Operações Bancárias Online – Contrato de utilização – Empresas e ENI

Sucursal	Código

Informação de contas

Conta de depósitos à ordem de suporte: ☐☐☐☐☐☐☐☐☐☐☐☐

Forma de obrigar a Empresa:
- ☐ Uma assinatura
- ☐ Duas ou mais assinaturas

Regras de autorização de operações:
- ☐ *Standard* (são **regras pré-definidas** destinadas a facilitar o processo de adesão)
- ☐ Personalizáveis (obriga ao preenchimento do anexo de regras)

Nota: Ao abrigo das regras *standard* a movimentação de fundos poderá ser efetuada com uma ou mais assinaturas, consoante a forma de obrigar da Empresa / Empresário implique uma ou mais assinaturas, respetivamente, com um limite por movimento de € 50.000. As assinaturas necessárias correspondem a utilizadores recenseados com capacidade para movimentar fundos e administrar o serviço. Ao escolher regras *standard*, o perfil dos utilizadores fica limitado às seguintes opções: acesso a todos os serviços (consultas, movimentação e administração do serviço), consultas e preparação de operações, ou só consultas. Se estas regras e perfis não se adequarem às suas necessidades poderá optar por regras personalizadas, caso em que deverá preencher e entregar o correspondente anexo ao Banco, junto com o contrato e o perfil dos utilizadores.

Identificação da Empresa / Empresário em Nome Individual

Cliente (Denominação Social): _____

N.º Contribuinte: ☐☐☐☐☐☐☐☐☐ Capital Social: _____Euros

Sede: _____

Matriculado na Conservatória do Registo Comercial de _____ Sob o n.º_____

E-mail: _____ @ _____

Responsáveis que obrigam a Empresa / Empresário em Nome Individual

Nome: _____ N.º Fiscal: ☐☐☐☐☐☐☐☐☐

Nome: _____ N.º Fiscal: ☐☐☐☐☐☐☐☐☐

Nome: _____ N.º Fiscal: ☐☐☐☐☐☐☐☐☐

Nome: _____ N.º Fiscal: ☐☐☐☐☐☐☐☐☐

Nome: _____ N.º Fiscal: ☐☐☐☐☐☐☐☐☐

Códigos para recenseamento de utilizadores (A preencher pelo Banco)

Número Identificação: ☐☐☐☐☐☐☐☐ Código de Adesão: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Mod. 10052092

Cláusula 1.ª: Âmbito

1. Ao subscrever/aceitar o presente Contrato, o Cliente adere às presentes Condições Gerais de utilização dos meios de comunicação à distância do Banco.
2. Para efeitos do disposto no presente Contrato, consideram- se meios de comunicação à distância entre o Banco e o Cliente, os seguintes canais de comunicação remota:
   a) Canal Internet – meio de acesso do Cliente ao Banco através do sítio de Internet www.millenniumbcp.pt;
   b) Canal Mobile - meio de acesso do Cliente ao Banco através do serviço Mobile App;
   c) Canal Telefonia Vocal, mais adiante designado por Centro de Contactos quando envolva um serviço de call center – meio de comunicação por telefone estabelecido por iniciativa do Banco ou do Cliente, incluindo os contactos telefónicos estabelecidos através do Centro de Contactos (comunicações associadas ao número telefónico 707504504 (chamada nacional) e +351210042424 (chamada internacional) ou outros números que os venham a substituir e divulgados pelo Banco.
3. Os meios de comunicação à distância são canais de comunicação remota de acesso do Cliente aos serviços que em cada momento o Banco tenha disponíveis para oferecer nesses canais, para a outorga de atos ou negócios jurídicos no âmbito da relação bancária estabelecida com o Banco, na sua qualidade de instituição de crédito e de agente de seguros, permitindo o acesso à conta de depósitos à ordem para consulta, obtenção de informações e realização de operações, bem como a divulgação e comercialização pelo Banco, e contratação à distância, de produtos e serviços financeiros, incluindo os relativos a serviços de pagamento, valores mobiliários e seguros.
4. Para efeitos do disposto no número anterior, consideram-se atos ou negócios jurídicos outorgados no âmbito da relação bancária e que poderão estar disponíveis para acesso remoto pelo Cliente, todos os que respeitam aos processos de abertura, manutenção e encerramento de contas de depósitos à ordem, incluindo a atualização de dados do Cliente e dos seus representantes e o cumprimento de deveres de identificação e diligência, de serviços de pagamento, de crédito ou de registo e depósito de instrumentos financeiros, à movimentação das referidas contas, bem como aos processos de celebração e de execução de contratos de seguros do ramo Vida e Não Vida e a gestão de sinistros, incluindo, designadamente, a realização de operações sobre seguros, a apresentação de reclamações ou pedidos diversos, a apresentação de pedidos de declarações, de pedidos de informação, de pedidos de segundas vias de extratos ou de outros documentos, a subscrição de contratos de utilização de instrumentos de pagamento, a pedidos de códigos de acesso ou de utilização de serviços de Internet ou de instrumentos de pagamento, a celebração de contratos de acquiring e requisição de TPA (Terminais de Pagamento Automático), a contratação de débitos diretos, a contratação de serviços de envio de fundos, a emissão e revogação de ordens de pagamento, incluindo de ordens permanentes ou periódicas, a emissão de ordens sobre instrumentos financeiros, a subscrição e resgate de produtos de investimento de retalho e de produtos de investimento com base em seguros, a requisição de cheques, a constituição, reforço ou liquidação de depósitos a prazo, a contratação e resolução de alugueres de cofres, a contratação ou gestão de operações de crédito, leasing, factoring, confirming, créditos e remessas documentárias, a emissão de garantias.
5. Pelos meios de comunicação à distância o Cliente poderá ainda solicitar a aquisição de produtos e serviços com terceiras entidades, nos termos do acordo celebrado entre estas e o Banco.
6. Todos os contratos celebrados através de meios de comunicação à distância ficam subordinados às presentes cláusulas, bem como ao disposto nos Documentos "Perfil de Utilizador", e, se for o caso, "Regras para Autorização de Operações", e às condições gerais e particulares aplicáveis à contratação de cada produto ou serviço concretamente disponibilizado, assim como ao tarifário em vigor no Preçário do Banco, legislação aplicável e usos bancários em geral.
7. A prestação de serviços através de meios de comunicação à distância rege-se também, em tudo o que aqui não se encontra especificamente previsto, pelo disposto nas cláusulas do precedente Capítulo A - Condições Gerais de Contas de Depósitos à Ordem e do antecedente Capitulo B - Condições Gerais de Prestação de Serviços de Pagamento, que aqui se dão por inteiramente reproduzidas para todos os efeitos.

Cláusula 2.ª: Riscos associados aos meios de comunicação à distância

1. Os meios de comunicação à distância para acesso do Cliente ao Banco estão sujeitos a riscos de fraude por terceiros, nomeadamente de "phishing", bem como, de consulta e realização de operações fraudulentas por terceiros não autorizados na conta do Cliente.
2. O "phishing" é uma fraude que consiste em substituir a identidade do Banco ou de qualquer outra entidade fidedigna, e cuja finalidade é a obtenção de informações confidenciais do Cliente, nomeadamente dados bancários, dados pessoais ou códigos de acesso. Os ataques de "phishing" podem produzir- se através de mensagens de correio eletrónico, SMS ou chamadas telefónicas nas quais se pode imitar e substituir a identidade do Banco ou de qualquer outra entidade fidedigna. Essas mensagens de correio eletrónico ou SMS podem conter um ficheiro anexo que efetua a instalação de software malicioso (malware) no equipamento do Cliente ou reencaminhar para uma página web fraudulenta, que reproduz ou copia o aspeto da página original do Banco, e na qual é solicitado ao Cliente a introdução de dados pessoais e/ou códigos acesso, como por exemplo, o Código de Utilizador, a Password e/ou (todas) as posições do Código de Acesso Multicanal, o Código de Autenticação, o número de telemóvel ou os números dos cartões bancários.
3. O Cliente deve estar atento, ser precavido e ter em conta que tanto a(s) mensagem de correio eletrónico ou SMS, como a página web fraudulenta, podem ser muito complexas e sofisticadas. O Cliente tem de desconfiar e suspeitar, nomeadamente:
   a) do tom de urgência de mensagens que o ameacem com a suspensão do acesso à conta, dos códigos de acesso ou do cartão se não fornecer os seus dados imediatamente;
   b) do pedido de confirmação dos seus dados pessoais via correio eletrónico ou SMS, designadamente remetendo-o para o preenchimento on-line de formulários de informações pessoais e de códigos de acesso;
   c) de erros ortográficos/gramaticais e outros erros patentes na mensagem ou na página web fraudulenta, ou outros elementos que sugiram a origem diversa ou suspeita dos mesmos;
   d) de mensagens de correio eletrónico ou SMS com links ou ficheiros em anexo;
   e) da indicação de que, deve fornecer Código(s) de Autorização que o Banco lhe enviou por SMS ou gerados via Token, para simular operações;
4. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição das fraudes comuns nesse período para a captura

Mod. 10052092

fraudulenta do Código de Utilizador, Password/ Código de Acesso Multicanal e demais credenciais personalizadas de acesso dos Clientes.

