lápis e papel não são permitidos, a não ser que o seu uso seja autorizado pelo diretor a fim de que determinado funcionário realize as suas funções.

3.6 O Fornecedor deve assegurar-se de que caso sejam produzidas, como parte das funções de um funcionário, quaisquer notas manuscritas, não sejam abandonadas sem vigilância e sejam armazenadas em local seguro (segundo as normas de tratamento e classificação da

[2] Ver: Matriz de Implementação para exemplos definitórios de "facilmente reconhecidos"
[3] Ver: Matriz de Implementação sobre a informação a constar no registo de visitas
[4] Ver: Matriz de Implementação para exemplos de processos de emergência pessoal

informação) ou eliminadas[5] no final do dia de trabalho, a fim de aplicar normas de "local de trabalho limpo"[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 O Fornecedor deve providenciar quadros brancos e blocos de notas reutilizáveis (incluindo marcadores e panos para apagar) em alternativa às canetas, lápis e papel. Deve também permitir que se tirem notas durante as chamadas. O Fornecedor deve assegurar-se de que as notas são apagadas assim que as questões do cliente sejam resolvidas e que todas as notas sejam apagadas dos quadros brancos no final de cada turno. Os Diretores e supervisores devem percorrer o espaço de trabalho e assegurar-se de que estas medidas são postas em prática.

3.8 O Fornecedor deve assegurar-se de que quaisquer notas temporárias gravadas online ou em quaisquer ferramentas eletrónicas (tiradas a fim de auxiliar a resolução das questões dos clientes) são automaticamente eliminadas no final de cada turno ou no final do dia de trabalho. Tal pode acontecer de forma automática ou, caso contrário, deve manter-se um registo que assegure o cumprimento deste requisito.

3.9 O Fornecedor deve assegurar-se da existência de um processo auditável para o uso de quadros brancos/papel a fim de assegurar:

- Que as notas em papel são devidamente armazenadas ou removidas e eliminadas no final de cada dia de trabalho;
- Que os quadros brancos são limpos no final de cada turno e no final de cada dia de trabalho.[7]

3.10 O Fornecedor deve assegurar-se de que todas as interações com os clientes são gravadas na conta (*memo* ou *notepad* dependendo do sistema utilizado).

3.11 O Fornecedor deve assegurar-se de que não são gravadas em Aplicações do Microsoft Office quaisquer interações com clientes, a não ser que autorizadas em avaliação de risco e como parte das suas funções.

3.12 O Fornecedor deve assegurar-se de que qualquer função que autorize a realização de qualquer uma das seguintes atividades dentro da área do centro de atendimento deve ser sujeita a avaliação de riscos, de acordo com os requisitos descritos na secção 11. As atividades supracitadas podem incluir (mas não estão limitadas a):

- Utilização de Aplicações do Microsoft Office;
- Utilização de dispositivos móveis de trabalho;
- Utilização de computadores portáteis da empresa;
- Utilização de artigos pessoais (conforme definidos no glossário);
- Imprimir ou copiar qualquer informação de clientes;
- Fazer download de gravações de chamadas do(s) servidor(es);
- Acesso a contas de e-mail internas ou externas ou outras ferramentas de comunicação (por exemplo, ferramentas de mensagens instantâneas);

[5] Ver: Matriz de Implementação para exemplos armazenamento seguro e eliminação
[6] Ver: Matriz de Implementação para o que deve ser incluído nas Normas de Local de Trabalho Limpo
[7] Ver: Matriz de Implementação para exemplos do que deve ser incluído no controlo dos quadros brancos/papel

- Utilização de canetas/lápis e papel pata tirar notas;
- Envio de várias mensagens de texto a clientes;
- Acesso remoto ao equipamento do cliente

3.13 O Fornecedor deve assegurar-se de que não é possível enviar várias mensagens de texto (ou uma mensagem de texto a vários clientes), a menos que autorizado e como parte das funções de um funcionário. Caso sejam enviadas mensagens de texto, estas devem ser registadas a fim de demonstrar quando ocorreu o envio, quais as razões do mesmo e quem foram os destinatários.

