CONTRATO DE PRESTAÇÃO DE SERVIÇOS

SISTEMA DE ACEITAÇÃO DE PAGAMENTOS

EM TERMINAL DE PAGAMENTO AUTOMÁTICO

ANEXO D - REQUISITOS PCI DSS

O Cliente obriga-se a respeitar e a fazer respeitar as normas que lhes sejam aplicáveis, emanadas do Payment Card Industry Security Standards Council (organização fundada pelas marcas Visa, MasterCard, American Express, JCB International e Discover Financial Services) e que devem obrigatoriamente ser seguidas pelas organizações que acedem, processam, armazenam ou transmitem dados de cartões de pagamento.

Nesse sentido o Cliente obriga-se ao cumprimento dos requisitos do PCI DSS[1] (Payment Card Industry Data Security Standard), que lhes sejam aplicáveis, identificados nos pontos seguintes:

1. Instalar e manter uma configuração de *firewall* e *router* para proteger os dados do Titular do Cartão;

   1.1 Definir uma configuração standard de *firewall* e *router* que formalize a realização de testes sempre que as configurações sejam alteradas; que identifique todas as ligações aos dados do Titular do Cartão (incluindo ligações sem fios); que utilize diversas configurações técnicas para cada implementação; e que estipule a revisão dos conjuntos de regras de configuração, no mínimo, a cada seis meses;

   1.2 Definir configurações de *firewall* e *router* que restrinjam todo o tráfego proveniente de redes ou *hosts* não confiáveis, exceto para os protocolos necessários para o ambiente de dados do Titular do Cartão;

   1.3 Proibir o acesso público direto entre a Internet e qualquer componente de sistema do ambiente de dados do Titular do Cartão;

   1.4 Instalar software de *firewall* pessoal em todos os computadores ou dispositivos com acesso à Internet (quer sejam propriedade do Cliente ou do seu colaborador) que são utilizados para aceder à rede do Cliente.

2. Não usar as definições de base disponibilizadas por omissão pelo fornecedor para palavras-chave do sistema e para outros parâmetros de segurança;

   2.1 Alterar sempre as definições base disponibilizadas por omissão pelo fornecedor antes de instalar um sistema na rede. Isto inclui dispositivos sem fios que estejam ligados ao ambiente de dados do Titular do Cartão ou sejam utilizados para transmitir dados do Titular do Cartão;

   2.2 Desenvolver standards de configurações para todos os componentes de sistema que lidam com todas as vulnerabilidades de segurança conhecidas, de acordo com definições que cumpram as boas práticas internacionais. Atualizar os standards de configuração de sistemas acompanhando a identificação de novas vulnerabilidades;

[1] O PCI DSS não se sobrepõe às leis nacionais, regionais ou locais, nem a normas governamentais ou outros requisitos legais e regulamentares em vigor.

2.3 Encriptar, utilizando criptografia forte, todos os acessos de administradores não realizados por consola (ex. através de ferramentas de administração baseadas em tecnologias Web);

2.4 Os fornecedores de serviços de *hosting* partilhados têm de proteger cada ambiente de *hosting* contratado por uma entidade bem como os respetivos dados do Titular do Cartão.

3. Proteger os dados armazenados do Titular do Cartão;

3.1 Limitar a quantidade de informação de dados do Titular do Cartão armazenada, bem como o período de retenção dos mesmos, ao estritamente necessário pelo negócio e em cumprimento das disposições legais, regulamentares e normativos internos existentes sobre esta matéria. Eliminar dados não necessários pelo menos trimestralmente;

3.2 Não armazenar os dados de autenticação sensíveis após ter sido efetuada a autorização, mesmo que esses dados estejam encriptados. Incluem-se nesta categoria o código de validação do Cartão (conjunto de algarismos impressos no verso do cartão identificados por CAV2/CVC2/CVV2/CID), os dados completos da tarja magnética ou o equivalente em chip, e os PINs ou PIN Blocks;

3.3 Mascarar o Número do Cartão (PAN - *Primary Account Number* ou Número da Conta Principal) quando for necessária a sua exibição. Os primeiros 6 e os últimos 4 dígitos são o número máximo de dígitos que podem ser exibidos. Esta obrigação não se aplica a pessoal autorizado que, por necessidades legítimas de negócio, deva ter acesso ao número completo do Cartão. Este requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do Titular do Cartão, por exemplo, para recibos emitidos nos TPA (Terminais de Pagamento Automático) / POS (Point Of Sale);