5. O Banco é responsável por assegurar a fiabilidade da sua página de Internet e serviços de Mobile Banking, bem como a segurança dos seus servidores e componentes informáticos.
6. O Cliente é responsável pela segurança e fiabilidade do equipamento informático e de comunicação utilizado para acesso ao Banco através dos meios de comunicação à distância, nomeadamente dos computadores, tablets, telemóveis, números de telemóvel, e ligações à Internet de sua propriedade ou sob sua alçada, nos termos do disposto nos números seguintes e nas recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra.
7. O Cliente deverá dispor de equipamento informático e de comunicação com as características adequadas para poder aceder ao Banco através dos meios de comunicação à distância, sendo da sua responsabilidade a segurança, manutenção e introdução das modificações eventualmente necessárias para assegurar em permanência o acesso, por essa via, ao Banco, de acordo com as inovações e alterações tecnológicas que vierem a ser introduzidas e o cumprimento rigoroso das regras e recomendações de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra, bem como, dos alertas divulgados pelo Banco, em cada momento, no sítio de Internet www.millenniumbcp.pt.
8. As características mínimas, de equipamento e comunicações, em cada momento necessárias para a utilização de cada meio de comunicação à distância, encontram-se descritas no sítio de Internet www.millenniumbcp.pt, nos espaços informativos de cada canal, que o Cliente se obriga a ir consultar periodicamente e a observar escrupulosamente.

Cláusula 3.ª: Utilizadores

1. A ativação do acesso do Cliente aos meios de comunicação à distância só será efetuada após receção e validação pelo Banco do Documento "Perfil de Utilizador", e, sempre que requerido, do Documento "Regras para Autorização de Operações", todos devidamente preenchidos e assinados pelos representantes com poderes bastantes para vincular o Cliente, o(s) qual(is) fica(m) a fazer parte integrante do presente acordo para todos os efeitos.
2. O(s) Utilizador(es) é(são) a(s) pessoa(s) singulares designada(s) pelo Cliente no Documento "Perfil de Utilizador", e que nos termos aí estabelecidos poderão aceder ao Banco, através dos meios de comunicação à distância, e em nome e representação do Cliente realizar determinadas operações, designadamente de consulta e/ou movimentação de conta(s) do Cliente, de acordo com o âmbito dos poderes respectivamente atribuídos e definidos pelo Cliente para cada Utilizador.
3. Por regra, o(s) Utilizador(es) é(são) a(s) pessoa(s) singulares designada(s) pelo Cliente na Ficha de Assinaturas de acordo com as regras de movimentação e de autorização de operações aí convencionadas para a respectiva conta de depósito do Cliente, salvo instruções diversas estabelecidas pelo Cliente no Documento "Regras para Autorização de Operações" e aceites pelo Banco.
4. Sem embargo do que precede, no Documento "Perfil de Utilizador" o Cliente designa o(s) Utilizador(es), e estabelece, para cada Utilizador, o respectivo perfil, isto é, o âmbito dos poderes que lhe atribui, indicando nomeadamente o(s) serviços/funções a que o mesmo terá acesso, tipo de assinatura digital e quais a(s) conta(s)s do Cliente a visualizar / movimentar pelo mesmo.
5. No Documento "Regras para Autorização de Operações", o Cliente poderá ainda estabelecer adicionais regras para autorização de operações pelo(s) Utilizador(es), designadamente o número e tipo de assinaturas digitais necessárias para autorizar as operações, bem como, escalões de montantes para as operações a realizar.
6. É da inteira e exclusiva responsabilidade do Cliente a selecção, nomeação, e a revogação e cancelamento dos seus Utilizadores, os quais poderão ser, ou não, colaboradores do Cliente, bem como a definição do respectivo Perfil de Utilizador, com o estabelecimento dos respetivos poderes de atuação neste âmbito.
7. O Cliente expressamente reconhece e aceita que o acesso e a utilização, pelos Utilizadores, dos meios de comunicação à distância do Banco, bem como a contratação, pelos mesmos, de operações com o Banco nos termos ora estabelecidos, será sempre, em qualquer caso e para todos os efeitos, uma atuação em representação e por conta do Cliente, que é sempre a única contraparte do Banco. Do mesmo modo, sempre que o Cliente seja instituição financeira, desempenhando funções de intermediação bancária ou financeira, fica bem entendido que o acesso e a utilização, pelos Utilizadores, dos meios de comunicação à distância do Banco, bem como a contratação, pelos mesmos, de operações com o Banco nos termos ora estabelecidos, é sempre, em qualquer caso e para todos os efeitos legais, uma atuação em representação e por conta do Cliente, que é sempre a única contraparte do Banco.
8. O Cliente é inteiramente responsável perante o Banco pelos actos dos seus representantes legais e dos seus Utilizadores praticados no acesso e na utilização dos meios de comunicação à distância, segundo o disposto no número um do artigo 800º do Código Civil.
9. Para a realização de transferências e demais operações que envolvam movimentação de fundos, o Cliente poderá personalizar regras para autorização de operações através de combinações de tipos de assinatura digital (A, B, C ou E) com um máximo de 5 combinações. Todas as operações que impliquem movimentação de fundos só serão executadas se forem cumpridos os requisitos em termos de montantes e de combinações de assinaturas digitais definidos pelo Cliente e previamente aceites pelo Banco.
10. O Cliente deverá atribuir no máximo até três Utilizadores a responsabilidade pela gestão do acesso ao serviço de meios de comunicação à distância, ou seja, designá-lo(s) como Administradores do Serviço. Caberá ao(s) assim designado(s) Administrador(es) do Serviço, em exclusivo, as funções de: alterar contas e serviços/funcionalidades a que cada Utilizador tem acesso, e estado (suspenso/reativado ou cancelado) de cada Utilizador. Não é permitido ao Administrador do Serviço efetuar alterações ao seu próprio perfil, bem como aos demais Administradores do Serviço, devendo neste caso proceder- se a um novo recenseamento mediante novo preenchimento, subscrição e entrega do Documento "Perfil de Utilizador".
11. As alterações decorrentes do ponto anterior efetuadas pelos Administradores do Serviço tornam-se efetivas após concluído o respetivo processo de autorização por assinatura eletrónica.
12. O Cliente poderá proceder à designação de novos Utilizadores, efetuando a sua identificação e recenseamento e enviando ao Banco o(s) Documento(s) – Perfil de Utilizador - devidamente preenchidos e assinados pelos representantes com poderes bastantes para vincular o Cliente. Sem embargo, o Administrador do Serviço terá poderes para substabelecer em Utilizadores com capacidade para efetuar consultas e preparar operações, mas obedecendo às regras de autorização de operações que sejam definidas pelo Cliente para esse efeito.
13. Por razões de segurança, o Banco fica autorizado a proceder à eliminação de Utilizadores que há mais de um ano não acedam aos serviços, competindo ao Cliente assegurar e acautelar os Utilizadores necessários para manter o serviço operacional. Os Utilizadores eliminados poderão ser recuperados a pedido de um Administrador do Serviço ou pelo Cliente.
14. O Cliente poderá a todo o momento, segundo o seu livre critério, ordenar ao Banco que suspenda/ retire a certo(s) Utilizador(es) a possibilidade de acesso e utilização dos meios de comunicação à distância. Aquando da receção desta comunicação por

telefone, o Banco suspenderá de imediato o acesso e utilização dos meios de comunicação à distância pelo(s) Utilizador(es) designado(s), e procederá à eliminação do(s) mesmo(s) somente após a receção da respetiva confirmação escrita do Cliente.

15. No caso previsto no número precedente, o Banco eliminará o acesso do(s) Utilizador(es) durante o primeiro dia útil de funcionamento bancário seguinte ao da receção da comunicação escrita ali prevista.
16. O Banco, por sua iniciativa, efetuará a eliminação de Utilizadores perante a comprovação documental de alterações estatutárias, caducidade dos mandatos, renúncia ou impedimento definitivo para o exercício das respetivas funções.