3.14 O Fornecedor deve assegurar-se de que o download de gravações de chamadas do(s) servidor(es) para computadores fixos/portáteis não é permitido/não é possível, a menos que o funcionário esteja autorizado a tal, como parte das suas funções. Caso o download seja autorizado, deve ser realizado um registo do(s) funcionário(s) com autorização para proceder ao download. Caso sejam realizados downloads de chamadas, devem ser realizados registos que indiquem o motivo para o download e que incluam a gravação em questão. Os consultores autorizados e quaisquer incumprimentos devem ser revistos e validados regularmente.

4. Equipamento

4.1 O Fornecedor deve assegurar-se de que todos os consultores dispõem de ecrãs de computador protegidos, que não são visíveis do exterior da área do centro de atendimento fisicamente separada.[8]

4.2 O Fornecedor deve assegurar-se de que todas as impressoras e faxes estão localizados em áreas seguras, restringidas apenas a pessoal autorizado e são utilizadas unicamente para os propósitos necessários. A lista dos utilizadores autorizados deve ser revista regularmente a fim de manter a sua validade. Quaisquer cópias físicas devem ser armazenadas em segurança, de acordo com as normas de classificação e manuseamento de informação e não devem abandonar o centro de atendimento, a menos que previamente autorizado pela BT.

4.3 O Fornecedor deve assegurar-se de que todas e quaisquer impressões ou cópias requeiram um ID de utilizador e um código de segurança, a fim de que possam ser monitorizadas e registadas para motivos de auditoria.

4.4 O Fornecedor deve assegurar-se e que todas as áreas onde existem impressoras e fazes dispõem de trituradores de papel caixotes de depósito de lixo confidencial. Os trituradores de papel e os caixotes de depósito de lixo confidencial devem ser esvaziados regularmente e o seu conteúdo deve ser eliminado em segurança.

4.5 O Fornecedor deve assegurar-se de que qualquer cópia física de informação deve ser eliminada em segurança, quer por trituração ou em caixotes de depósito de lixo confidencial, de acordo com a secção 4.4.

4.6 O Fornecedor deve assegurar-se de que quaisquer Ativos Físicos atribuídos a quaisquer indivíduos no início do seu trabalho são devolvidos/removidos aquando do término das suas funções na área do centro de atendimento, ou após término do contrato com a BT/EE. Deve manter-se um inventário de todos os Ativos Físicos.[9]

[8] Ver: Matriz de Implementação para exemplos do que constitui um "ecrã de computador protegido"
[9] Ver: Matriz de Implementação para exemplos do que deve ser incluído do inventário de Ativos Físicos

4.7 O Fornecedor deve assegurar-se de que todos os Ativos Físicos que foram devolvidos ou removidos são eliminados em segurança, de acordo com os requisitos de segurança de eliminação.[10]

5. Acesso aos sistemas

5.1 Com a finalidade de proteger os dados dos clientes, todos os consultores devem gravar o seus ID de utilizadores aquando do acesso às contas/dados, bem como deve ser registada a razão de todos os acessos. O acesso só deve ser concedido após aprovação por parte do Proprietário do Sistema ou do diretor de linha. Para além disso, o acesso às contas dos clientes deve apenas ser permitido se requerido para tarefas de consultor e deve ter apenas as permissões mínimas necessárias para que o consultor realize as suas funções. A qualquer pessoa que não necessite de aceder aos sistemas da BT e/ou da EE a fim de ver dados de clientes não deve ser permitido o acesso para quaisquer fins.

5.2 A menos que requisitado para razões operacionais, o acesso para "visualização" deve ser evitado. Todos os acessos de "visualização" autorizados devem ser registados e monitorizados a fim de prevenir usos inapropriados.

5.3 O Fornecedor deve assegurar-se de que os funcionários não estão autorizados a aceder à internet, e-mail pessoal ou e-mail externo, redes sociais (como, por exemplo, o Facebook) ou quaisquer outras ferramentas de comunicação como o *messenger* ou o *communicator,* a menos que autorizado pela BT e seja parte das suas funções.