3.4 Tornar ilegível o Número do Cartão, independentemente do meio de suporte de armazenamento, recorrendo, por exemplo, a métodos de *hashing*, processos para o truncar ou a soluções de criptografia forte para o proteger;

3.5 Proteger as chaves de encriptação utilizadas para tornar os dados do Titular do Cartão seguros, evitando a sua divulgação ou uso incorreto;

3.6 Documentar e implementar devidamente todos os processos e procedimentos de gestão de chaves criptográficas utilizadas para a encriptação de dados do Titular do Cartão.

4. Encriptar a transmissão dos dados do Titular do Cartão em redes informáticas abertas e públicas;

4.1 Utilizar criptografia forte e protocolos de segurança, tais como SSL/TLS, SSH ou IPSec, para proteger os dados sensíveis do Titular do Cartão no decorrer da sua transmissão em redes informáticas abertas e públicas (por exemplo: Internet, redes *wireless*, GSM, GPRS e 3G); garantir que as redes *wireless* que transmitem dados do Titular do Cartão ou que estão ligadas ao ambiente de dados do Titular do Cartão utilizam as boas práticas internacionais (por exemplo: IEEE 802.11i) para implementar encriptação forte na autenticação e transmissão de dados; a utilização de WEP como protocolo de segurança é proibida;

4.2 Nunca enviar PANs desprotegidos através de tecnologias de envio de mensagens eletrónicas (por exemplo, *e-mail*, sistemas de mensagens instantâneas, *chat*).

5. Usar e atualizar regularmente os programas e *software* antivírus;

5.1 Instalar e configurar *software* de antivírus em todos os sistemas passíveis de serem afetados por *software* malicioso (nomeadamente, computadores pessoais e servidores);

5.2 Garantir que todos os mecanismos de antivírus estão ativos, atualizados e a gerar *logs* de auditoria.

6. Desenvolver e manter aplicações e sistemas de informação seguros;

   6.1 Garantir que todo o *software* e componentes de sistema estão protegidos face às vulnerabilidades conhecidas através da instalação das atualizações de segurança mais recentes. Instalar atualizações críticas num prazo máximo de um mês a partir da sua data de disponibilização;

   6.2 Estabelecer um processo para identificar e atribuir uma classificação do risco de novas vulnerabilidades de segurança detetadas. Os critérios de classificação de risco devem ser baseados em boas práticas. A classificação de riscos é um requisito em vigor.

   6.3 Desenvolver aplicações de software em concordância com os requisitos do PCI DSS e baseando-se em boas práticas internacionais. Incorporar a segurança de informação ao longo do ciclo de vida de desenvolvimento de software;

   6.4 Seguir processos e procedimentos de controlo de alterações para a realização de todas as alterações a componentes de sistema;

   6.5 Desenvolver aplicações baseadas em boas práticas de desenvolvimento de código seguro e rever o código desenvolvido à medida, de modo a identificar vulnerabilidades do mesmo. Seguir boas práticas internacionais para a identificação e gestão de vulnerabilidades;

   6.6 Garantir que todas as aplicações Web com interfaces públicas estão protegidas contra os tipos de ataque conhecidos, através da revisão (pelo menos uma vez por ano) de vulnerabilidades do código, ou através da instalação de uma firewall para as aplicações Web, colocada em frente das mesmas.

7. Implementar uma política de restrições relativamente ao acesso aos dados do Titular do Cartão, ocorrendo esse acesso apenas de acordo com uma efetiva necessidade de conhecimento;

   7.1 Limitar o acesso a componentes de sistema e a dados do Titular do Cartão apenas a utilizadores cujas funções necessitem efetivamente desse acesso;

   7.2 Estabelecer um sistema de controlo de acessos para componentes de sistema com múltiplos utilizadores que restrinja o acesso com base na necessidade de conhecimento do utilizador e que esteja definido por omissão para negar todos os acessos, a menos que este tenha sido especificamente autorizado.