Cláusula 4.ª: Open Banking

1. Fica expressamente convencionado e aceite que, em conformidade com o disposto na Diretiva (UE) 2015/2366 de 25.03.2015 e nas disposições legais que a regulamentam e transpõem, o Banco, na sua qualidade de prestador de serviços de pagamento do Cliente, está obrigado a disponibilizar o acesso à conta(s) de pagamento do Cliente junto do Banco a terceiras partes (*third-party providers*) sem necessidade de existir qualquer relação contratual entre estas e o Banco e desde que o Cliente ofereça o seu consentimento, para efeitos da prestação do serviço de informação sobre contas, e do serviço de iniciação de pagamentos e confirmação da disponibilidade de fundos, melhor descritos no ANEXO 2 - OPEN BANKING, que aqui consta infra e faz parte integrante do presente acordo.
2. No Documento "Perfil de Utilizador" o Cliente pode, se assim o entender, optar por conferir poderes para o serviço Open Banking ao(s) Utilizador. A gestão do serviço Open Banking é efetuada pelo(s) Utilizador(es) a quem o Cliente tenha conferido poderes para o efeito.
3. A iniciação de pagamentos através de terceiras partes (third- party providers) tem como montantes máximos por transação os definidos na Ficha de Assinaturas de acordo com as regras de autorização de operações aí convencionadas para a respectiva conta de depósito do Cliente, salvo instruções diversas estabelecidas pelo Cliente no Documento "Regras para Autorização de Operações" e aceites pelo Banco.
4. O Cliente é exclusivamente responsável pelo consentimento que conceda a terceiras partes (third-party providers) para efeitos de acesso por estes à(s) conta(s) do Cliente junto do Banco, no âmbito do serviço de informação sobre contas e do serviço de iniciação de pagamentos e confirmação da disponibilidade de fundos.

Cláusula 5. ª: Mobile App

1. No Documento "Perfil de Utilizador", o Cliente pode, se assim o entender, optar por conferir ao(s) Utilizador(es) poderes para acesso e utilização em nome e representação do Cliente do serviço Mobile App, de entre os canais disponíveis dos meios de comunicação à distância do Banco, na opção "Nível de acesso a Serviços".
2. Nesse caso, a gestão do serviço Mobile App é efetuada pelo(s) Utilizador(es) a quem o Cliente tenha conferido o acesso ao serviço Mobile App, através da opção "Gestão de Utilizadores" no sítio de Internet www.millenniumbcp.pt. Designadamente, o Utilizador com acesso autorizado ao Serviço Mobile App poderá definir/alterar um montante máximo por transação que funcionará como limite de segurança adicional no Canal Mobile, mas sem prejuízo das regras estabelecidos pelo Cliente no Documento "Regras para Autorização de Operações", as quais prevalecem.
3. O serviço Mobile App pode ser utilizado em diversos equipamentos. No processo de instalação do serviço num novo equipamento pode ser atribuído um novo Código de Utilizador exclusivo para esse equipamento e que mantém as mesmas condições inicialmente definidas para o serviço Mobile App. Independentemente da utilização do serviço Mobile App em diversos equipamentos o limite definido para a realização de operações não é cumulativo.

Cláusula 6.ª: Códigos para Autenticação do Cliente

1. O acesso e utilização dos meios de comunicação à distância do Banco, nos termos previstos nas presentes Condições Gerais de Meios de Comunicação à Distância implica a correta utilização de um conjunto de Códigos ou Dados de Autenticação nos termos ora estabelecidos e no ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo.
2. A cada Utilizador serão atribuídos um Código de Utilizador e um código pessoal secreto – Password/Código de Acesso (Multicanal) – indispensáveis para aceder aos canais Internet e Mobile.
3. O Cliente poderá ainda recorrer a Certificado(s) Digital(ais) para acesso e utilização do Canal Internet. Para este efeito, o Banco disponibiliza gratuitamente certificados digitais, até ao máximo de 5, válidos por 1 ano, que possibilitam efetuar 5 adesões de Utilizadores do Cliente. Caso o Cliente pretenda adicionais certificados digitais deverá solicitá-los ao Serviço de Apoio ao Utilizador, suportando, neste caso, os custos correspondentes indicados no Preçário do Banco em cada momento.
4. O acesso à App M Empresas do serviço Mobile App é efetuado através do Código Secreto (PIN) constituído por 4 algarismos, definido no respectivo processo do registo, atento o disposto na anterior Cláusula 5ª (Mobile App). Neste caso, em alternativa à utilização do Código Secreto (PIN) para acesso à App M Empresas do serviço Mobile App, é possível optar por validar o acesso com dados biométricos (Face ID ou Touch ID), desde que o equipamento móvel contemple alguma destas tecnologias.
5. Para a outorga de determinados atos ou negócios jurídicos nos meios de comunicação à distância, nomeadamente para a realização de operações de pagamento acima de certo montante realizadas por débito de conta de depósito do Cliente, pode ser exigível ademais uma confirmação adicional através de um sistema de Autenticação Forte do Cliente (AFC), ou de um Certificado Digital ou ainda de qualquer outra forma ou meio alternativo, com condições de segurança equivalentes, que o Banco disponibilize para esse fim.
6. O Cliente, através dos serviços disponíveis, poderá, em cada momento, definir e gerir as operações de pagamento que, designadamente possam acarretar diminuição do património, e/ou em função dos beneficiários envolvidos, não carecerão da utilização da AFC para a sua realização.
7. O Banco poderá, em cada momento, definir um conjunto de condições – designadamente relativas a beneficiários, montantes e/ou operações – cuja verificação poderá dispensar a utilização da AFC para a execução das mesmas.
8. No sítio de Internet www.millenniumbcp.pt o Utilizador pode alterar a qualquer momento a Password / Código de Acesso (Multicanal), e deverá efetuá-lo regularmente.

Cláusula 7.ª: Convenção sobre prova

1. O(s) Código(s) de Utilizador, os Código Pessoal Secreto (Password / Código de Acesso Multicanal), o(s) Certificado(s) Digital(is), o PIN e/ou os dados biométricos para acesso à App M Empresas do serviço Mobile App são credenciais de segurança personalizadas que permitem ao Banco verificar a identidade do Cliente, autenticar o respectivo acesso e utilização de cada canal à distância, e estabelecer a autoria das ordens aí transmitidas, consubstanciando uma assinatura eletrónica objeto de um direito individual e

exclusivo cuja utilização em conformidade ao acordado identifica e autentica o Cliente perante o Banco e lhe atribui a autoria das instruções e dos documentos electrónicos assim transmitidos.

2. As partes aceitam a equiparação jurídica das sobreditas credenciais de segurança personalizadas do Cliente, a assinaturas manuscritas dos representantes do Cliente.
3. O Banco assumirá legitimamente qualquer acesso, pedido de informação, transmissão de ordens ou instruções, subscrição de contrato ou outorga de quaisquer atos ou negócios jurídicos mediante a utilização das sobreditas credenciais de segurança personalizadas, nos termos ora convencionados, como sendo da autoria do Cliente, não lhe sendo exigível verificar a mesma por qualquer outra via.
4. O referido no número anterior não pode ser interpretado como inibindo o Banco de, se assim o entender, optar por obter a confirmação junto do Cliente das ordens ou instruções recebidas, incluindo uma confirmação por escrito, com assinatura autografa(s), nem prejudica a adoção de outra forma de contratualização das operações bancárias a pedido do Banco ou em resultado de disposição legal, podendo limitar a aceitação de determinado tipo de instruções em função de montantes, número de ordens ou outro critério.
5. As ordens e instruções que o Banco recebe, bem como os atos de subscrição de contratos, ou outorga de quaisquer atos ou negócios jurídicos, desde que corretamente validados mediante a utilização das sobreditas credenciais de segurança personalizadas, gozam de plenos efeitos jurídicos, ficando o Banco irrevogavelmente legitimado para cumpri-las ou executá-los e efetuar os débitos e créditos que deles decorram, entendendo-se, em qualquer caso, que o Banco atua em cumprimento das ordens e instruções recebidas e da vontade real do Cliente.
6. Fica expressamente pactuado entre o Cliente e o Banco que, nos termos e para os efeitos do n.º 4 do art. 3º do Decreto- Lei nº 290-D/99, de 2 de agosto, a utilização das sobreditas credenciais de segurança personalizadas do Cliente, terão o mesmo valor jurídico e probatório da assinatura manuscrita dos representantes legais do Cliente em papel.
7. O disposto na cláusula precedente e na presente cláusula aplica-se também à contratação de produtos e serviços com terceiras entidades, prevista no número 5 da anterior cláusula 1ª, agindo o Banco, nesse âmbito, em nome e em representação daquelas entidades.