5.4 O Fornecedor deve assegurar-se de que todas as mensagens são enviadas através dos sistemas dos fornecedores, registadas e monitorizadas. Caso sejam enviadas mensagens de texto, estas devem ser registadas a fim de demonstrar quando ocorreu o envio, quais as razões do mesmo e quem foram os destinatários.

5.5 O Fornecedor deve assegurar-se de que são apenas permitidas ferramentas de acesso remoto pré-aprovadas e cujo seu uso é restringido a funcionários que necessitam das mesmas para o desempenho das suas funções. O acesso deve ser revisto a cada 3 meses e revogado caso não seja necessário. Devem ser implementadas soluções a fim de identificar ferramentas de acesso remoto não aprovadas.[11]

5.6 O Fornecedor não deve permitir o acesso remoto ao email dos funcionários do centro de atendimento, nem a qualquer sistema de registo de dados de clientes.

5.7 O Fornecedor deve assegurar-se de que o acesso de "visualização" dos funcionários é apenas permitido a discos partilhados fornecidos e geridos pela BT e/ou EE. Não devem ser utilizados quaisquer outros discos partilhados no centro de atendimento. Não é permitido o download, cópia ou modificação de informações de clientes de qualquer sistema, *app* ou base de dados da BT e/ou EE.

[10] Ver: Matriz de Implementação para o que deve ser incluído nos requisitos de segurança de eliminação
[11] Ver: Matriz de Implementação para exemplos de comportamentos a identificar e ferramentas de acesso remoto

6. Gravação das chamadas

6.1 O Fornecedor deve assegurar-se de que todas as chamadas são gravadas. O Fornecedor deve assegurar-se de que a gravação das chamadas (voz e ecrã) está protegida durante a sua transmissão do computador fixo para o(s) servidor(es) de gravação de chamadas.[12]

6.2 O Fornecedor deve assegurar-se de que as gravações das chamadas são armazenadas em segurança, particularmente se incluírem Informações de Cartões de Pagamento (ICP), a fim de evitar perdas ou uso inapropriado de dados de clientes. Os dados de ICP devem ser encriptados e devem ser implementados sistemas de gestão de chaves a fim de proteger e garantir as boas-práticas desta empresa. A BT e/ou a EE podem avaliar a encriptação e a proteção do armazenamento dos dados periodicamente, a fim de assegurar que estes são adequados.

7. Autenticação de clientes

7.1 O Fornecedor deve assegurar-se de que está definido e em prática um processo de autenticação de clientes para as chamadas recebidas e efetuadas. [13]

7.2 O Fornecedor deve assegurar-se de que são utilizados números PIN e palavras-passe para que os utilizadores autentiquem a sua identidade e que estes não são visíveis aos restantes funcionários do centro de atendimento através de, por exemplo, a utilização de ecrãs protegidos ou separação física.

7.3 O Fornecedor deve assegurar-se de que a autenticação dos clientes se processa de forma automática, de modo a que o cliente não necessite de revelar o seu número PIN ou palavra-passe ao consultor, por exemplo, através de um pedido gerado automaticamente de dígitos aleatórios da palavra-passe, como, por exemplo, o 1º, 3º e 5º dígitos. A BT e/ou a EE podem avaliar o processo de autenticação de clientes periodicamente, a fim de assegurar que estes cumprem os Requisitos.

7.4 O Fornecedor deve assegurar-se de que, caso o cliente perca o acesso ao seu número PIN ou palavra-passe e necessite de os repor, o processo de reposição não ocorra sem autenticações adicionais.[14]

7.5 O Fornecedor deve assegurar-se de que os sistemas que geram os números PIN e palavras-passe dos clientes são automatizados e não requerem interação por parte dos funcionários do centro de atendimento.

7.6 O Fornecedor deve assegurar-se de que a criação de novos números PIN e palavras-passe é feita por um sistema automatizado e de que os números PIN e palavras-passe novos são enviados diretamente ao cliente por mensagem de texto ou email, sem requerer intervenção por parte de qualquer consultor.

