BANCO DO ESTADO DO RIO GRANDE DO SUL S/A
PRÉ-QUALIFICAÇÃO PERMANENTE Nº 0000607/2019

O **BANCO DO ESTADO DO RIO GRANDE DO SUL S/A,** torna público que a partir do dia 24/09/2019, iniciará o recebimento da documentação para abertura da **PRÉ-QUALIFICAÇÃO PERMANENTE**, regida pela Lei Federal nº 13.303 de 30 de junho de 2016 e legislação pertinente, no que dispõe a Lei Complementar nº 123, de 14 de dezembro de 2006, sujeitando-se às disposições da Lei Estadual nº 11.389 de 25 de novembro de 1999, Lei Estadual nº 15.228, de 25 de setembro de 2018 e no Regulamento de Licitações e Contratos do Banrisul, disponível no endereço eletrônico www.banrisul.com.br, na UNIDADE DE LICITAÇÕES E COMPRAS, situada na Rua Sete de Setembro, nº745, 4º andar, Centro Histórico, Porto Alegre/RS, CEP 90.010-190, telefone (51) 3215-4510.

FORMALIZAÇÃO DE CONSULTAS: banrisul_licitacoes@banrisul.com.br
REFERÊNCIA DE TEMPO: para todas as referências de tempo será observado o horário de Brasília (DF).

I. DISPOSIÇÕES PRELIMINARES

1.1. Este procedimento é anterior à licitação e destina-se a identificar bens que atendam às exigências técnicas e de qualidade estabelecidas neste Edital e seus anexos.

1.2. O Banrisul não promoverá sessão pública para entrega da documentação de pré-qualificação.

II. DO OBJETO

2.1. Este procedimento tem por objeto a Pré-Qualificação permanente para futuras aquisições de equipamentos Mobile PINPad, Mobile POS, POS Fixo, POS Móvel e SmartPOS em futuras licitações, restritas aos pré-qualificados, cujo objeto é manter um banco de equipamentos qualificado e dentro das especificações técnicas da Banrisul Cartões, conforme detalhado nos anexos "Termo de Referência para Pré-Qualificação Permanente" e "Especificações Técnicas".

III. DA VALIDADE DA PRÉ-QUALIFICAÇÃO

3.1. O prazo de validade da Pré-Qualificação será de **até 1 (um) ano, podendo ser atualizada a qualquer tempo**, nos termos do § 5º, art. 80, do Regulamento de Licitações e Contratos do Banco do Estado do Rio Grande do Sul S/A.

IV. DAS CONDIÇÕES GERAIS DE PARTICIPAÇÃO

4.1. Somente poderão participar desta Pré-Qualificação os interessados que satisfaçam as exigências deste edital, da Lei n° 13.303/2016 e do

Regulamento de Licitações e Contratos do Banrisul.

4.2. Os interessados entregarão o envelope contendo a documentação exigida no item VII do edital, na recepção da Unidade de Licitações e Compras, das 10h as 16h, trazendo em seu subscrito as referências indicadas abaixo:

- BANCO DO ESTADO DO RIO GRANDE DO SUL S/A.
- Razão Social da Empresa Proponente.
- PRÉ-QUALIFICAÇÃO Nº 0000607/2019 – Banrisul –

4.3. Enquanto perdurarem os motivos determinantes de punições ou até que seja promovida a reabilitação, não poderão participar da presente pré-qualificação as empresas ou profissionais que tenham sofrido penalidades resultantes de contratos firmados anteriormente com o Banco, na condição de prestadores de serviços, fornecedores, empreiteiros ou construtores, tais como suspensão, declaração de inidoneidade, bem como aqueles impedidos de operar com o Banco por determinação do Banco Central do Brasil.

4.4. Os documentos necessários à participação na presente pré-qualificação deverão conter rubrica do representante legal do interessado e estarem numerados sequencialmente, da primeira à última folha, de modo a refletir o seu número exato.

4.5. Poderão participar desta pré-qualificação os interessados em concorrer a futuras licitações para o fornecimento do objeto descrito e que atenderem às exigências deste Edital e seus anexos.

4.6. A pré-qualificação do objeto deste instrumento não gera direito à contratação futura e nem implica a preclusão da faculdade legal de inabilitação quando do certame.

4.7. O interessado poderá pré-qualificar um ou mais itens conforme descrição.

4.8. Este procedimento de pré-qualificação estará permanentemente aberto à inscrição de qualquer interessado.

4.9. A simples participação neste processo de pré-qualificação implica aceitação de todos os seus termos, condições, normas, especificações e detalhes.

V. DOS IMPEDIMENTOS À PARTICIPAÇÃO

5.1. Não poderão participar deste processo de pré-qualificação empresas que se encontrem em processo de falência, de recuperação judicial ou extrajudicial, dissolução ou liquidação, que estejam punidas com suspensão temporária de participar de licitações e impedidas de contratar com o Contratante, bem como as que tenham sido declaradas inidôneas para licitar ou contratar com a Administração Pública direta ou indireta Federal, Estadual ou Municipal.

5.2. Não será permitida a participação de empresas em consórcio.

5.3. Estará impedida de participar da presente pré-qualificação, em qualquer fase do processo, a empresa que se enquadre em uma das hipóteses abaixo:

I. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado do Banrisul ou uma de suas Controladas;

II. Que esteja cumprindo penalidade de suspensão aplicada pelo Banrisul ou uma de suas Controladas;

III. Que tenha sido declarado inidônea pelo Banrisul e ou por órgãos da administração pública direta e/ou indireta do Estado do Rio Grande do Sul, enquanto perdurarem os efeitos da sanção;

IV. Que seja constituída por sócio de empresa que estiver suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul;

V. Cujo administrador seja sócio de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul;

VI. Constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul, no período dos fatos que deram ensejo à sanção;

VII. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul, no período dos fatos que deram ensejo à sanção;

VIII. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

5.4. A vedação prevista no item 5.1 deste edital também se aplica para as seguintes situações:

I. À contratação de empregado ou dirigente do Banrisul ou de uma de suas Controladas, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

II. A quem tenha relação de parentesco, até o terceiro grau civil, com:

a) Dirigente do Banrisul ou de uma de suas Controladas;

b) Empregado do Banrisul ou de uma de suas Controladas cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

c) Autoridade do ente público a que o Banrisul ou uma de suas Controladas está vinculado.

III. Empresa cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com o Banrisul ou uma de suas Controladas há menos de 6 (seis) meses.

VI. DO RECEBIMENTO DO PROTÓTIPO E DA DOCUMENTAÇÃO

6.1. Os documentos de qualificação técnica do interessado deverão ser encaminhados em conformidade com o item IV deste edital.

6.2. A análise da documentação e do protótipo pela administração deverá ocorrer em até 160 (cento e sessenta) dias a contar do recebimento dos mesmos.

6.2.1. O prazo para conclusão da homologação de segurança de hardware será de 10 (dez) dias corridos, a contar da entrega do lote de equipamentos necessários para o processo homologatório;

6.2.2. O prazo para conclusão da homologação de software funcional, de performance e usabilidade será de 120 (cento e vinte) dias corridos, a contar a partir da conclusão da homologação de hardware;

6.2.3. O prazo para início e conclusão do piloto será de 30 (trinta) dias corridos.

6.3. O interessado deverá enviar a quantidade estabelecida neste Edital, conforme o objeto a ser pré-qualificado, os quais deverão estar de acordo com as especificações técnicas exigidas.