Cláusula 8.ª: Obrigações e responsabilidades do Cliente

1. O Cliente obriga-se a tomar todas as medidas de cuidado e de diligência razoáveis para preservar a segurança e a confidencialidade das credenciais de segurança personalizadas indicadas no número 1 da precedente cláusula 7ª, para efeitos de autenticação perante o Banco, e a não permitir nem facilitar o seu conhecimento nem a sua utilização por terceiros, obrigando-se a manter sempre a respetiva confidencialidade, e a uma utilização atenta, cuidadosa, reservada e exclusivamente pessoal dos mesmos.
2. O Cliente é responsável pela guarda, utilização e manutenção corretas das credenciais de segurança personalizadas indicadas no número 1 da precedente cláusula 7ª, para efeitos de autenticação perante o Banco.
3. Designadamente, o Cliente obriga-se a adotar todas as precauções e medidas razoáveis e adequadas para que não se tornem acessíveis ou percetíveis a terceiros não autorizados o(s) Código(s) os Código Pessoal Secreto (Password / Código de Acesso Multicanal), o(s) Certificado (s) Digital(is), o PIN e/ ou os dados biométricos para acesso à App M Empresas do serviço Mobile App, os quais não devem nunca ser anotados em suporte facilmente acessível a outrem, nem no dispositivo móvel ou computador, nem em qualquer outro documento ou suporte que esteja junto dos mesmos.
4. O Cliente deve estar atento, ser precavido e ter em conta que existe o risco de receber mensagens de correio eletrónico, SMS ou até chamadas telefónicas com intuitos fraudulentos, nas quais se imita e substitui a identidade do Banco, a fim de, ardilosa e fraudulentamente obter as credenciais personalizadas de segurança do Cliente. Designadamente, o Cliente tem de suspeitar e de desconfiar do tom de urgência de mensagens que solicitem uma acção imediata ou ameacem por exemplo com a suspensão do acesso se não fornece imediatamente as credenciais de acesso, ou o pedido de confirmação de dados nomeadamente remetendo para o preenchimento on- line de formulários de informações e fornecimento de códigos e credenciais de acesso, ou mensagens SMS ou de correio eletrónico com links ou ficheiros anexos para descarregar e instalar.
5. O Cliente obriga-se conhecer e a assegurar o cumprimento escrupuloso das recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, bem como a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição de concreto(s) procedimento(s) utilizados nesse período para a captura fraudulenta de credenciais de segurança personalizadas de Clientes.
6. O Cliente obriga-se a aceder e utilizar os meios de comunicação à distância do Banco de acordo com as cláusulas e condições que regem a respetiva utilização, e a comunicar ao Banco, sem atraso injustificado, logo que:
   a) Tenha conhecimento da perda, furto, roubo, apropriação abusiva, qualquer utilização não autorizada de credenciais de segurança personalizadas de um (ou mais) Utilizador(es), designadamente de algum(s) Código(s) de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), o Certificado(s) Digital(is), PIN e/ou de dados biométricos para acesso à App M Empresas do serviço Mobile App, e/ou
   b) Suspeite de que terceiros não autorizados têm conhecimento das credenciais de segurança personalizadas de um (ou mais) Utilizador(es), designadamente de algum(s) Código(s) de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), o Certificado(s) Digital(is), PIN e/ou os dados biométricos para acesso à App M Empresas do serviço Mobile App, e/ou
   c) Suspeite de acesso indevido ao seu endereço de correio eletrónico e/ou ao seu computador, telemóvel ou dispositivo móvel, ou ao seu número de telemóvel, por qualquer forma, e/ou
   d) Tenha conhecimento da perda, extravio, roubo, ou de apropriação abusiva do equipamento móvel onde a App M Empresas está instalada; e/ou
   e) Constate o registo em conta de depósito do Cliente de qualquer transação não consentida ou a existência de erros ou irregularidades na efetivação das operações.

   Em qualquer destes casos, o Cliente ou qualquer dos Utilizadores deverá entrar de imediato em contacto com o Banco, por via telefónica para o telefone 21 427 04 02, que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/ impedimento de uso abusivo ou fraudulento. O Cliente deverá ademais confirmar os factos assim comunicados ao Banco, de forma escrita num prazo não superior a 5 dias de calendário.
7. O Cliente é inteiramente responsável perante o Banco pelos actos dos seus representantes legais e dos seus Utilizadores praticados no acesso e na utilização dos meios de comunicação à distância, segundo o disposto no número um do artigo 800º do Código Civil.

8. Neste âmbito, fica bem entendido que compete exclusivamente ao Cliente seleccionar criteriosamente os seus Utilizadores, e instuir e dotar cada Utilizador dos conhecimentos e dos meios adequados para o acesso e utilização dos meios de comunicação à distância do Banco em conformidade às disposições das presentes cláusulas, do(s) Documento(s) "Perfil de Utilizador", e, se for o caso, do Documento "Regras para Autorização de Operações", bem como, transmitir- lhe(s) as recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente Contrato. Designadamente, Cliente obriga-se a:
   a) Comunicar a cada Utilizador especificas instruções e informação sobre os riscos de fraude, nomeadamente de "phishing", alertando-o para a indispensabilidade de ser cuidadoso, atento e precavido e transmitindo-lhe as informações e sinais de alerta expostos no precedente número quatro; e
   b) Facultar a cada Utilizador um exemplar do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, assegurando-se que este o lê atentamente; e
   c) Assegurar que cada Utilizador consulta e lê atentamente, pelo menos uma vez em cada trimestre do ano civil, todos os avisos de segurança e alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição das fraudes mais comuns em cada momento para a captura fraudulenta de credenciais de acesso personalizadas, para se manter devidamente informado e atualizado sobre as precauções e regras de cuidado a adoptar; para tanto, o Cliente deverá instruir cada Utilizador nesse sentido e assegurar o cumprimento periódico dessas instruções; e
   d) Instruir e alertar cada Utilizador de que os respectivos Código de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), Certificado Digital, o PIN e/ou os dados biométricos para acesso à App M Empresas do serviço Mobile App são confidenciais e intransmissíveis, informando-o de todas as medidas de cuidado e de diligência razoáveis que devem ser adoptadas para preservar a posse, segurança, e a utilização exclusiva, reservada e confidencial das mesmas, em nome e por conta do Cliente; e
   e) Instruir e alertar o(s) Utilizador(es) ao(s) qual(is) haja concedido poderes para o serviço Mobile App de que devem adotar todas as medidas de cuidado e de diligencia razoáveis para preservar a posse, a segurança e a utilização exclusiva, reservada e confidencial, em cada momento, do telemóvel ou dispositivo móvel no qual tenha instalado a App App M Empresas; e
   f) Informar cada Utilizador de que no sítio de Internet www. millenniumbcp.pt poderá alterar a qualquer momento a Password / Código de Acesso (Multicanal) que lhe foi atribuída, e instruí-lo de que deverá efectuar essa alteração periodicamente com regularidade; e
   g) Instruir cada Utilizador para que este aceda e utilize os meios de comunicação à distância do Banco de acordo com as cláusulas e condições que regem a respetiva utilização; e
   h) Instruir e alertar cada Utilizador de que deve comunicar ao Cliente e ao Banco, sem atraso injustificado, logo que tenha conhecimento ou suspeite de algum dos factos indicados nas alíneas do precedente número seis desta cláusula, nomeadamente a perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada de credenciais de segurança personalizadas, designadamente de algum(s) Código (s) de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), o Certificado(s) Digital(is), PIN e/ou os dados biométricos para acesso à App M Empresas do serviço Mobile App Millennium, e/ou do endereço de correio eletrónico do Cliente e/ou do telemóvel ou dispositivo móvel em que haja instalado a App M Empresas, ou do número de telemóvel associado, por qualquer forma, devendo entrar de imediato em contacto com o Banco, por via telefónica para o telefone 21 427 04 02, que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento; e
   i) Assegurar que os Utilizadores se vinculam a observar as instruções e obrigações elencadas nas alíneas precedentes deste número.
9. Após a comunicação do Cliente referida no precedente número seis desta cláusula, o Banco bloqueará o acesso às contas do Cliente através dos meios de comunicação à distância.
10. É aqui aplicável o disposto nas cláusulas 12ª (Operações não autorizadas ou incorretamente executadas) e 13ª (Responsabilidade por operações não autorizadas) do antecedente Capítulo B - Condições Gerais de Prestação de Serviços de Pagamento, que aqui se dão por reproduzidas para todos os efeitos.