7.7 O Fornecedor deve assegurar-se de que a reposição de números PIN e palavras-passe pode ser feita pelo cliente, quer online ou através de um sistema de *Interactive Voice Response - IVR* (Sistema interativo de resposta por voz).

7.8 O Fornecedor deve assegurar-se de que existe uma área de "reposição de dados assistida", que permite ao cliente repor o número PIN ou a palavra-passe com o auxílio de um funcionário

[12] Ver: Matriz de Implementação para exemplos de como proteger as transmissões das gravações das chamadas.
[13] Ver: Matriz de Implementação para exemplos do que deve envolver o processo de autenticação de clientes.
[14] Ver: Matriz de Implementação para exemplos do que devem envolver autenticações adicionais.

do centro de atendimento. A capacidade de repor números PIN e palavras-passe deve ser restringida a um número limitado de funcionários.[15]

7.9 O Fornecedor deve ser capaz de gerar, quando requisitado, um registo de auditoria revelador de todas reposições de números PIN e palavras-passe, bem como qual o sistema utilizado para a reposição (online, IVR ou reposição assistida por um funcionário) e qual o funcionário envolvido no processo.

8. Privacidade dos dados

Em adição à formação em Proteção e Segurança de Dados obrigatória da BT (ver Anexo 2) que todos os funcionários do Fornecedor devem completar e reconhecer a sua compreensão, devem ser também cumpridos os seguintes requisitos:

8.1 O Fornecedor deve assegurar-se de que os funcionários da área do centro de atendimento têm facilidade de acesso a informação relevante sobre proteção e segurança de dados na página inicial da intranet (ou, caso não tenham acesso a intranet, através de e-mails regulares e formação).

8.2 O Fornecedor deve enviar lembretes, pelo menos duas vezes por ano, a todos os funcionários da área do centro de atendimento, com o intuito de reforçar comportamentos positivos e boas-práticas de segurança.

9. Monitorização

9.1 O Fornecedor deve certificar-se de que são realizados, por parte de supervisores/diretores, controlos de qualidade a uma seleção aleatória de chamadas telefónicas (recebidas e efetuadas), uma vez por semana, de forma a assegurar que o processo de autenticação de clientes se verifica, bem como outros requisitos.[16]

9.2 O Fornecedor deve assegurar-se de que todas as chamadas são classificadas como "contactos falhados" se o processo de autenticação de clientes não for cumprido. Após cada contacto falhado, o Fornecedor deve ter um processo de feedback que recorde os consultores das suas responsabilidades na autenticação correta dos clientes e/ou da confidencialidade das palavras-passe (conforme o caso).

9.3 O Fornecedor deve possuir um processo auditável para o caso de um funcionário do centro de atendimento possuir vários registos de "contactos falhados" e não cumprir corretamente o processo de autenticação de clientes. Este processo deve incluir as consequências para um consultor que não cumpra, de forma recorrente, o processo de autenticação ou o processo de armazenamento de dados corretos, e deve servir de evidência para a gestão do desempenho ou procedimentos disciplinares que envolvam indivíduos relevantes.

10. Cumprimento

10.1 O Fornecedor deve assegurar-se de que existe um processo auditável documentado para levar a cabo verificações de segurança no local, que comprovem o cumprimento dos Requisitos de

[15] Ver: Matriz de Implementação para exemplos do que deve constar numa área de reposição de dados assistida.

[16] Ver: Matriz de Implementação para exemplos dos mínimos necessários no controlo de qualidade

Segurança da BT, como por exemplo, percorrer toda a área do centro de atendimento, local de trabalho limpo, etc.[17]

10.2 O Fornecedor deve implementar um processo que assegure uma avaliação trimestral (baseada em 10% do influxo) aos funcionários do centro de atendimento ou quaisquer outros colaboradores da BT e/ou EE, a fim de assegurar que o processo de seleção de novos funcionários e formação em segurança (como parte do processo de iniciação) são completados e ocorrem de forma eficaz. Serve este processo para assegurar que o historial de todos os funcionários do centro de atendimento foi verificado (de acordo com as normas de admissão da BT) e que estes foram devidamente formados em segurança, para que se confie na proteção adequada dos dados sensíveis dos clientes.