6.4. O protótipo deverá ser entregue, para análise, na sede da Banrisul Cartões S.A. – Gerência de Soluções de Captura, localizada na Rua Siqueira Campos, nº832, 2º andar, bairro Centro Histórico, Porto Alegre/RS, em horário comercial compreendido entre as 8h às 18h.

6.5. A participação na Pré-Qualificação, através da apresentação do protótipo e dos documentos exigidos neste instrumento, implicará na aceitação plena e irretratável das normas e especificações que a ordenam.

VII. DOCUMENTOS PARA PRÉ-QUALIFICAÇÃO TÉCNICA

7.1. Para habilitação o interessado deverá apresentar a seguinte documentação:

7.1.1. Jurídica:

7.1.1.1. Registro Comercial, no caso de empresa individual;

7.1.1.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrados na Junta Comercial em se tratando de Sociedade Empresária e/ou no caso de sociedade por ações, acompanhados de documentos de eleição de seus administradores, e no Cartório de Registro de Títulos Especiais em se

tratando de Sociedade Simples;

7.1.1.3. Decreto de autorização devidamente arquivado na Junta Comercial em se tratando de empresa ou sociedade estrangeira em funcionamento no país;

7.1.2. Laudos Técnicos:

7.1.2.1. Para cada equipamento apresentado para testes e homologação de pré-qualificação deverá estar acompanhado das certificações correspondentes, conforme solicitado no documento "Especificações Técnicas", anexo II deste edital.

7.1.2.2. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

7.1.3. Em nenhuma hipótese será aceita documentação incompleta, sendo a mesma de inteira responsabilidade do interessado.

7.1.4. Havendo necessidade do interessado em providenciar documentação complementar, o prazo informado no item 6.2 será reaberto a contar do recebimento da nova documentação.

VIII. IMPUGNAÇÃO E ESCLARECIMENTOS AO EDITAL

8.1. As solicitações mencionadas de impugnação ou esclarecimentos ao presente Edital deverão ser encaminhadas por meio eletrônico via internet, para o endereço banrisul_licitacoes@banrisul.com.br.

8.2. Caberá ao Banrisul decidir sobre a petição no prazo de 24 (vinte e quatro) horas.

8.3. Acolhida a petição contra ato convocatório, será designada nova data para a abertura do processo de Pré-Qualificação.

IX. CRITÉRIOS DE AVALIAÇÃO DA PRÉ-QUALIFICAÇÃO

9.1. O protótipo deverá cumprir todas as exigências deste Instrumento, conforme especificação apresentada.

9.2. Os resultados serão apresentados conforme item **X – RESULTADO DA PRÉ-QUALIFICAÇÃO**, deste Edital.

9.3. Os exemplares colocados à disposição poderão ser manuseados, desmontados e destruídos pela equipe técnica responsável pela análise.

9.4. Os protótipos deverão ser retirados pelo interessado no estado em que se encontrarem, em endereço a ser informado, no prazo de até 15 (quinze) dias corridos da publicação do resultado.

9.5. O Banco poderá descartar o bem/material não retirado, não cabendo qualquer tipo de indenização ao interessado.

9.6. A entrega e a montagem, quando necessárias, serão obrigatoriamente realizadas por representante do interessado.

9.7. O interessado será responsável pela retirada e descarte dos materiais inservíveis resultantes da montagem dos protótipos, como embalagens, protetores etc.

9.8. Durante o período de exame dos protótipos e da documentação técnica, o Banco poderá efetuar diligências às dependências do interessado a fim de sanar eventuais dúvidas, realizar avaliação das instalações, capacidade e qualidade do processo produtivo, considerando a validação do maquinário mínimo declarado e a análise do sistema de gestão da qualidade do interessado.

9.9. Posteriormente à publicação do resultado, qualquer interessado poderá solicitar, no prazo de 03 (três) dias úteis, vistas ao protótipo, onde será permitida a manipulação e registros fotográficos.

9.10. A análise de qualidade dos protótipos abrangerá a validação das especificações técnicas, com base em requisitos de desempenho e características técnicas definidas e padronizadas, e constará de:

a) inspeção visual (cores, acabamentos, formas e dimensões);

b) manuseio das partes móveis;

c) verificação de conformidade de materiais, acessórios, acabamentos e mecanismos;

d) verificação da estabilidade e resistência, com possibilidade da realização de ensaios destrutivos (quando for o caso);

e) validação da documentação de qualificação técnica exigida; e

f) demais verificações que se fizerem necessárias.

X. RESULTADO DA PRÉ-QUALIFICAÇÃO

10.1. O resultado da pré-qualificação será divulgado no sítio eletrônico do Banco – www.banrisul.com.br > Áreas Temáticas Banrisul > Licitações e Leilões > Vender para o Banrisul > Em Andamento, e terá validade **de até 01 (um) ano, podendo ser atualizado a qualquer tempo**.

10.2. Poderá o Banco, caso entenda pertinente e de forma justificada, revalidar a Pré-Qualificação cujo prazo tenha expirado, desde que as condições à época da pré-qualificação se mantenham inalteradas e, ainda, não houver indicação para nova avaliação do objeto/fornecedor qualificado.

XI. DA FASE RECURSAL

11.1. Das decisões proferidas pela Comissão de Licitações caberá recurso no prazo de 05 (cinco) dias úteis, na forma do art. 59 da Lei n° 13.303/2016, para a autoridade que designar a pré-qualificação, interposto por escrito e entregue, mediante protocolo, na recepção da Unidade de Licitações e Compras, conforme endereço indicado no preâmbulo deste edital, ou encaminhadas para o endereço eletrônico banrisul_licitacoes@banrisul.com.br, impreterivelmente no horário compreendido entre 10h e 16h.

11.2. É assegurada aos interessados vista aos autos do processo, resguardado os documentos considerados sigilosos.

11.3. A Comissão de Licitações poderá reconsiderar sua decisão, ou, no caso de mantê-la, deverá encaminhar o recurso à Autoridade Superior para decisão.

11.3.1. A decisão da Autoridade Superior tem caráter final, não cabendo qualquer outro recurso.

11.4. O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

11.5. Decididos os recursos e constatada a regularidade dos atos praticados, a instância competente poderá ratificar o resultado da Pré-Qualificação.

XII. DAS DISPOSIÇÕES GERAIS

12.1. Somente será considerado pré-qualificado o interessado que houver preenchido os requisitos exigidos no edital.

12.2. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do processo.

12.3. É facultado em qualquer fase da pré-qualificação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo.

12.4. A administração do Banco poderá anular ou revogar, parcialmente ou na sua totalidade, este procedimento de pré-qualificação, observadas as disposições legais pertinentes.

12.5. Os casos omissos serão resolvidos pela administração, que a eles aplicará as disposições da Lei Federal 13.303/2016, e disposições supletivas, se couber, desde que não venha conflitar com a referida legislação.

12.6. Fica desde logo esclarecido que todos os participantes deste procedimento de pré-qualificação, sujeitam-se a todos os seus termos, condições, normas, especificações e detalhes, comprometendo-se a cumpri-lo fielmente, independentemente de qualquer manifestação expressa ou tácita.