8. Atribuir um código de Identificação (ID) único para cada pessoa que tenha acesso a um computador;

   8.1 Atribuir a todos os utilizadores um ID único antes de permitir que acedam a componentes do sistema ou a dados do Titular do Cartão;

   8.2 Aplicar pelo menos um dos seguintes métodos para autenticar todos os utilizadores: algo que o utilizador sabe (como uma palavra-chave), algo que o utilizador tem (como um *token*) ou algo que o utilizador é (como um dado biométrico);

   8.3 Implementar mecanismos de autenticação que utilizem dois fatores de autenticação distintos, (ver por exemplo métodos referidos na alínea anterior) para acessos remotos à rede por parte de colaboradores, administradores de sistemas ou entidades externas;

   8.4 Tornar todas as palavras-chave ilegíveis durante o seu armazenamento ou transmissão, para todos os componentes de sistema, utilizando criptografia forte;

   8.5 Garantir uma gestão adequada da identificação e autenticação de utilizadores, para utilizadores que não sejam clientes e para administradores de sistemas, em todos os componentes de sistema.

9. Restringir o acesso físico aos dados do Titular do Cartão;

9.1 Utilizar controlos físicos de entrada nas instalações que sejam apropriados, de modo a limitar e monitorizar acessos físicos aos sistemas no ambiente de dados do Titular do Cartão;

9.2 Desenvolver procedimentos para facilmente distinguir entre colaboradores internos e visitantes, especialmente em áreas onde os dados do Titular do Cartão são acessíveis;

9.3 Garantir que:

- Todos os visitantes são devidamente autorizados antes de entrarem em áreas onde dados do Titular do Cartão sejam processados ou mantidos;

- É atribuído a todos os visitantes um token físico que expira e que os identifica como pessoas externas;

- É solicitado aos visitantes que entreguem o token físico antes de saírem das instalações ou na data de expiração;

9.4 Utilizar um *log* de visitantes para manter um registo da informação e atividades dos visitantes, incluindo o nome do visitante e a empresa representada, bem como qual o colaborador interno que autorizou o seu acesso; Manter o *log* pelo menos por três meses, a não ser que exista alguma restrição imposta por lei;

9.5 Armazenar os suportes de *backup* numa localização segura, preferencialmente fora das instalações do Cliente;

9.6 Proteger fisicamente todos os meios de armazenamento eletrónico de informação;

9.7 Manter um controlo rigoroso sobre a distribuição interna ou externa de quaisquer meios de armazenamento eletrónico de informação. Classificar os meios de armazenamento eletrónico de informação de modo a ser possível determinar a sensibilidade dos dados que contém;

9.8 Garantir que existe aprovação superior da Gestão, quando um meio de armazenamento eletrónico de informação é movido a partir de uma área segura, especialmente quando o mesmo é distribuído a pessoas;

9.9 Manter um controlo rigoroso sobre o armazenamento e acessibilidade dos meios de armazenamento eletrónico de dados de Titular do Cartão;

9.10 Destruir os meios de armazenamento eletrónico de informação quando estes não forem mais necessários para fins de negócio ou para fins legais.

10. Registar e monitorizar todos os acessos aos recursos da rede informática e aos dados do Titular do Cartão;

10.1 Estabelecer um processo para associar todos os acessos a componentes de sistema a cada utilizador individual – especialmente para acessos realizados com privilégios de administração;

10.2 Implementar *logs* de auditoria automáticos para todos os componentes de sistema para permitir a recuperação dos seguintes eventos: todos os acessos individuais ao ambiente de dados do Titular do Cartão; todas as ações levadas a cabo por qualquer utilizador com acessos de *root* ou privilégios de administração; acesso a *logs* de auditoria; tentativas falhadas de acessos lógicos; utilização de mecanismos de identificação e autenticação; inicialização dos logs de auditoria; criação e eliminação de objetos de sistema;

10.3 Gravar *logs* de auditoria para todos os componentes de sistema para cada evento, incluindo, no mínimo: o ID do utilizador, o tipo de evento, a data e hora, a indicação de sucesso ou falha, origem do evento e identidade ou nome dos dados, componente de sistema ou recurso afetados;

10.4 Utilizar uma tecnologia de sincronização temporal, sincronizando todos os relógios dos sistemas críticos e implementando controlos para obter, distribuir e armazenar as horas;

10.5 Proteger os *logs* de auditoria de modo a que não possam ser alterados;

10.6 Analisar os *logs* para todos os componentes de sistema relacionados com funções de segurança, pelo menos diariamente;

10.7 Manter o histórico de *logs* de auditoria durante pelo menos um ano, sendo que o correspondente aos últimos três meses deverá estar imediatamente acessível para análise.