10.3 O Fornecedor deve implementar um processo que assegure uma avaliação trimestral (baseada em 100% do influxo) aos funcionários do centro de atendimento ou quaisquer outros colaboradores da BT e/ou EE, a fim de assegurar que a formação em Proteção e Segurança de Dados foi realizada.

10.4 O Fornecedor deve assegurar-se de que têm lugar trimestralmente reuniões de esclarecimento que abranjam as obrigações dos funcionários em Proteção e Segurança de Dados, e que a participação e entendimento dos mesmos seja devidamente documentada.

10.5 O Fornecedor deve assegurar-se de que as políticas/normas/orientações e processos estão disponíveis a todos os funcionários do centro de atendimento a fim de garantir a conformidade com esta regra e com os Requisitos de Segurança da BT.

11. Avaliação de Riscos

O Fornecedor deve assegurar-se de que quaisquer incumprimentos, autorizações ou exceções específicas a estes requisitos são sujeitos a avaliação de riscos por parte do fornecedor e documentados de acordo com o processo de gestão de risco. A avaliação de risco deve incluir:

- As razões pelas quais a atividade é necessária e porque se justifica o incumprimento destes Requisitos;
- Estado de qualquer incumprimento, por exemplo, permanente ou temporário;
- Caso seja temporário, a data na qual os controlos são implementados e a data na qual se prevê o término da atividade;
- Qual a função/tarefa dos indivíduos e a razão pela qual a atividade é apropriada para esta função (e a razão pela qual são excluídos da necessidade de cumprimento com estes controlos);
- Atenuantes aplicadas a fim de minimizar os riscos inerentes à atividade;
- Justificação para a implementação de determinados controlos e/ou não implementação do(s) controlo(s) necessários;
- Provas de aprovação por parte dos Quadros Superiores.

12. Glossário

Termo	Explicação

[17] Ver: Matriz de Implementação para exemplos do que deve ser incluído nas verificações de segurança no local.

Centro de Atendimento ao Cliente	Um centro de atendimento (também denominado de centro de interação com o cliente ou centro de atendimento eletrónico) é um ponto central de uma empresa, no qual são geridos todos os contactos de clientes. O centro de atendimento inclui geralmente um ou mais call centres online, podendo também incluir outras formas de contacto com clientes, como por exemplo, e-mail, boletins informativos, catálogos por correio, questionários de website, chats e a informação recolhida dos clientes durante as compras em lojas físicas. Um centro de atendimento é geralmente parte do departamento de Gestão de Relacionamento com o Cliente (*Customer Relationship Management*) de uma empresa.
Cacifos Pessoais	Não são permitidos, dentro da área do centro de atendimento, artigos pessoais capazes de gravar informações de clientes como, por exemplo, telemóveis. Estes artigos devem ser guardados nos cacifos pessoais dos funcionários (devidamente assinalados), longe da área do centro de atendimento.
Funcionário(s) / funcionário(s)	O termo "funcionário" aplica-se a qualquer individuo que trabalhe na área do centro de atendimento e aos funcionários temporários do Fornecedor, colaboradores da agência, empresas contratadas e os seus trabalhadores.
Escoltado	Deve existir um processo formal de visitantes que garanta, no mínimo, que todas as visitas ao centro de atendimento são constantemente escoltadas, de forma a que ninguém se perca ou entre em áreas restritas.
Matriz de Implementação	A matriz anexada estabelece, como mínimos, os resultados e normas que o Fornecedor deve atingir e cumprir aquando da implementação de determinados processos, políticas ou procedimentos referidos nos Requisitos.
Trabalho solitário	Deve existir um processo que assegure que nenhum individuo trabalhe na área do centro de atendimento, fora do horário de expediente, sem autorização da gerência. Esta norma aplica-se também a funcionários de limpeza ou indivíduos externos à empresa como, por exemplo, equipas de manutenção.
Aplicações do Microsoft Office	As Aplicações do Microsoft Office incluem, mas não estão limitadas a, Word, PowerPoint, Excel, Outlook e OneNote. A fim de evitar a fuga de dados, as interações com clientes que envolvam sistemas online não devem ser registadas nestas aplicações (a não ser que o seu registo seja autorizado) por se verificar fácil copiar e extrair as informações nelas contidas.
Artigos Pessoais	Qualquer artigo pessoal capaz de registar/gravar informações de clientes - incluindo, mas não estando limitado a: telemóveis, *smart watches*, iPods, iPads, câmaras, USB *flash drives*, canetas e papel.
Controlos do Acesso Físico	Os tipos de controlos do acesso físico a utilizar dependem da área onde o centro de atendimento está localizado. Os controlos do acesso físico podem ser técnicos (por exemplo, cartão de banda magnética, teclado numérico, controlo biométrico), ou processuais (por exemplo, chaves com processo auditável de saída ou um processo de controlo de entradas com um funcionário que controla o acesso e verifica ID), contudo, os controlos do acesso físico a utilizar devem ser apropriados para a área em questão.
Ativo Físico	Para os propósitos do presente documento, ativo físico refere-se a qualquer ativo capaz de processar ou armazenar dados ou informações de clientes.