12.7. O desatendimento de exigências formais não essenciais não importará no afastamento o interessado, desde que sejam possíveis a aferição da sua qualificação e a exata compreensão da sua documentação, e desde que não comprometa o interesse do Banco.

12.8. Vista ao processo será fornecida ao representante legal devidamente identificado e mediante solicitação formal, na Rua Sete de Setembro, nº745, 4º andar, Centro Histórico, Porto Alegre/RS, de segunda à sexta-feira, no horário das 10 horas às 16 horas. As cópias serão fornecidas mediante pagamento dos emolumentos devidos. É facultado ao interessado, por intermédio de equipamento pessoal, digitalizar ou fotografar os documentos do processo, em recinto disponibilizado pelo Banco.

12.9. Fazem parte integrante e complementar deste edital:

ANEXO I – Termo de Referência para Pré-Qualificação Permanente;

ANEXO II – Especificações Técnicas dos Equipamentos;

ANEXO III – Acordo de Confidencialidade e Sigilo.

12.10. Fica eleito o Foro da Comarca de Porto Alegre/RS para dirimir quaisquer dúvidas oriundas deste procedimento de pré-qualificação.

Porto Alegre, 24 de setembro de 2019.

_____

BANCO DO ESTADO DO RIO GRANDE DO SUL S/A

UNIDADE DE CONTRATAÇÕES E PAGADORIA

Gerência de Instrumentalização de Processos de Compras e Contratações

BANRISUL JURÍDICO

TERMO DE REFERÊNCIA PARA PRÉ-QUALIFICAÇÃO PERMANENTE

Nº DO PROCESSO: 0000607/2019
Numeração fornecida pelo Sistema BMP

UNIDADE REQUISITANTE Unidade que elaborou o Termo de Referência	BANRISUL CARTÕES S/A
GESTOR DOS SERVIÇOS Unidade responsável pela execução do objeto	BANRISUL CARTÕES S/A
GESTOR TÉCNICO Unidade com o conhecimento técnico do objeto a ser contratado	BANRISUL CARTÕES S/A

1. DO OBJETO

Pré-qualificação permanente para futuras aquisições de equipamentos Mobile PINPad, Mobile POS, POS Fixo, POS Móvel e SmartPOS em futuras licitações, restritas aos pré-qualificados, cujo objeto é manter um banco de equipamentos qualificado e dentro das especificações técnicas da Banrisul Cartões.

1.1. ESPECIFICAÇÕES TÉCNICAS

As especificações dos objetos estão descritas no Anexo - Especificações Técnicas das Soluções de Captura.

2. CONTRATANTE

( ) BANCO DO ESTADO DO RIO GRANDE DO SUL S.A.
(X) BANRISUL CARTÕES S.A.
( ) BANRISUL S.A. - CORRETORA DE VALORES MOBILIÁRIOS E CÂMBIO
( ) BANRISUL S/A – ADMINISTRADORA DE CONSÓRCIOS

3. DA EXECUÇÃO

O interessado deverá enviar a quantidade de amostras estabelecida no quadro abaixo, conforme o objeto a ser pré-qualificado, os quais deverão estar de acordo com as especificações técnicas exigidas:

ITEM	DESCRIÇÃO	QUANTIDADES NECESSÁRIAS DE AMOSTRAS PARA A FASE DE HOMOLOGAÇÃO	QUANTIDADES SUPLEMENTARES DE AMOSTRAS PARA A FASE PILOTO
1	Mobile PINPad	4	20
2	Mobile POS	4	20

3	POS Fixo	4	20
4	POS Móvel	4	20
5	SmartPOS	4	20

3.1. NECESSIDADE TÉCNICA

Para cada modelo de equipamento devem ser entregues os equipamentos conforme abaixo:
3.1.1. 02 (dois) equipamentos com chaves de desenvolvimento para homologação de segurança de hardware e homologação de software funcional em ambiente de desenvolvimento.
3.1.2. 02 (dois) equipamentos com chaves de produção para testes de performance e usabilidade em ambiente de produção.
3.1.3. 20 (vinte) equipamentos com chaves de produção para piloto controlado em estabelecimentos comerciais da Vero.

4. LOCAL DE ENTREGA DOS EQUIPAMENTOS

Os equipamentos deverão ser entregues na sede da Banrisul Cartões S.A. - Gerência de Soluções de Captura, localizada na Rua Siqueira Campos, 832 / 2º andar, bairro Centro Histórico em Porto Alegre/RS, em horário comercial das 8h às 18h.

5. PROCESSO DE HOMOLOGAÇÃO

5.1. HARDWARE

5.1.1. Os equipamentos devem atender a todas as especificidades técnicas de hardwares presentes no Anexo - Especificações Técnicas das Soluções de Captura.
5.1.2. O interessado deverá disponibilizar todos os certificados e documentos atualizados exigidos presentes no Anexo - Especificações Técnicas das Soluções de Captura.
5.1.3. O interessado deverá assinar o anexo denominado Acordo de Confidencialidade e Sigilo (NDA) para poder se qualificar a homologação do seu equipamento.
5.1.4. Além da entrega da documentação e NDA assinado, o interessado deverá encaminhar os equipamentos para homologação com os softwares embarcados e todos demais componentes necessários para perfeito funcionamento (cabos, fontes e etc.).
5.1.5. O prazo de qualificação começará a contar a partir da entrega do lote de equipamentos necessários para o processo homologatório, conforme descrito no capítulo 3 deste documento.
5.1.6. Serão priorizados os primeiros equipamentos entregues, respeitando a capacidade de homologação do laboratório de testes do Banrisul e os projetos em andamento da Banrisul Cartões S.A.
5.1.7. Cada modelo de equipamento terá seu processo homologatório conduzido de maneira independente.
5.1.8. O interessado deverá indicar, formalmente, as empresas responsáveis pelos seus respectivos desenvolvimentos de software, de acordo com as soluções de captura descritas no capítulo 3 deste documento.
5.1.9. O prazo para conclusão da homologação de segurança de hardware será de **10 (dez) dias corridos**, a contar da entrega do lote de equipamentos necessários para o processo homologatório.
5.1.10. A Banrisul Cartões através de envio de e-mail formal comunicará os referidos prazos durante o início deste processo, bem como na conclusão do mesmo.

5.1.11. Caso o equipamento atenda todas especificações de hardware e segurança, o mesmo será considerado apto para continuidade do processo homologatório.
5.1.12. Caso o equipamento não atenda as especificações de hardware e segurança, o mesmo será considerado inapto para continuidade do processo homologatório.

5.2. SOFTWARE

5.2.1. Após conclusão do processo de homologação de hardware, de forma satisfatória, o processo de homologação de software será iniciado imediatamente.
5.2.2. O prazo para conclusão da homologação de software funcional, de performance e usabilidade será de **120 (cento e vinte) dias** corridos, a contar a partir da conclusão da homologação de hardware, conforme item 5.1 deste documento.
5.2.3. A Banrisul Cartões através de envio de e-mail formal comunicará os referidos prazos durante o início deste processo, bem como na conclusão do mesmo.
5.2.4. Serão aceitos, dentro do prazo estipulado no item 5.2.2, no máximo de 3 (três) ciclos de homologação durante o processo.
5.2.5. Caso o equipamento passe pelo processo de homologação de software **sem** ocorrências graves, o mesmo será considerado apto para continuidade do processo homologatório.
5.2.6. Caso o equipamento passe pelo processo de homologação de software **com** ocorrências graves, sem solução dentre o prazo de homologação e quantidade de ciclos máximos estipulados, o mesmo será considerado inapto para continuidade do processo homologatório.
5.2.7. Serão consideradas "ocorrências graves":
5.2.7.1. Anomalias na mensageria trocada entre os terminais e os sistemas da Vero, que afetem ou comprometam o fluxo transacional de adquirência.
5.2.7.2. Problemas relacionados ao hardware que sejam constatados durante o processo e que não tenham solução dentro dos prazos preestabelecidos.
5.2.7.3. Inconformidades segundo princípios do PCI DSS (Payment Card Industry Data Secutiry Standards).