Cláusula 9.ª: Tratamento das instruções do Cliente

1. Sem prejuízo do disposto na Cláusula 11ª (Suspensão, bloqueio do acesso e resolução do Contrato) infra, o Cliente pode dar instruções ao Banco através dos meios de comunicação à distância a qualquer hora do dia, todos os dias do ano.
2. A execução das ordens transmitidas pelo Cliente será efetuada de acordo com as condições aplicáveis ao tipo de canal à distância em causa, serviço ou produto solicitado.
3. O Banco poderá abster-se de executar ordens transmitidas pelo Cliente quando estas não respeitarem as disposições legais aplicáveis ou colidirem com os usos bancários, quando a conta a movimentar não se encontre provisionada para a operação pretendida, ou ainda quando não for cumprida qualquer disposição constante das presentes cláusulas de Condições Gerais e das regras dos ANEXOS 1 e 2, bem como, dos Documento(s) "Perfil de Utilizador", do Documento "Regras para Autorização de Operações", e se for o caso de outros documentos aplicáveis ao Serviço, ou em virtude de alguma irregularidade no processo de transmissão e/ou autorização da ordem em causa que não seja devidamente sanada no prazo de 72 horas.
4. Uma vez autorizadas e enviadas ao Banco para processamento imediato não é possível efetuar alterações, nem cancelar as ordens transmitidas através dos meios de comunicação à distância.
5. As ordens dadas em dias bancários não úteis serão consideradas como tendo sido ordenadas no primeiro dia útil seguinte. Deverá atender-se sempre às horas limite para processamento de ordens no próprio dia, estabelecidas pelo Banco para os diversos produtos e serviços.
6. A função "BancoMail" do Canal Internet não obriga o Banco à execução de ordens, salvo acordo expresso para o efeito.
7. Considerando que os serviços ou operações disponibilizados pelo Banco através dos meios de comunicação à distância estão sujeitos a interferências, interrupções, desconexões ou outras anomalias, designadamente em consequência de avarias, sobrecargas, cargas de linha, faltas de energia, o Cliente reconhece expressamente que o Banco não será responsável pelos danos, potenciais ou atuais, incluindo lucros cessantes, que, direta ou indiretamente, possam resultar para o Cliente por força da ocorrência de tais eventos, na medida em que as referidas interferências, interrupções, desconexões ou anomalias tenham origem em atos ou omissões de terceiros, nestes incluindo as entidades fornecedoras ou licenciadoras de serviços ao Banco, e em serviços cuja detenção e controlo lhes pertença.

Cláusula 10.ª: Registo das operações e Disponibilização de Extratos, Notas de lançamento e Faturas

1. O Cliente e o Banco acordam que o registo informático das operações realizadas ao abrigo do presente Contrato, o qual poderá ser visualizado em terminal e/ou impresso em papel, constitui prova adequada das ordens dadas pelo Cliente.
2. O Banco compromete-se a manter permanentemente atualizada a informação que disponibiliza ao Cliente através dos canais Internet e Mobile. Todavia, sobre esta prevalecerão sempre os registos contabilísticos próprios do Banco.
3. O Cliente expressamente aceita que os extratos combinados e de movimentos, as notas de lançamento e faturas lhe sejam disponibilizados por via eletrónica, podendo tais documentos electrónicos ser visualizados em terminal e/ou impressos em papel.

Cláusula 11.ª: Suspensão, bloqueio do acesso e resolução do Contrato

1. O Banco poderá inibir e bloquear, total ou parcialmente, o acesso e a utilização dos meios de comunicação à distância pelo Cliente por motivos objetivamente fundamentados que se relacionem com:
   a) Ameaça para a segurança ou por razões de assistência, manutenção, reparação, ou introdução de melhorias na segurança dos meios de comunicação à distância;
   b) Risco ou suspeita de utilização não autorizada ou fraudulenta por terceiros;
   c) O aumento significativo do risco de o Cliente não poder cumprir as suas responsabilidades de pagamento, quando exista linha de crédito associada.
2. De acordo com as circunstâncias do caso, poderão constituir situações enquadráveis numa das alíneas do número anterior os seguintes motivos:
   a) Quando ocorram fundadas razões de ameaça para a segurança e, nomeadamente, se o Banco for informado ou tiver conhecimento de que ocorreu perda, extravio, roubo, furto ou apropriação abusiva de uma ou mais credenciais de segurança personalizadas;
   b) Se o Banco tiver conhecimento ou suspeitar de qualquer uso fraudulento ou de qualquer irregularidade no acesso e utilização dos meios de comunicação à distância de que possa resultar um prejuízo sério para o Sistema de Pagamentos, ou para o Banco ou para o Cliente;
   c) Se o Cliente for inibido do uso do cheque, ou se, por outro motivo fundado houver um aumento significativo do risco do Cliente não poder cumprir as suas responsabilidades creditícias;
   d) Se o saldo de alguma Conta à Ordem do Cliente se apresentar indisponível por penhora, arrolamento, arresto, congelamento, falência, insolvência ou qualquer outra medida de apreensão decretada por ordem judicial e/ou de autoridades judiciárias ou de supervisão.
3. Nos casos referidos no número 1 precedente desta cláusula, o Banco deve informar o Cliente do bloqueio realizado, e da respetiva justificação por mensagem automática ou outro meio expedito, se possível antes de operar o bloqueio ou, o mais tardar, imediatamente após o bloqueio, salvo se tal informação não puder ser prestada por razões de segurança objetivamente fundamentadas ou for proibida por outras disposições legais aplicáveis.
4. Logo que deixem de se verificar os motivos que levaram ao bloqueio, o Banco retirará o bloqueio operado.
5. Por motivos de segurança o Utilizador ficará inibido de aceder aos serviços do Banco através da Internet e Mobile caso ocorram três falhas consecutivas no uso do Código de Utilizador, ou da Password / Código de Acesso (Multicanal). Neste caso, a reativação do acesso poderá ser obtida através de comunicação escrita devidamente assinada do Cliente a solicitar a reativação do Utilizador, de solicitação direta do Utilizador em qualquer Sucursal do Banco ou de outro método igualmente seguro que o Banco venha a comunicar para o efeito.
6. O presente acordo de acesso e utilização dos meios de comunicação à distância pode ser resolvido por qualquer das partes nos termos gerais de Direito. Sem prejuízo do disposto nas cláusulas precedentes, o Banco pode, nomeadamente, resolver o presente Contrato de Condições Gerais de meios de comunicação à Distância e cancelar de imediato o acesso e utilização dos meios de comunicação à distância mediante envio de comunicação escrita, a qual se presume recebida pelo Cliente no terceiro dia posterior à sua expedição, em qualquer dos seguintes casos:
   a) Por qualquer um dos motivos e factos elencados nas alíneas do número dois precedente;
   b) O Cliente, por qualquer forma, der causa à interrupção da sua atividade social, à diminuição considerável das suas garantias de solvabilidade, ou apresentar um projeto de dissolução voluntária;
   c) O Cliente se apresentar à insolvência ou for requerida a insolvência do Cliente;
   d) O Cliente requerer processo especial de revitalização;
   e) Se for revogada a autorização de exercício da actividade do Cliente;
   f) Se for aplicada ao Cliente alguma medida de intervenção corretiva, administração provisória ou de resolução;
   g) Quando se verifique serem falsas ou incorretas informações prestadas no âmbito de reclamação(ões) apresentadas ao Banco, relativas ao acesso e/ou utilização dos meios de comunicação à distância;
   h) Se for requerida alguma providência cautelar de suspensão de deliberações sociais do Cliente e/ou de destituição de gerente(s) ou de membro de órgão de administração do Cliente;
   i) Se a existência de litígio ou de falta de entendimento e de consenso entre os membros do órgão de administração/ gestão do Cliente vier a ser reportada ao Banco por algum(s) dele(s), ou se forem dadas ao Banco instruções contraditórias por algum(s) dele(s) em circunstâncias que indiciem ou demonstrem falta de coesão ou de entendimento entre os membros do órgão administração/gestão do Cliente.

Cláusula 12.ª: Informação financeira

1. A informação financeira disponível através dos canais Internet e Mobile, nomeadamente cotações, índices, notícias, estudos ou outra, é disponibilizada pelo Banco com um intuito meramente informativo e é elaborada por terceiros, que autorizam o Banco a difundir tal informação aos Clientes.
2. Apesar de o Banco selecionar criteriosamente as fontes de informação, podem escapar à sua análise erros ou omissões, não podendo por isso garantir a exatidão ou completude da informação difundida nem ser por tal responsabilizado, ou responsabilizado pela má interpretação ou utilização da mesma.
3. O Cliente utilizará a informação financeira difundida por sua conta e risco, sendo o Cliente exclusivamente responsável pelas decisões de investimento tomadas com base na referida informação.

Cláusula 13.ª: Custos dos serviços

1. O Cliente autoriza o Banco a debitar a Conta de depósitos à ordem aqui identificada infra junto das assinaturas e data do presente, pelos custos relativos aos serviços e operações realizadas através dos meios de comunicação à distância, incluindo as que respeitem à aquisição de bens ou serviços a outros fornecedores presentes no Canal Internet e Mobile , autorizando desde já

o Banco, em caso de insuficiência de saldo e se assim o entender, mas sem a tal estar obrigado, a debitar a referida conta a descoberto pelas quantias necessárias ou debitar qualquer outra conta que o Cliente seja ou venha a ser titular junto do Banco.