Fisicamente Separado	Para os propósitos do presente documento, fisicamente separado implica que as conversações não possam ser escutadas e que a informação não possa ser vista a partir de outras áreas de negócios. Deve ser implementada uma barreira física (paredes, edifícios separados, etc.) com controlos do acesso físico à entrada da área segregada.
Incidente de segurança	Um incidente de segurança é uma alteração ao exercício do centro de atendimento ao cliente que impacte a confidencialidade, integridade, disponibilidade ou ativos de informação, indicando uma possível quebra nas políticas de segurança ou nas normas/requisitos de segurança ou uma falha num dispositivo de segurança. Alguns exemplos: Uso indevido do sistema, acesso não autorizado, equipamento perdido/roubado e infeção por *malware*.
Aprovação por parte dos Quadros Superiores.	Quando é necessário concordar numa exceção aos presentes requisitos, as circunstancias devem ser submetidas a uma avaliação de risco, e o autorizador deve ser alguém com responsabilidades de direção na área funcional e com a autoridade necessária.
Proprietário do Sistema	Refere-se ao funcionário responsável pela aquisição geral, desenvolvimento, integração, modificação ou operação e manutenção de um sistema de informação.
Tailgating	Tailgating refere-se à pratica de seguir outro individuo a fim de entrar numa área controlada, ou permitir a entrada na mesma a um individuo não autorizado, através de uma porta/barreira de controlo; não usar o passe de segurança para entrar numa área autorizada das instalações que o fornecedor utiliza para gerir os contactos da BT/EE.
Acreditações de Segurança Temporárias	Estes passes devem ser atribuídos através de um processo auditável (como, por exemplo, um livro de registos ou uma folha de cálculo), e devem comportar um registo de todas as acreditações de segurança temporárias atribuídas, a data da atribuição, o nome do departamento, o número de contacto, a razão da atribuição, bem como o nome do recipiente e a data da devolução do passe. Deve existir um processo para dar resposta aos casos em que o passe não é devolvido.
ID de utilizador	As impressoras e faxes localizadas na área do centro de atendimento devem requerer que os seus utilizadores introduzam um ID e um código de segurança, a fim de monitorizar o uso individual de cada utilizador. Para além disso, os utilizadores devem introduzir este ID quando acedem às contas/registo de clientes, em conformidade com a secção 5.1.

PROJETO KITE: Matriz de Implementação para os Requisitos ao Fornecedor do centro de atendimento.