5.3. PILOTO

5.3.1. Os equipamentos que passarem pelas etapas de homologação de hardware e software poderão passar por um piloto em ambiente de produção.
5.3.2. Serão pilotados os equipamentos que não constem na base de equipamentos da rede de adquirência Vero.
5.3.3. Deverão ser enviados pelo menos amostras adicionais de **20 (vinte) equipamentos** de produção para a etapa de piloto.
5.3.4. Equipamentos já pilotados e em operação na base Vero serão considerados aptos e qualificados, não necessitando participar por esta etapa do processo.
5.3.5. O prazo para início e conclusão do piloto será de **30 (trinta) dias** corridos.
5.3.6. A Banrisul Cartões através de envio de e-mail formal comunicará os referidos prazos durante o início deste processo, bem como na conclusão do mesmo.
5.3.7. Caso o equipamento passe pelo processo de piloto **sem** ocorrências graves, o mesmo será considerado qualificado e apto para aquisições/compras futuras.
5.3.8. Caso o equipamento passe pelo processo de piloto **com** ocorrências graves, o mesmo será considerado desqualificado e inapto para aquisições/compras futuras.
5.3.9. Os equipamentos homologados e qualificados a participar dos futuros pregões realizados pela Banrisul Cartões serão anunciados no site da empresa, no link: https://www.banrisul.com.br/bob/data/Vero-EquipamentosPOS,mPOSePINPadshomologados.pdf
5.3.10. Serão consideradas "ocorrências graves":
5.3.10.1. Anomalias na mensageria trocada entre os terminais e os sistemas da Vero, que

afetem ou comprometam o fluxo transacional de adquirência.

5.3.10.2. Problemas relacionados ao hardware que sejam constatados durante o processo e que não tenham solução dentro dos prazos preestabelecidos.

5.3.10.3. Inconformidades segundo princípios do PCI DSS (Payment Card Industry Data Secutiry Standards).

6. CUSTOS

6.1. Não caberá ao interessado o ressarcimento do valor da amostra ou custo qualquer de apresentação da mesma. O interessado arcará com todos os custos decorrentes da apresentação das amostras e demais custos decorrentes da participação neste edital de pré-qualificação, independentemente da condução ou resultado do processo, pois a Banrisul Cartões não é, em nenhum caso, por isso responsável.

6.2. O interessado fica isento dos custos referentes a fase interna de homologação realizada no laboratório de homologação da Banrisul Cartões.

6.3. As amostras exigidas, que sejam passíveis de devolução, deverão ser procuradas por suas proprietárias após **180 (cento e oitenta)** dias da finalização do processo de homologação, sob pena de lhes serem dadas outra destinação, a critério do Banrisul Cartões.

7. VIGÊNCIA DA PRÉ-QUALIFICAÇÃO

7.1. O prazo de validade da pré-qualificação será de até 1 (um) ano, podendo ser atualizada a qualquer tempo, nos termos do § 5º, art. 80, do Regulamento de Licitações e Contratos do Banco do Estado do Rio Grande do Sul S/A.

7.2. Poderá o Contratante, caso entenda pertinente e de forma justificada, revalidar a pré-qualificação cujo prazo tenha expirado, desde que as condições à época da pré-qualificação se mantenham inalteradas e, ainda, não houver indicação para nova avaliação do objeto/fornecedor qualificado.

8. PROCEDIMENTOS DE GERENCIAMENTO E FISCALIZAÇÃO

8.1. **ATIVIDADES DO GESTOR DOS SERVIÇOS:** Realiza atividades de controle e a inspeção sistemática do objeto contratado (aquisição de bens, serviços ou obras) pela Administração, com a finalidade de examinar ou verificar se sua execução obedece às especificações, ao projeto, aos prazos estabelecidos e demais obrigações previstas no contrato. Envolve, portanto, responsabilidade com o mérito técnico do que está sendo executado, observadas as condições convencionadas.

8.2. **ATIVIDADES DA GERÊNCIA DE INSTRUMENTALIZAÇÃO:** Realiza atividades de assessorar os gestores das unidades que integram a Direção-Geral, na elaboração dos Projetos Básicos, Termos de Referência e/ou expedientes que visem a contratação de serviços, sistemas ou aquisições, locações ou comodato de bens imóveis, necessárias ou relacionadas ao desenvolvimento da atividade empresarial do Banco e/ou das Empresas Controladas; nas situações em que se vislumbre a necessidade de afastamento de licitação, remeter à Assessoria Jurídica, em conjunto com o gestor do negócio ou serviço ao qual se relaciona o objeto da proposta, o processo com as especificações e razões/justificativas necessárias para que aquela verifique a legalidade do afastamento da licitação e emita parecer sobre o mesmo; assegurar, nas hipóteses de afastamento de licitações, que o processo seja instruído, no que couber, com os elementos referidos no art. 30 - § 3º da Lei 13.303/2016, e nos demais dispositivos legais ou normativos aplicáveis; nos casos de deliberações para abertura de processo licitatório, elaborar,

em conjunto com a Assessoria Jurídica e com o gestor do negócio/processo relacionado, a minuta do edital e do contrato respectivo, e, na sequência, remeter o processo à Comissão de Licitações.

9. ASSINATURAS, LOCAL E DATA

Porto Alegre, 26 de agosto de 2019.

10. IDENTIFICAÇÃO DE ANEXOS

10.1. Anexo - Especificações Técnicas das Soluções de Captura
10.2. Anexo - NDA Acordo de Confidencialidade
10.3. Anexo ao Acordo de Confidencialidade e Sigilo

ITEM 1 - EQUIPAMENTO MOBILE PINPAD

ESPECIFICAÇÕES TÉCNICAS
EQUIPAMENTO MOBILE PINPAD BLUETOOTH

1. CARACTERÍSTICAS GERAIS:
1.1. Terminal deve ser um TRSM (Tamper-Resistant Security Module).
1.2. Dimensões máximas de 140 x 80 x 30 mm (comprimento, largura e altura, respectivamente).
1.3. Peso máximo de 230g.
1.4. Compatível com sistemas operacionais Android e iOS (no mínimo).

2. CARACTERÍSTICAS ESPECÍFICAS:

2.1. MÓDULO DE COMUNICAÇÃO:
2.1.1. Conexão Bluetooth.

2.2. DISPLAY:
2.2.1. Gráfico com resolução mínima de 128 x 32 pixels.
2.2.2. Capacidade de exibir, no mínimo, 2 (duas) linhas de 16 (dezesseis) caracteres por linha.
2.2.3. LCD retro iluminado (mínimo branco).