2. As operações que o Cliente realiza com o Banco através do Canal Internet e Mobile, assim como as comissões de utilização que sejam devidas, estão sujeitas ao disposto no Preçário do Banco em vigor em cada momento. O Banco poderá, a todo o tempo, modificar o seu Preçário. As alterações do Preçário deverão ser comunicadas ao Cliente mediante circular, mensagem no extrato de conta, correio eletrónico ou por outro meio de comunicação apropriado estipulado pelas partes. As alterações propostas pelo Banco entrarão em vigor após comunicação ao Cliente com pelo menos 30 dias de antecedência, podendo o Cliente declarar por escrito pôr termo à relação contratual por não concordar com as alterações propostas, no prazo máximo de 30 dias a contar da data de comunicação pelo Banco das alterações, presumindo-se que as aceita se não o fizer.
3. Os contactos de iniciativa do Banco não implicam custos para o Cliente, sem prejuízo do preço e encargos devidos pelo serviço financeiro que venha a ser contratado na sequência de cada contacto.

Cláusula 14.ª: Denuncia, alteração do Contrato e Resolução

1. O Banco pode propor modificações ao clausulado das Condições Gerais dos Meios de Comunicação à Distância, emergentes de determinações legais ou relacionadas com sistemas internacionais e regras de segurança, ou ainda quando o entenda conveniente.
2. Essa(s) modificação(ões) será(ão) comunicada(s) ao Cliente em suporte duradouro remetido para o endereço electrónico do Cliente, ou através de pré-aviso ou mensagem inserta no extrato da Conta Cartão e/ou da Conta à Ordem Associada, por circular ou outro meio apropriado habitualmente utilizado, com antecedência não inferior a dois meses sobre a data da sua aplicação.
3. Fica expressamente convencionado que, perante o silêncio subsequente do Cliente se considera que este aceita tacitamente a(s) alteração(ões) assim proposta(s) pelo Banco, exceto se, antes da entrada em vigor dessa proposta, o Cliente notificar o Banco de que não a(s) aceita.
4. Discordando dessa(s) modificação(ões) proposta(s), o Cliente poderá resolver e pôr termo imediato ao presente acordo de Condições Gerais de meios de comunicação à Distância, desde que o efetue antes da entrada em vigor da(s) alteração(ões) proposta(s), e por escrito.
5. O presente Contrato de Condições Gerais de meios de comunicação à Distância poderá ser denunciado a todo o tempo, com efeitos imediatos, pelo Cliente através de comunicação efetuada por escrito ao Banco.
6. O acordo poderá ser denunciado pelo Banco, mediante um pré-aviso escrito de dois meses sobre a data em que a denúncia haja de produzir efeitos.

ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA

Regras gerais para o acesso/uso de todos os Meios de Comunicação à Distância do Banco

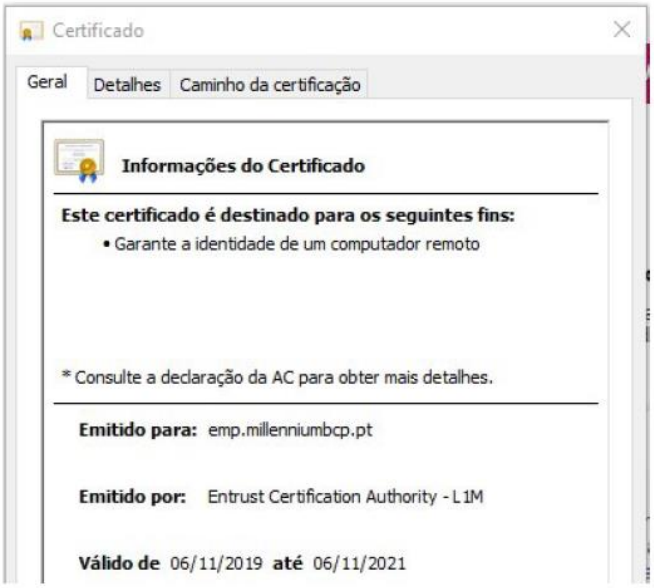
1. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às presentes recomendações e regras de segurança aqui constantes, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, todos os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição das fraudes perpetradas em cada momento para a captura fraudulenta de credenciais de segurança personalizadas.
2. O Cliente deve estar atento e ser precavido contra tentativas de fraude por terceiros não autorizados. Designadamente, o Cliente tem de suspeitar e de desconfiar de qualquer mensagem, por correio eletrónico ou SMS, que peça uma "ação imediata" ou crie uma sensação de urgência, que contenha erros ortográficos/gramaticais, contenha links e/ou anexos de ficheiros executáveis.
3. O Millennium bcp não envia mensagens de correio eletrónico ou SMS com links e nunca solicita a confirmação de dados pessoais ou confidenciais nem de códigos ou dados de autenticação para acesso a contas bancárias por estas vias de comunicação, designadamente remetendo para o preenchimento on-line de formulários de informações pessoais e fornecimento de credenciais de acesso. Se tal vier a suceder, o Cliente deve considerar que se pode tratar de uma tentativa de fraude.
4. O Cliente deve analisar as mensagens de correio eletrónico que recebe antes de abrir, confirmando sempre a origem e o assunto da mesma e, se continuar com dúvidas, confirme previamente junto da entidade emitente. O Cliente não deve aceitar a execução de programas cujo download se ative sem o ter solicitado.
5. Se em algum momento o Cliente receber um Código de Autenticação para confirmação de uma operação que não tenha solicitado, o Cliente deve abster-se de introduzir ou divulgar esse código e deve de imediato reportar o facto sem demora para o(s) número telefónico 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/ dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp.
6. O Cliente não deve nunca facultar o(s) Código(s) de Autenticação a terceiros, sob nenhum pretexto, obrigando-se a fazer uma utilização atenta, prudente, e exclusivamente pessoal do mesmo, e assumindo todos os riscos e consequências inerentes à sua divulgação indevida.
7. Se verificar em algum momento que o telemóvel se encontra inativo ou que o número de telemóvel não funciona corretamente, o Cliente deverá contactar de imediato a sua operadora de telecomunicações e garantir o correto funcionamento do cartão SIM relativo ao seu número de telemóvel indicado ao Banco.
8. Se em algum momento, o Cliente:
   a) Tiver conhecimento da perda, furto, roubo, apropriação abusiva, qualquer utilização não autorizada de credenciais de segurança personalizadas de um (ou mais) Utilizador(es), designadamente de algum(s) Código(s) de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), o Certificado(s) Digital(is), PIN e/ou de dados biométricos para acesso à App M Empresas do serviço Mobile App Millennium, e/ou
   b) Suspeitar de que terceiros não autorizados têm conhecimento das credenciais de segurança personalizadas de um (ou mais) Utilizador(es), designadamente de algum(s) Código(s) de Utilizador, Código Pessoal Secreto (Password / Código de Acesso Multicanal), o Certificado(s) Digital(is), PIN e/ou os dados biométricos para acesso à App M Empresas do serviço Mobile App Millennium, e/ou
   c) Suspeitar de acesso indevido ao seu endereço de correio eletrónico e/ou ao seu computador, telemóvel ou dispositivo móvel, ou ao seu número de telemóvel, por qualquer forma, e/ou
   d) Tiver conhecimento da perda, extravio, roubo, ou de apropriação abusiva de equipamento móvel onde a App M Empresas está instalada, e/ou
   e) Constatar o registo em conta de depósito do Cliente de qualquer transação não consentida ou a existência de erros ou irregularidades na efetivação das operações;

Então deverá, sem demora entrar de imediato em contacto com o Banco, por via telefónica para o telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional), que é um serviço de atendimento permanente – 24 horas/ dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp. O Cliente deverá ainda confirmar ao Banco o sucedido, por escrito, num prazo não superior a 5 dias.

Regras Adicionais para o sítio de Internet www.millenniumbcp.pt:

1. Sempre que aceder às suas contas bancárias, através do sítio do Millennium bcp, verifique se: (i) o endereço se inicia por https://emp.millenniumbcp.pt/, (ii) a barra de endereços se apresenta a verde e (iii) junto ao endereço se encontra um cadeado, seguido de "Millennium BCP", conforme:

2. Em caso de dúvida, confirme a origem do certificado digital - efetuando clique sobre o cadeado - e verifique se corresponde, efetivamente, ao Millennium bcp:



3. O acesso ao sítio de Internet www.millenniumbcp.pt pode ser realizado através de 2 métodos:
   a) identificação do Código de Utilizador, da Password e dois (2) dígitos aleatórios do documento de identificação fiscal (que serão sempre os mesmos até que o login seja efetuado com sucesso);
   b) identificação do Código de Utilizador e três (3) dígitos aleatórios do Código de Acesso (Multicanal), que serão sempre os mesmos até que o login seja efetuado com sucesso.