Referências	Descrição Geral	Resultados mínimos esperados.
1.2	Processo de Acesso Auditável	Uma folha de cálculo ou registo de dados de nomes, incluindo detalhes de quando o acesso foi concedido, a razão do acesso, data do cancelamento do acesso e as razões do mesmo.
2.1	Facilmente Reconhecido	Funcionários aos quais é permitido o uso de telemóveis, computadores portáteis, iPads e *tablets* para o desempenho das suas funções devem ser facilmente reconhecidos através de métodos como, por exemplo, fitas de suporte de Acreditações de Segurança de cor diferente ou outros métodos de distinção.
2.4	Registos de visitas	Deve ser registada a seguinte informação: i) nome do indivíduo, ii) entidade de onde vem, iii) data e hora de entrada e de saída, iv) motivo da visita, v) nome da pessoa que vem visitar, vi) matrícula de qualquer veículo trazido ao local, vii) número de telemóvel, viii) número do passe de visitante.
3.5	Emergência Pessoal	Deve existir um sistema que permita que a família ou amigos de um funcionário entrem em contacto com o mesmo em casos de emergência pessoal. O contacto pode ser feito através de um número de telefone dedicado ou do número de um supervisor usado como ponto central de contacto.
3.7	Armazenamento e Eliminação Seguros	Os sistemas de armazenamento e eliminação seguros de notas produzidas por um funcionário como parte das suas funções incluem, mas não estão limitados, ao uso de trituradores de papel, caixotes de lixo de informação confidencial (potencialmente trancados) e/ou armazenamento em instalações seguras e trancadas por funcionários.
3.7	Norma de Local de Trabalho Limpo	Todos os materiais devem ser Armazenados ou Eliminados em segurança imediatamente após o seu uso. Não devem ser deixados materiais nas secretárias no final do dia de trabalho. Devem ser feitas vistorias aos funcionários no local e deve existir um processo disciplinar capaz de lidar com o incumprimento desta norma.

3.10	Auditoria a Quadros Brancos/Papel	De acordo com a secção 3, deve ser mantido um registo (na forma de uma folha de cálculo) que demonstre que as vistorias ao local são realizadas e que o cumprimento deste requisito se verifica.
4.1	Ecrãs de Computados Protegidos	Não deve ser possível ver os ecrãs dos consultores a partir do centro de atendimento e a informação neles constante não deve poder ser lida por pessoal não autorizado presente na área do centro de atendimento (como, por exemplo, funcionários da limpeza e técnicos de manutenção). Os dados dos clientes nos ecrãs dos funcionários devem ser mantidos ocultos através do posicionamento dos monitores ou do uso de *privacy screens*.
4.6	Inventário de Ativos Físicos	O inventário de Ativos Físicos atribuídos a quaisquer indivíduos como, por exemplo, acreditações de segurança, chaves de cacifos, computadores fixos ou códigos de acesso remoto, deve ser armazenado por motivos de auditoria. Quando um consultor termina o seu contrato ou é removido do centro de atendimento, deve ser implementado um processo que garanta que entram em vigor medidas imediatas de remoção de todos os meios de acesso lógicos e físicos e recuperação de todos e quaisquer Ativos Físicos, chaves, e acreditações de segurança. Tal deve constar no processo de despedimento, à data da conclusão do contrato.
4.7	Requisitos de Eliminação Segura	Quando são eliminados Ativos Físicos no final da sua vida útil, devem ser utilizados softwares como o "Tabernus" ou "Blanco" que garantam a eliminação permanente de quaisquer informações confidenciais de clientes. Esta eliminação permanente deve satisfazer os requisitos aprovados pela BT e/ou EE. Caso a eliminação dos dados não se revele possível através dos métodos supracitados, o equipamento deve ser submetido a uma destruição segura, utilizando um processo aprovado pela BT e/ou pela EE. A BT e/ou a EE podem fornecer assistência adicional nesta área. Uma vez que as informações confidenciais de clientes tenham sido eliminadas, os Ativos Físicos podem ser reutilizados ou eliminados, conforme for apropriado.
5.5	Ferramentas de Acesso Remoto	A fim de evitar acessos não autorizados aos dados de clientes, deve ser implementado um processo que garanta que apenas ferramentas de acesso remoto aprovadas pela BT e/ou pela EE são capazes de aceder aos dispositivos dos clientes. Devem ser implementadas soluções a fim de identificar ferramentas de acesso remoto não aprovadas. Estas soluções devem ser revistas regularmente a fim de garantir que não foram/não podem ser utilizadas ferramentas não aprovadas. Ademais, o uso de ferramentas de acesso aprovadas deve ser restringido apenas a indivíduos autorizados, e esta autorização deve apenas ser obtida através de um