2.3. TECLADO:
2.3.1. Teclado seguro com, no mínimo, 13 teclas físicas – de 0 (zero) a 9 (nove), entra-limpa/corrige-anula/cancela.
2.3.2. Tecla entra/enter na cor verde.
2.3.3. Tecla anula/corrige/clear na cor amarela.
2.3.4. Tecla cancela/cancel na cor vermelha.
2.3.5. Tecla contendo o número 1 (um) deve estar posicionada no canto superior esquerdo do teclado numérico.
2.3.6. Identificador tátil identificando o número 5 (no centro do teclado) e as teclas entra/enter, anula/corrige/clear e cancela/cancel.

2.4. LEITOR DE CARTÃO MAGNÉTICO:
2.4.1. Leitor de tarja magnética integrado ao corpo do equipamento capaz de ler as trilhas 1 e 2 conforme padrões ISO7810 e ISO7811.
2.4.2. Possuir identificação visual da posição de passagem do cartão.

2.5. LEITOR DE CARTÃO COM CHIP:
2.5.1. Leitor de SmartCard integrado (IFM).
2.5.2. Apresentar tempo máximo de 11 (onze) segundos para uma transação EMV com algoritmo CDA usando um cartão de testes fornecido pelo Banrisul.
2.5.3. Possuir identificação visual da posição de inserção do cartão.

2.6. LEITOR DE CARTÃO CONTACTLESS:
2.6.1. Possuir leitor ISO14443 A/B e Mifare compatível com Mastercard Paypass M/Chip, Mastercard PayPass Magstripe, Visa Paywave MSD, Visa PayWave QVSDC, Discover Zip, American Express ExpressPay e aplicações NFC.
2.6.2. Possuir o módulo Contactless como parte integrante do equipamento, sem a necessidade de acoplar ou acrescentar posteriormente tal funcionalidade.
2.6.3. Possuir identificação visual de equipamento leitor Contactless.

2.7. INTERFACE EXTERNA:
2.7.1. Possuir interface para conexão de cabo de dados e carga da bateria.

2.8. ALIMENTAÇÃO:
2.8.1. Teclas com funções liga e desliga no próprio terminal.

2.8.2. Possuir conjunto completo de carregador (carregador “tomada” + cabo), com variação de voltagem automática de entrada entre 100 e 240v, no mínimo.
2.8.3. Bateria interna de no mínimo 400 mAh.
2.8.4. Deve permitir configuração para desativação automática por ociosidade.

3. SOFTWARE:
3.1. O equipamento deve ser compatível com aplicativo (App) Vero Up, desenvolvido para sistemas operacionais Android e iOS, executado em smartphones, baseado nas especificações técnicas da Vero/Banrisul.

4. SEGURANÇA / CRIPTOGRAFIA:
4.1. Comunicação bluetooth:
4.1.1. O equipamento deve ser capaz de operar com o modo de segurança 3 (ou superior) do protocolo bluetooth.
4.2. Chaves criptográficas:
4.2.1. Cumprir os requisitos de carga de tabelas da especificação do protocolo de comunicação de equipamentos ABECS, versão 2.03 ou superior.
4.3. Todo o gerenciamento e o armazenamento de chaves criptográficas devem estar em conformidade ao estipulado na norma “payment card industry - pin security requirements”, sendo que se destacam os seguintes itens:
4.3.1. Toda chave criptográfica utilizada deve ser armazenada em hsm que esteja em conformidade com os padrões de segurança fips 140-2 level 3 ou 4, não sendo aceita a utilização de chaves criptográficas armazenadas em claro (plain text), em aplicação ou arquivo.
4.3.2. Todo processamento criptográfico deve ser realizado somente por hardware.
4.3.3. Deve haver segregação de ambientes para produção e testes, sendo que nenhuma chave criptográfica pode ser compartilhada entre os ambientes.
4.3.4. Toda chave criptográfica deve ser destinada exclusivamente para sua finalidade, por exemplo, chaves para proteção de pin não podem ser utilizadas como transporte de chaves.
4.3.5. Todo o gerenciamento de chaves criptográficas e acesso ao hsm, deve ser realizado sob duplo controle de acesso.
4.3.6. Deve haver trilhas de auditoria que documentem todo o acesso físico e lógico ao hsm.
4.3.7. Deve haver processos documentados referentes ao gerenciamento de chaves criptográficas, bem como de manutenção dos dispositivos criptográficos.
4.4. O equipamento deve estar apto a trabalhar com os métodos de gerenciamento de chaves criptográficas dukpt, conforme definido na norma ans x9.24-1:2009.
4.5. O equipamento deve possibilitar o armazenamento de pelo menos duas chaves dukpt.
4.6. O equipamento deve suportar a captura e criptografia de pin utilizando chaves dukpt.
4.7. O equipamento deve suportar a captura e criptografia de dados utilizando chaves dukpt.
4.8. As informações sensíveis do cartão (trilha2, pan e data de validade) devem ser enviadas ao dispositivo móvel criptografada com a chave dukpt fornecida pelo Banrisul.
4.9. O Banrisul pode solicitar formalmente, a qualquer momento, que o fornecedor destrua chaves criptográficas especificadas e o fornecedor deve apresentar documento registrando o processo de destruição.
4.10. Deve haver documentos descrevendo o plano de continuidade de negócio, referente ao comprometimento de chaves criptográficas ou a perda de chaves.
4.11. O Banrisul pode solicitar, a qualquer momento, o envio de documentos e evidências referentes ao objeto do contrato, como processos criptográficos, gerenciamento de chaves, plano de continuidade de negócio, inclusive trilhas de auditoria relacionados à eventos e incidentes.
4.12. Para o processo de troca de chaves criptográficas entre as instituições, o fornecedor deve seguir o processo de cerimonial de inserção de chaves a ser fornecido posteriormente pelo Banrisul. Este processo deverá ser executado na presença dos representantes do Banrisul (custodiantes).
4.13. O cerimonial de inserção de chaves deve acontecer no ambiente do fornecedor. Este ambiente deve atender aos seguintes requisitos:
4.13.1. Possuir acesso restrito, sob controle duplo de acesso.
4.13.2. Possuir trilhas de auditoria registrando os acessos.
4.13.3. Possuir monitoração por cftv, sendo que as imagens captadas por este dispositivo devem ser armazenadas por no mínimo 45 dias.
4.13.4. O cftv não deve possibilitar a visualização dos componentes a serem digitados.

4.13.5. Possuir mecanismos que impeçam a visualização dos componentes digitados, por outras pessoas que não sejam o custodiante do componente.
4.13.6. Deverá ser aprovado pelo Banrisul.
4.14. O fornecedor deve seguir os seguintes requisitos mínimos para a destruição de chaves criptográficas:
4.14.1. Sempre que o Banrisul informar e solicitar a exclusão de uma chave a mesma deve ser imediatamente apagada do hsm em que está armazenada.
4.14.2. Os procedimentos devem garantir que a chave seja integralmente destruída, incluindo eventuais cópias de backup.
4.14.3. Os procedimentos devem ser acompanhados por no mínimo duas testemunhas.
4.14.4. Os procedimentos devem ser registrados em ata e devem ser colhidas as assinaturas dos participantes e testemunhas.
4.14.5. Cópia da ata deve ser encaminhada o Banrisul para arquivamento na sala de segurança da unidade de segurança da tecnologia da informação, juntamente das demais documentações da chave.
4.14.6. O inventário de chaves deve manter registro da cerimônia de destruição de chaves.
4.15. Requisitos mínimos para chaves criptográficas e criptografia de pin:
4.15.1. As chaves criptográficas devem ser definidas de acordo com a necessidade identificada, respeitando, obrigatoriamente, os seguintes critérios e requisitos mínimos:
4.15.1.1. Toda criptografia simétrica baseada em algoritmo 3des deve usar chaves de, no mínimo, 16 bytes.
4.15.1.2. Chaves de transporte de chaves (kek – key encryption keys) devem ser tão fortes quanto as chaves que serão transportadas.