11. Testar regularmente os sistemas e processos de segurança;

11.1 Testar e detetar a presença de pontos de acesso *wireless*, pelo menos, trimestralmente,

11.2 Realizar verificações internas e externas para detetar vulnerabilidades de rede, pelo menos, trimestralmente e após alterações significativas na rede. Após a aprovação numa verificação inicial à conformidade com o PCI DSS, o Cliente deverá, nos anos seguintes, conseguir aprovação em quatro verificações trimestrais consecutivas como requisito para a conformidade. As verificações externas trimestrais têm de ser realizadas por um *Approved Scanning Vendor* (ASV). As verificações realizadas após alterações na rede podem ser efetuadas por uma equipa interna do Cliente;

11.3 Realizar testes de intrusão, interna e externa, incluindo testes de intrusão ao nível de rede e aplicacional, pelo menos anualmente e após alguma alteração significativa à infraestrutura ou atualização/ alteração aplicacional;

11.4 Utilizar sistemas de deteção de intrusões de rede (IDS) e/ou sistemas de prevenção de intrusões (IPS) para monitorizar o tráfego no perímetro e em pontos críticos do ambiente de dados do Titular do Cartão e alertar para suspeitas de comprometimento desse ambiente. Os motores IDS/IPS, *baselines*, e assinaturas têm que ser mantidos atualizados;

11.5 Utilizar uma ferramenta de monitorização da integridade de ficheiros que alerte para modificações não autorizadas de ficheiros de sistema críticos, ficheiros de configuração ou ficheiros de conteúdos. Configurar o software para realizar comparações de ficheiros críticos, pelo menos semanalmente.

12. Manter uma política que endereça a segurança de informação e que abrange todos os colaboradores:

12.1 Definir, publicar, manter e disseminar uma política de segurança que enderece todos os requisitos do PCI DSS, inclua um processo anual para identificação de vulnerabilidades e avaliação formal de riscos e que seja revista pelo menos uma vez por ano e quando o ambiente se altera;

12.2 Desenvolver procedimentos operacionais de segurança diários que estejam em concordância com os requisitos do PCI DSS;

12.3 Desenvolver políticas de utilização para tecnologias críticas de modo a definir a sua utilização apropriada por parte de todos os colaboradores. Estas incluem acesso remoto, *wireless*, dispositivos de armazenamento eletrónico amovíveis, portáteis, *tablets*, PDAs, *e-mail* e Internet;

12.4 Garantir que a política e procedimentos de segurança definem claramente as responsabilidades quanto à segurança de informação para todos os colaboradores;

12.5 Atribuir a um indivíduo ou a uma equipa as responsabilidades de segurança de informação definidas nas subsecções 12.5.1 a 12.5.5. deste ponto 12.5 do PCI DSS (consultar a informação mais detalhada disponibilizada no site institucional do *Payment Card Industry Security Standards Council)*;

12.6 Implementar um programa formal de sensibilização de segurança de modo a sensibilizar todos os colaboradores para a importância da segurança dos dados do Titular do Cartão;

12.7 Analisar potenciais colaboradores antes da sua contratação de forma a minimizar o risco de ataques a partir de fontes internas;

12.8 Se os dados do Titular do Cartão forem partilhados com prestadores de serviços, manter e implementar políticas e procedimentos para formalmente identificar as responsabilidades dos prestadores de serviços na proteção dos dados do Titular do Cartão, e monitorizar o estado de *compliance* dos prestadores de serviços com o PCI DSS pelo menos uma vez por ano.

12.9 Implementar um plano de resposta a incidentes. Estar preparado para responder imediatamente a uma quebra ou vulnerabilidade de segurança no sistema.

Feito em _____, _____ de _____ de 20____, em dois exemplares, sendo um para cada parte.

Caixa Geral de Depósitos	**Cliente**
(simples assinatura de representante, sob carimbo).	(simples assinatura das pessoas que, segundo o Contrato Social ou os estatutos tenham poderes para obrigar a pessoa coletiva no presente ato, devendo as assinaturas ser feitas sob carimbo da Empresa e menção da qualidade em que as pessoas intervêm, a conferir pela Caixa).