   Tudo o que for solicitado para além do referido constitui uma tentativa de fraude que deverá reportar imediatamente e sem demora para o 707 50 24 24. Para chamadas a partir do estrangeiro, ligue para +351 210 04 24 24. Atendimento personalizado, disponível nos dias úteis das 8 horas às 02 horas e nos dias não úteis das 10 horas às 24 horas, hora de Portugal Continental.
4. No acesso ao sítio de Internet www.millenniumbcp.pt o Banco nunca solicita o número de telemóvel nem a instalação de software/programas de segurança.
5. O Millennium bcp envia sempre SMS e e-mails sem links.
6. Nunca aceda ao sítio do Millennium bcp através de links de mensagens, motores de pesquisa ou, mesmo, através da opção "Favoritos". Digite sempre o endereço completo www. millenniumbcp.pt para evitar o acesso a páginas fraudulentas e muito idênticas à do sítio do Millennium bcp, bem como evitar a instalação de software malicioso no equipamento utilizado para acesso ao sítio do Millennium bcp.
7. O Millennium bcp nunca solicita elementos de carater pessoal e/ou confidencial, como por exemplo a Password/ Código de Acesso (Multicanal), número de telemóvel, alteração de dados, etc. por email, SMS, nem por qualquer outro meio.
8. Não confie em qualquer mensagem de correio eletrónico supostamente enviada pelo Millennium bcp, solicitando elementos de caráter pessoal e/ou confidencial, como por exemplo o Código de Acesso, Chave de Confirmação, número de telemóvel, etc. O Millennium bcp nunca solicita este tipo de informação aos seus Clientes, por correio electrónico, por SMS ou por qualquer outro meio.
9. Deve ler atentamente o conteúdo do SMS recebido com Código de Autenticação, pois os dados da operação são identificados no texto da mensagem. Nunca forneça a terceiros os Códigos de Autenticação recebidos por SMS ou obtidos via token.
10. Não utilize uma Password/Código de Acesso (Multicanal) óbvio (1234567 ou 1111111 ou data de nascimento, etc.) para o acesso ao sítio de Internet www.millenniumbcp.pt. Periodicamente altere os seus códigos de acesso ao Millennium bcp em "Outros Serviços» Gestão de dados pessoais: Alterar Password/Código de acesso Multicanal".
11. Defina códigos de acesso únicos para o sítio de Internet www.millenniumbcp.pt e não os utilize em outros sítios.
12. Nunca forneça a terceiros quaisquer elementos pessoais de identificação que possam ser utilizados para certificação junto das operadoras móveis, nem os Códigos de Utilizador e de Acesso (Multicanal) ou outros, nomeadamente os Códigos de Autenticação recebidos por SMS ou obtidos via token.
13. Deve impedir o acesso de terceiros aos equipamentos utilizados para confirmar operações bancárias bem como aos seus componentes, como sejam os cartões SIM.

14. Sempre que suspeite que os códigos de acesso ao Millennium bcp possam estar comprometidos, não hesite em alterá-los ou pedir o seu bloqueio através do Centro de Contactos do Banco.
15. O Millennium bcp nunca solicita, em situação alguma, em simultâneo, mais de 3 dígitos do Código de Acesso (Multicanal).
16. O Cliente deve manter o(s) computador(es) e dispositivos móveis protegidos, obrigando-se nomeadamente a:
    - Instalar um bom antivírus, mantendo-o permanentemente atualizado;
    - Utilizar uma firewall para filtrar o tráfego da Internet que entra e sai do computador;
    - Estar atento às atualizações de segurança que os fornecedores credíveis de software disponibilizam, aplicando-as de acordo com as instruções fornecidas;
    - Utilizar sempre versões atualizadas dos navegadores e sistemas operativos;
    - Desativar as opções guardar palavra-passe e preenchimento automático do seu navegador;
    - Se se tratar de computador partilhado, deverá ter em atenção e aplicar sempre as medidas de proteção básicas: desconectar ou terminar sempre cada sessão, e apagar a memória cache;
    - Não deve abrir mensagens eletrónicas de origem desconhecida, e sobretudo não deve clicar ou abrir anexos ou links constantes das mesmas;
    - Não deve abrir ficheiros provenientes de remetentes desconhecidos;
    - Deve manter-se informado sobre a segurança geral quanto à utilização da internet.
17. Consulte sempre as newsletters do Banco e a informação que lhe fornecemos sobre segurança no separador Segurança em www.millenniumbcp.pt. Quando pretender ver algum tema de segurança abordado na nossa newsletter, envie-nos a sua sugestão. Sempre que tenha dúvidas ou necessite de esclarecimentos, por favor contacte-nos através do e-mail empresas@millenniumbcp.pt ou através do telefone 707 504 504. Para chamadas a partir do estrangeiro, ligue para +351 210 04 24 24. Atendimento personalizado, disponível nos dias úteis das 8 horas às 2 horas e nos dias não úteis das 10 horas às 24 horas, hora de Portugal Continental.

Regras adicionais para o acesso ao Serviço do Centro de Contactos

1. O acesso ao serviço telefónico do Banco para:
    a) Suporte a utilizadores de Empresas efetua-se através do número 707 504 504. A partir do estrangeiro, ligue +351 210 04 24 24. O atendimento é personalizado e é solicitado o Código de Utilizador ou/e o Número de Identificação Fiscal (NIF) da Empresa/ENI;
    b) Informações adicionais efetua-se através do número 707 50 24 24. A partir do estrangeiro, ligue +351 210 05 24 24. O atendimento é personalizado e é solicitada a conta à ordem e 3 posições aleatórias do Código de Acesso (Multicanal);
2. Para realização de manutenções aos acessos do sítio de Internet www.millenniumbcp.pt poderão ser solicitadas informações adicionais de segurança (pessoais ou de relação com o Banco).

Regras adicionais para o acesso ao Serviço Mobile App

1. O Cliente deve:
    a) Ativar uma forma de bloqueio automático do seu equipamento móvel e de desbloqueio por código secreto ou dado biométrico do Utilizador;
    b) Proteger o seu smartphone/tablet com um bom antivírus, mantendo-o sempre atualizado e operacional;
    c) Estar atento às atualizações de segurança que os fornecedores credíveis de software disponibilizam e aplicá-las de acordo com as instruções que são fornecidas;
    d) Desativar a opção de instalação de aplicações de origem desconhecida nas definições de segurança do seu equipamento;
    e) Recorrer sempre aos sites/stores oficiais quando necessitar de instalar qualquer aplicação, e ser cauteloso: antes de efetuar o download de uma aplicação, leia a opinião de outros utilizadores e verifique a que funcionalidades e permissões terá de dar acesso no seu equipamento (ex: leitura e envio de sms, acesso aos seus contactos, localização). É muito importante que esteja atento às permissões que concede às aplicações que instala no dispositivo móvel;
    f) Ao usar o correio eletrónico no seu equipamento móvel, o Cliente deve certificar-se que nunca acede a mensagens que não reconhece, principalmente a anexos ou links constantes das mesmas. No caso de receber algum correio eletrónico suspeito aparentemente proveniente do Banco, não o abra, e deve reportar o facto ao Banco, sem demora, numa Sucursal ou por via telefónica para o telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional), que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta;
    g) Recordar que o Millennium bcp nunca envia correio eletrónico e SMS com links;
    h) Ter em atenção que as redes Wi-Fi gratuitas facilitam o acesso de terceiros ao seu telemóvel e aos dados e comunicações do mesmo. Não deve utilizar redes Wi-Fi públicas para aceder ao Canal Internet ou Mobile do Banco e nem para aceder a sites que requeiram a introdução de informações sensíveis, compras online e homebanking. Para este tipo de acessos utilize sempre e só a rede de dados do equipamento móvel;
    i) Desativar o Bluetooth quando não precisar porquanto o telemóvel ficará menos vulnerável a ciberataques;
    j) Manter o seu smartphone/tablet seguro fisicamente, e sob vigilância permanente.
2. As aplicações do Millennium bcp para instalação e utilização no telemóvel/tablet estão disponíveis para equipamentos Apple e Android TM. Instale as aplicações a partir das lojas de aplicações oficiais das marcas (Apple Store, e Play Store). Nunca o faça utilizando links que lhe sejam facultados por terceiros, nomeadamente por correio eletrónico ou por SMS.
3. Registo App M Empresas:
   Depois de instalada a App M Empresas, defina o PIN de Segurança constituído por 4 dígitos numéricos para acesso à App e não o utilize noutras aplicações. De seguida, introduza na App o Código de Utilizador e solicite ali o envio do Código SMS, indispensável ao registo da aplicação; introduza consoante habitualmente solicitado as 3 posições aleatórias do Código de Acesso (Multicanal) ou a sua Password para validar o envio do SMS. Por último, introduza o código que recebeu por SMS e valide com mais 3 posições aleatórias do Código de Acesso (Multicanal) ou a sua Password.
   O Millennium bcp nunca lhe solicitará, em situação alguma, em simultâneo, mais de 3 dígitos do Código de Acesso (Multicanal).
4. Acesso à App M Empresas:
   4.1 A autenticação de acesso através da App M Empresas é efetuada através do PIN constituído por 4 algarismos, definido no processo do registo.