5. CERTIFICAÇÕES:
5.1. Referente ao módulo leitor de certificação EMV 4.0 (ou superior) nível 1:
5.1.1. CONTATO:
5.1.1.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.1.2. Carta declaratória comprovando homologação TQM (Terminal Quality Management).
5.1.2. SEM CONTATO:
5.1.2.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.2.2. Carta declaratória comprovando homologação/certificação TQM (Terminal Quality Management).
5.1.2.3. Carta declaratória comprovando homologação/certificação kernel Visa (msd e qvsdc, versão vcps 2.1 ou superior).
5.1.2.4. Carta declaratória comprovando homologação/certificação kernel MasterCard (magstripe e m/chip, versão mci 3.0 ou superior).
5.1.2.5. Carta declaratória comprovando homologação/certificação kernel Discover.
5.1.2.6. Constar na lista vigente de leitores aprovados pela EMVco Type Approval Contactless Level 1 (EMV 2.0 ou superior) a ser comprovado através de cópia do certificado.
5.2. Referente ao núcleo (kernel) EMV com certificação EMV 4.0 (ou superior) nível 2: carta declaratória identificando o kernel EMV de forma que permita a consulta na seção “emv type approved level 2 application kernels” no site www.emvco.com.
5.3. Ainda referente a certificação EMV 4.0 nível 2, deve possuir as seguintes características relacionadas ao kernel da aplicação EMV, presentes na emvco letter of approval - terminal level 2:
- terminal type: 22
- manual key entry: yes
- magnetic stripe: yes
- ic with contacts: yes
- plaintext pin for icc verification: yes
- online enciphered pin: yes
- signature (paper): yes
- offline enciphered pin: yes
- no cvm: yes
- sda: yes
- dda: yes
- cda: yes
- goods: yes
- services: yes
- cash back: yes
- numeric keys: yes

- alpha and special char keys: yes
- command keys: yes
- function keys: yes
- print, attendant: yes
- display, attendant: yes
- code table 1: yes

5.4. Referente a certificação PCI Security Standards Council: carta declaratória identificando o equipamento, versão de firmware e versão de hardware, de forma que permita a sua identificação no site do “pci security standards – pin transaction security devices”, versão 3.0 ou superior, do tipo on-line e off-line (https://www.pcisecuritystandards.org).
5.5. Referente à certificação da Associação Brasileira de Empresas de Cartões de Crédito (ABECS): o equipamento deve ser homologado pelo comitê ABECS, sendo possível identificá-lo junto ao site da ABECS em http://www.abecs.org.br.
5.6. Referente à certificação Anatel: o equipamento deve possuir carta declaratória da Anatel comprovando que as interfaces de rede contidas no equipamento foram homologadas.
5.7. Referente certificação PCI PIN Security, a empresa deverá apresentar atestado de conformidade emitido por entidade competente, sendo possível identificá-lo junto aos sites PCI ou das bandeiras.
5.8. Certificado PCI PTS.

6. DOCUMENTAÇÃO:
6.1. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

ITEM 2 - EQUIPAMENTO MOBILE POS

ESPECIFICAÇÕES TÉCNICAS
EQUIPAMENTO MOBILE POS 3G/WIFI

1. CARACTERÍSTICAS GERAIS:
1.1. Terminal deve ser um TRSM (Tamper-Resistant Security Module).
1.2. Permitir operação totalmente independente de base de apoio através de bateria própria.
1.3. Terminal deve ser um mPOS (mobile point of sale), operando com aplicação embarcada homologada pela Vero/Banrisul.

2. CARACTERÍSTICAS ESPECÍFICAS:

2.1. PROCESSADOR:
2.1.1. No mínimo microprocessador de 32 bits.

2.2. MEMÓRIA:
2.2.1. No mínimo 64 mb – ram e 128 mb – flash

2.3. MÓDULO DE COMUNICAÇÃO:
2.3.1. Comunicação sem fio.
2.3.2. Suporte a redes WiFi.
2.3.3. Suporte a rede de telefonia móvel 3G/2G/GSM/GPRS – Quad Band classe 10 (900-1800 mhz e 850-1900 mhz), permitindo downgrade conforme infraestrutura do local.
2.3.4. Capacidade de contingenciamento entre comunicações.

2.4. DISPLAY:
2.4.1. Colorido – no mínimo 240 x 120 pixels.
2.4.2. Capacidade de exibir no mínimo 5 (cinco) linhas de 20 (vinte) caracteres por linha.

2.5. RELÓGIO – CALENDÁRIO:
2.5.1. Autonomia mínima de 5 (cinco) anos devendo manter a data/hora independente do fornecimento de energia para o terminal.
2.5.2. Independente das aplicações Vero/Banrisul.
2.5.3. Gerenciamento automático de ano bissexto.

2.6. TECLADO:
2.6.1. Teclado seguro com no mínimo 15 teclas físicas de 0 (zero) a 9 (nove), entra, anula, cancela e de função.
2.6.2. Tecla entra/enter na cor verde.
2.6.3. Tecla anula/corrige/clear na cor amarela.
2.6.4. Tecla cancela/cancel na cor vermelha.
2.6.5. Tecla contendo o número 1 (um) deve estar posicionada no canto superior esquerdo do teclado numérico.
2.6.6. Identificador tátil identificando o número 5 (no centro do teclado) e as teclas entra/enter, anula/corrige/clear e cancela/cancel.

2.7. LEITOR DE CARTÃO MAGNÉTICO:
2.7.1. Leitor de tarja magnética integrado ao corpo do equipamento capaz de ler as trilhas 1 e 2 conforme padrões ISO7810 e ISO7811.
2.7.2. Possuir identificação visual da posição de passagem do cartão.

2.8. LEITOR DE CARTÃO COM CHIP:
2.8.1. Leitor de SmartCard integrado (IFM).
2.8.2. Apresentar tempo máximo de 11 (onze) segundos para uma transação EMV com algoritmo CDA usando um cartão de testes fornecido pelo Banrisul.

2.8.3. Possuir identificação visual da posição de inserção do cartão.

2.9. LEITOR DE CARTÃO CONTACTLESS:
2.9.1. Possuir leitor ISO14443 A/B e Mifare compatível com Mastercard Paypass M/Chip, Mastercard PayPass Magstripe, Visa Paywave MSD, Visa PayWave QVSDC, Discover Zip, American Express ExpressPay e aplicações NFC.
2.9.2. Possuir o módulo Contactless como parte integrante do equipamento, sem a necessidade de acoplar ou acrescentar posteriormente tal funcionalidade.
2.9.3. Possuir identificação visual de equipamento leitor Contactless.