		processo formal, que englobe uma avaliação de risco para a necessidade de acesso remoto.
6.1	Transmissão da Gravação das Chamadas	É essencial que se proceda à encriptação da transmissão da gravação das chamadas dos clientes dos computadores para os servidores de gravação, sendo que esta encriptação deve incluir voz e os detalhes do ecrã.
7.1	Autenticação de Clientes	Todos os consultores devem seguir o processo de autenticação de clientes aprovado pela BT/EE a fim de assegurar que o cliente é, de facto, quem afirma ser. Este processo ficará claro para os Fornecedores e consultores, e pode diferir consoante a(s) função(ões) que o centro de atendimento desempenha.
7.4	Verificações de Autenticação Adicionais	Os consultores devem assegurar-se de que, antes de procederem à alteração do número PIN ou palavra-passe de um cliente, adquirem informações suficientes sobre o cliente a fim de se certificarem da sua identidade. Este processo deve ser realizado através de perguntas de segurança sobre a sua identidade, nome, morada, atividade recente da conta, valor da última fatura ou há quanto tempo são clientes da BT ou EE. Estes são, contudo, apenas exemplos, não sendo esta lista exaustiva.
7.8	Assistência de Reposição por Funcionários	A fim de auxiliar os clientes que não se mostram capazes de repor o seu número PIN ou a sua palavra-passe online ou com recurso a IVR, esta reposição deve ser possível com recurso à assistência de um funcionário do call centre. Contudo, deve existir um processo formal que se assegure de que as instalações nas quais é feita a reposição são restringidas a um número limitado de funcionários, e devem ser tomadas medidas que assegurem que estes funcionários estão fisicamente separados dos restantes funcionários do centro de atendimento, com os devidos controlos ativos. A lista dos funcionários autorizados deve ser revista regularmente a fim de garantir que esta autorização é requisitada e está a ser utilizada com a devida descrição.
9.1	Verificação da Monitorização da Qualidade das Chamadas	Os diretores devem realizar controlos de qualidade, incluindo a monitorização semanal de chamadas aleatórias de clientes (realizadas e efetuadas) tratadas pelos consultores, bem como uma revisão mensal de todos os registos e processos implementados pelo Fornecedor. Tal deve servir para assegurar que o Fornecedor cumpre com estes Requisitos e, em particular, que os funcionários estão

		a utilizar um processo de autenticação de clientes correto e a manter os devidos registos.
10.1	Cumprimento das Vistorias	Deve ser implementado um processo auditável que leve a cabo e gira o cumprimento das normas de segurança e o cumprimento das vistorias a todos os Requisitos. Para além da obrigação, por parte do Fornecedor, em realizar todas estas vistorias, também a BT e/ou a EE podem realizar vistorias em qualquer altura. As vistorias podem incluir, mas não estão limitas a: • ID de Segurança / Acreditação de Segurança • Local de trabalho limpo/ecrã limpo • Uso de cacifos pessoais • Dispositivos móveis pessoais • Uso de quadros brancos • Remoção e eliminação de informação confidencial impressa ou enviada por faxe • Autenticação de clientes • Verificação da Monitorização da Qualidade das Chamadas • Registo das auditorias de reposição de palavras-passe • Uso de mensagens de texto • Cumprimento com a formação em segurança e proteção de dados Todas as auditorias às vistorias devem incluir detalhes de todas as ações a levar a cabo em caso de discrepâncias ou incumprimentos. Quaisquer medidas corretivas requisitadas por parte da BT e/ou EE devem ser aplicadas.