4.2 Em alternativa à utilização do Código de Acesso Único (PIN), o acesso pode efetuar-se através de impressão digital ou reconhecimento facial, (FaceID ou Touch ID) desde que o equipamento contemple estas tecnologias. Na página de login, poderá sempre optar pelo acesso com impressão digital, reconhecimento facial ou através do PIN. Para ativar/ desativar o acesso à App M Empresas por impressão digital ou reconhecimento facial, basta aceder à área de "Configurações".

4.3 Ao decidir ativar a funcionalidade de autenticação com Touch/Face ID na App M Empresas, o Utilizador deve:

a) Garantir que as únicas impressões digitais/registo facial que estão registadas no dispositivo móvel são suas;

b) Informar o Banco sempre que detete que o seu dispositivo de autenticação por Touch/Face ID tenha sido comprometido, para que Banco a proceda ao bloqueio imediato do acesso ao canal até o problema ficar resolvido;

c) Ter em atenção que o módulo de autenticação via impressão digital/reconhecimento facial do dispositivo móvel não é propriedade nem proporcionado pelo Banco, pelo que este não presta garantia quanto à segurança do acesso por esta forma de autenticação, nem o Banco pode ser responsabilizado por eventual funcionamento deficiente e eventuais perdas inerentes ao uso desta forma de autenticação.

5. Para realização e confirmação de transações a App M Empresas nunca lhe solicitará mais de 3 dígitos do Código de Acesso (Multicanal) ou a Password, para confirmar operações na App. Tudo o que for solicitado para além do referido, constitui uma tentativa de fraude e deverá ser reportada para o 707 504 504. Para chamadas a partir do estrangeiro, ligue para +351 210 04 24 24.

Riscos

A utilização dos meios de comunicação à distância com incumprimento das regras e recomendações acima transmitidas, pode acarretar riscos, incluindo:

- Acesso de terceiros a dados pessoais e confidenciais;
- Realização de transações por terceiros que implicam movimentação do património da conta e perdas financeiras para o Cliente.

ANEXO 2 - OPEN BANKING

1. Compete ao Cliente avaliar se quer ou não partilhar os seus dados bancários. O Open Banking dá ao Cliente a possibilidade de compartilhar com terceiras entidades saldos e movimentos das contas detidas junto do Banco, mas apenas se o Cliente nisso consentir expressamente.
2. Se o Cliente considerar adequado que determinadas instituições ou operadores de serviços de pagamento, sem qualquer relação contratual com o Banco (third parties payment services providers - TPPs) tenham acesso eletrónico ao saldo da conta de pagamento de que é titular no Banco, bem como a outras informações financeiras da conta, ou que iniciem pagamentos diretamente na conta, poderá contratar com essas instituições ou operadores alguns dos seguintes serviços de Open Banking:
   - Serviços de iniciação de pagamentos;
   - Serviços de informação sobre contas;
   - Serviços de confirmação de saldos.

   Os serviços de iniciação de pagamentos permitem a um TPP iniciar uma ordem de pagamento na conta de que o Cliente é titular no Banco (ex., um pagamento online diretamente da conta do cliente para a conta do TPP). Os serviços de informação sobre contas permitem a um TPP agregar no seu sítio de Internet informação financeira de várias contas, incluindo os saldos e movimentos da conta detida pelo Cliente junto do Banco (instituições financeiras ou entidades que gerem sites de comparação de preços estarão entre as empresas que prestarão esse tipo de serviço). Os serviços de confirmação de saldos permitem a um TPP que emite instrumentos de pagamento baseados em cartões, no momento em que o Cliente realiza um pagamento com o cartão, confirmar que a conta detida junto do Banco tem saldo suficiente para realizar o pagamento. A possibilidade de um TPP prestar os serviços atrás referidos requer que a conta detida junto do Banco esteja acessível nos canais digitais do Banco e, consequentemente, a prévia adesão do Cliente ao presente Contrato de Utilização dos Meios de Comunicação à Distância. O Banco fica obrigado a disponibilizar ao TPP o IBAN da conta detida pelo Cliente junto do Banco e, conforme os casos, o respetivo saldo ou o saldo e movimentos da conta, ou a aceitar a operação de pagamento por aquele iniciada, não sendo requerido ao TPP identificar o Cliente nem fazer prova do contrato que com ele celebrou para prestar os serviços de Open Banking e aceder diretamente ao Banco.
3. É responsabilidade do Cliente, uma vez redirecionado para a página web/app do Millennium bcp, confirmar a autorização dada a um TPP para que este possa prestar determinado serviço de Open Banking e aceder diretamente ao Banco, devendo para o efeito, no sítio de Internet www.millenniumbcp.pt, introduzir corretamente o Código de Utilizador, três posições aleatórias do Código de Acesso Multicanal e um Código de Autenticação enviado por SMS para o número de telemóvel registado no Banco ou obtido por Token, ou, na App M Empresas, introduzir corretamente o PIN de Segurança constituído por quatro dígitos numéricos e um Código de Autenticação enviado por SMS para o número de telemóvel registado no Banco. Tudo o que for solicitado para além do referido supra constitui uma tentativa de fraude e deverá reportar para o 707 50 24 24. Para chamadas a partir do estrangeiro, ligue para +351 210 05 24 24.
4. O Código de Utilizador, a Password/Código de Acesso Multicanal e o PIN, indicados no ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA destas Condições Gerais, são elementos de autenticação pessoais, confidenciais e intransmissíveis, pelo que o Cliente não pode permitir a sua utilização por terceiros, fazendo uma utilização rigorosa, exclusivamente pessoal dos mesmos.
5. Antes de decidir compartilhar com terceiras entidades saldos e movimentos das contas detidas junto do Banco, o Cliente deve tomar as medidas necessárias para confirmar que o TPP é uma entidade legítima, verificando designadamente tratar-se de uma entidade registada junto do Banco de Portugal ou junto da National Competent Authority do país de origem.
6. Constitui obrigação do TPP prestar informações claras e objetivas sobre a sua identidade e contactos, finalidade e fundamento do tratamento da informação que diz respeito ao Cliente, os destinatários dos dados se os houver, o facto de tencionar transferir dados para um país terceiro, se for o caso.
7. O Cliente deve ter em consideração que se decidir conferir a um TPP o seu acordo para que este tenha acesso aos seus dados bancários e se, além disso, confirmar na página web/app do Millennium bcp a autorização dada a um TPP para que este possa prestar determinado serviço de Open Banking e aceder diretamente ao Banco, o Banco não pode garantir a forma nem as finalidades com que a informação será tratada por aquele, e tratando-se de um serviço de iniciação de pagamentos a operação considera-se assim autorizada, não podendo o consentimento para a sua execução ser então retirado. Não obstante, obtido o consentimento do Cliente, nos termos supra referidos, e tendo acedido aos dados bancários que lhe dizem respeito, o TPP é única e exclusivamente responsável pela segurança dos dados assim obtidos.

8. O Cliente deve ter presente que pode a qualquer momento gerir e retirar na página web/App do Millennium bcp as autorizações para serviços de Open Banking conferidas a TPP´s, devendo para o efeito aceder ao menu Área M ao sítio de Internet www.millenniumbcp.pt. Pode igualmente ligar para a linha de apoio do Millennium bcp.
9. Em qualquer caso, nos termos da lei, o Banco tem a prerrogativa de recusar o acesso de um TPP aos dados bancários do Cliente se considerar que há risco de fraude.

Data _____ / _____ / _____
Ano Mês Dia

Cliente

Assinaturas e Carimbos

_____

_____

_____

Abonação das Assinaturas

A(s) assinatura(s) do Cliente ou representante(s) que obrigam a Empresa confere(m) com a(s) existente(s) nos nossos ficheiros.

Data_____/_____/_____

Banco Comercial Português, S.A.

(Assinatura dos Procuradores do Banco)

_____ NUC _____

_____ NUC _____