2.10. INTERFACE EXTERNA:
2.10.1. Possuir interface para conexão de cabo de dados e carga da bateria.

2.11. ALIMENTAÇÃO:
2.11.1. Teclas com funções liga e desliga no próprio terminal.
2.11.2. Possuir conjunto completo de carregador (carregador "tomada" + cabo), com variação de voltagem automática de entrada entre 100 e 240v, no mínimo.
2.11.3. Bateria interna de no mínimo 1200 mAh.
2.11.4. Deve permitir configuração para desativação automática por ociosidade.

3. SOFTWARE:
3.1. O equipamento deve ser compatível e disponibilizado com aplicação de meios de pagamento Vero/Banrisul.
3.2. As especificações técnicas para desenvolvimento e integração referentes ao item 3.1 serão fornecidas pela Vero/Banrisul após assinatura de NDA.

4. SEGURANÇA / CRIPTOGRAFIA:
4.1. O equipamento deve estar apto a trabalhar com o método de gerenciamento de chaves criptográficas DUKPT conforme definido na norma ANS x9.24-1:2009.
4.2. O equipamento deve suportar a captura e criptografia de PIN e dados utilizando chaves do método DUKPT.
4.3. As chaves DUKPT devem ser armazenadas de acordo com as especificações Vero/Banrisul;
4.4. O equipamento deve possuir quantidade de slots suficientes para suportar a gravação de todas as chaves Vero/Banrisul.
4.5. O equipamento deve suportar a gravação de no mínimo 2 chaves criptográficas 3-des Vero/Banrisul, de no mínimo 16 bytes cada uma, para utilização com o método de gerenciamento de chaves DUKPT (uma para PIN e outra para dados).
4.6. O equipamento deve ser fornecido com a versão vigente do Mapa de Chaves da ABECS devidamente carregado, contendo as chaves Vero/Banrisul e demais autorizadas.
4.7. As chaves criptográficas a serem inseridas nos equipamentos serão geradas e inseridas pelo Banrisul no HSM do fornecedor, através de processo a ser definido posteriormente entre as empresas.
4.8. O Banrisul pode a qualquer momento solicitar formalmente que a empresa destrua as informações referente as suas chaves criptográficas.
4.9. Os equipamentos de teste e homologação devem ser carregados com chaves de testes.
4.10. As chaves de teste não podem ser carregadas no ambiente de produção.
4.11. O fornecedor deverá sempre possuir o Mapa de chaves da ABECS em sua última versão, garantindo assim que, havendo necessidade de manutenção nos equipamentos da Vero, os mesmos possam receber em laboratório sempre o Mapa de chaves da ABECS mais recente.

5. CERTIFICAÇÕES:
5.1. Referente ao módulo leitor de certificação EMV 4.0 (ou superior) nível 1:
5.1.1. CONTATO:
5.1.1.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.1.2. Carta declaratória comprovando homologação TQM (Terminal Quality Management).
5.1.2. SEM CONTATO:
5.1.2.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.2.2. Carta declaratória comprovando homologação/certificação TQM (Terminal Quality Management).

5.1.2.3. Carta declaratória comprovando homologação/certificação kernel Visa (msd e qvsdc, versão vcps 2.1 ou superior).
5.1.2.4. Carta declaratória comprovando homologação/certificação kernel MasterCard (magstripe e m/chip, versão mci 3.0 ou superior).
5.1.2.5. Carta declaratória comprovando homologação/certificação kernel Discover.
5.1.2.7. Constar na lista vigente de leitores aprovados pela EMVco Type Approval Contactless Level 1 (EMV 2.0 ou superior) a ser comprovado através de cópia do certificado.
5.2. Referente ao núcleo (kernel) EMV com certificação EMV 4.0 (ou superior) nível 2: carta declaratória identificando o kernel EMV de forma que permita a consulta na seção “emv type approved level 2 application kernels” no site www.emvco.com.
5.3. Ainda referente a certificação EMV 4.0 nível 2, deve possuir as seguintes características relacionadas ao kernel da aplicação EMV, presentes na emvco letter of approval - terminal level 2:
- terminal type: 22
- manual key entry: yes
- magnetic stripe: yes
- ic with contacts: yes
- plaintext pin for icc verification: yes
- online enciphered pin: yes
- signature (paper): yes
- offline enciphered pin: yes
- no cvm: yes
- sda: yes
- dda: yes
- cda: yes
- goods: yes
- services: yes
- cash back: yes
- numeric keys: yes
- alpha and special char keys: yes
- command keys: yes
- function keys: yes
- print, attendant: yes
- display, attendant: yes
- code table 1: yes

5.4. Referente a certificação PCI Security Standards Council: carta declaratória identificando o equipamento, versão de firmware e versão de hardware, de forma que permita a sua identificação no site do “pci security standards – pin transaction security devices”, versão 3.0 ou superior, do tipo on-line e off-line (https://www.pcisecuritystandards.org).
5.5. Referente à certificação da Associação Brasileira de Empresas de Cartões de Crédito (ABECS): o equipamento deve ser homologado pelo comitê ABECS, sendo possível identificá-lo junto ao site da ABECS em http://www.abecs.org.br.
5.6. Referente à certificação Anatel: o equipamento deve possuir carta declaratória da Anatel comprovando que as interfaces de rede contidas no equipamento foram homologadas.
5.7. Referente certificação PCI PIN Security, a empresa deverá apresentar atestado de conformidade emitido por entidade competente, sendo possível identificá-lo junto aos sites PCI ou das bandeiras.
5.8. Certificado PCI PTS.

6. DOCUMENTAÇÃO:
6.1. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

ITEM 3 - EQUIPAMENTO POS FIXO

ESPECIFICAÇÕES TÉCNICAS
EQUIPAMENTO POS COMBO HDLC/ADSL

1. CARACTERÍSTICAS GERAIS:
1.1. Terminal deve ser um TRSM (Tamper-Resistant Security Module).
1.2. Terminal deve ser um POS (Point of Sale).
1.3. Terminal deve ter suporte para bobinas termossensíveis com no mínimo 57 mm de largura por 35 mm de espessura.

2. CARACTERÍSTICAS ESPECÍFICAS:

2.1. PROCESSADOR:
2.1.1. No mínimo microprocessador 32 bits.

2.2. MEMÓRIA:
2.2.1. No mínimo 128 Mb – Ram e 256 Mb – Flash.

2.3. MÓDULO DE COMUNICAÇÃO:
2.3.1. Suporte a rede de internet banda larga com cabo ethernet/ADSL.
2.3.2. Suporte a rede de telefonia fixa com cabo dial/HDLC.
2.3.3. Capacidade de contingenciamento entre comunicações internet banda larga e telefonia fixa.

2.4. DISPLAY:
2.4.1. Colorido – no mínimo 240 x 320 pixels.
2.4.2. Capacidade de exibir no mínimo 5 (cinco) linhas de 20 (vinte) caracteres por linha.
2.4.3. Display touchscreen (opcional).

2.5. RELÓGIO – CALENDÁRIO:
2.5.1. Autonomia mínima de 5 (cinco) anos devendo manter a data/hora independente do fornecimento de energia para o terminal.
2.5.2. Independente das aplicações Vero/Banrisul.
2.5.3. Gerenciamento automático de ano bissexto.

2.6. TECLADO:
2.6.1. Teclado seguro com no mínimo 15 teclas físicas de 0 (zero) a 9 (nove), entra, anula, cancela e de função.
2.6.2. Tecla entra/enter na cor verde.
2.6.3. Tecla anula/corrige/clear na cor amarela.
2.6.4. Tecla cancela/cancel na cor vermelha.
2.6.5. Tecla contendo o número 1 (um) deve estar posicionada no canto superior esquerdo do teclado numérico.
2.6.6. Identificador tátil identificando o número 5 (no centro do teclado) e as teclas entra/enter, anula/corrige/clear e cancela/cancel.

2.7. LEITOR DE CARTÃO MAGNÉTICO:
2.7.1. Leitor de tarja magnética integrado ao corpo do equipamento capaz de ler as trilhas 1 e 2 conforme padrões ISO7810 e ISO7811.
2.7.2. Possuir identificação visual da posição de passagem do cartão.

2.8. LEITOR DE CARTÃO COM CHIP:
2.8.1. Leitor de SmartCard integrado (IFM).
2.8.2. Apresentar tempo máximo de 11 (onze) segundos para uma transação EMV com algoritmo CDA usando um cartão de testes fornecido pelo Banrisul.
2.8.3. Possuir identificação visual da posição de inserção do cartão.

2.9. LEITOR DE CARTÃO CONTACTLESS:
2.9.1. Possuir leitor ISO14443 A/B e Mifare compatível com Mastercard Paypass M/Chip, Mastercard PayPass Magstripe, Visa Paywave MSD, Visa PayWave QVSDC, Discover Zip, American Express ExpressPay e aplicações NFC.
2.9.2. Possuir o módulo Contactless como parte integrante do equipamento, sem a necessidade de acoplar ou acrescentar posteriormente tal funcionalidade.
2.9.3. Possuir identificação visual de equipamento leitor Contactless.

2.10. INTERFACE EXTERNA:
2.10.1. Possuir interface para conexão de cabo de dados e fonte de alimentação.

2.11. ALIMENTAÇÃO:
2.11.1. Teclas com funções liga e desliga no próprio terminal (Opcional).
2.11.2. Possuir fonte de alimentação externa, com variação de voltagem automática de entrada entre 100 e 240v, no mínimo.

3. SOFTWARE:
3.1. O equipamento deve ser compatível e disponibilizado com aplicação de meios de pagamento Vero/Banrisul.
3.2. A aplicação mencionada no item 3.1 deve ser compatível com o marketplace de aplicações da Vero, denominado Vero Store, que é a plataforma responsável pelas atualizações de software da solução de forma remota.
3.3. As especificações técnicas para desenvolvimento e integração referentes aos itens 3.1 e 3.2 serão fornecidas pela Vero/Banrisul após assinatura de NDA.

4. SEGURANÇA / CRIPTOGRAFIA:
4.1. O equipamento deve estar apto a trabalhar com o método de gerenciamento de chaves criptográficas DUKPT conforme definido na norma ANS x9.24-1:2009.
4.2. O equipamento deve suportar a captura e criptografia de PIN e dados utilizando chaves do método DUKPT.
4.3. As chaves DUKPT devem ser armazenadas de acordo com as especificações Vero/Banrisul;
4.4. O equipamento deve possuir quantidade de slots suficientes para suportar a gravação de todas as chaves Vero/Banrisul.
4.5. O equipamento deve suportar a gravação de no mínimo 2 chaves criptográficas 3-des Vero/Banrisul, de no mínimo 16 bytes cada uma, para utilização com o método de gerenciamento de chaves DUKPT (uma para PIN e outra para dados).
4.6. O equipamento deve ser fornecido com a versão vigente do Mapa de Chaves da ABECS devidamente carregado, contendo as chaves Vero/Banrisul e demais autorizadas.
4.7. As chaves criptográficas a serem inseridas nos equipamentos serão geradas e inseridas pelo Banrisul no HSM do fornecedor, através de processo a ser definido posteriormente entre as empresas.
4.8. O Banrisul pode a qualquer momento solicitar formalmente que a empresa destrua as informações referente as suas chaves criptográficas.
4.9. Os equipamentos de teste e homologação devem ser carregados com chaves de testes.
4.10. As chaves de teste não podem ser carregadas no ambiente de produção.
4.11. O fornecedor deverá sempre possuir o Mapa de chaves da ABECS em sua última versão, garantindo assim que, havendo necessidade de manutenção nos equipamentos da Vero, os mesmos possam receber em laboratório sempre o Mapa de chaves da ABECS mais recente.

5. CERTIFICAÇÕES:
5.1. Referente ao módulo leitor de certificação EMV 4.0 (ou superior) nível 1:
5.1.1. CONTATO:
5.1.1.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.1.2. Carta declaratória comprovando homologação TQM (Terminal Quality Management).
5.1.2. SEM CONTATO:
5.1.2.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.2.2. Carta declaratória comprovando homologação/certificação TQM (Terminal Quality Management).
5.1.2.3. Carta declaratória comprovando homologação/certificação kernel Visa (msd e qvsdc, versão vcps 2.1 ou superior).

5.1.2.4. Carta declaratória comprovando homologação/certificação kernel MasterCard (magstripe e m/chip, versão mci 3.0 ou superior).
5.1.2.5. Carta declaratória comprovando homologação/certificação kernel Discover.
5.1.2.6. Constar na lista vigente de leitores aprovados pela EMVco Type Approval Contactless Level 1 (EMV 2.0 ou superior) a ser comprovado através de cópia do certificado.
5.2. Referente ao núcleo (kernel) EMV com certificação EMV 4.0 (ou superior) nível 2: carta declaratória identificando o kernel EMV de forma que permita a consulta na seção “emv type approved level 2 application kernels” no site www.emvco.com.
5.3. Ainda referente a certificação EMV 4.0 nível 2, deve possuir as seguintes características relacionadas ao kernel da aplicação EMV, presentes na emvco letter of approval -terminal level 2:
- terminal type: 22
- manual key entry: yes
- magnetic stripe: yes
- ic with contacts: yes
- plaintext pin for icc verification: yes
- online enciphered pin: yes
- signature (paper): yes
- offline enciphered pin: yes
- no cvm: yes
- sda: yes
- dda: yes
- cda: yes
- goods: yes
- services: yes
- cash back: yes
- numeric keys: yes
- alpha and special char keys: yes
- command keys: yes
- function keys: yes
- print, attendant: yes
- display, attendant: yes
- code table 1: yes

5.4. Referente a certificação PCI Security Standards Council: carta declaratória identificando o equipamento, versão de firmware e versão de hardware, de forma que permita a sua identificação no site do “pci security standards – pin transaction security devices”, versão 3.0 ou superior, do tipo on-line e off-line (https://www.pcisecuritystandards.org).
5.5. Referente à certificação da Associação Brasileira de Empresas de Cartões de Crédito (ABECS): o equipamento deve ser homologado pelo comitê ABECS, sendo possível identificá-lo junto ao site da ABECS em http://www.abecs.org.br.
5.6. Referente à certificação Anatel: o equipamento deve possuir carta declaratória da Anatel comprovando que as interfaces de rede contidas no equipamento foram homologadas.
5.7. Referente certificação PCI PIN Security, a empresa deverá apresentar atestado de conformidade emitido por entidade competente, sendo possível identificá-lo junto aos sites PCI ou das bandeiras.
5.8. Certificado PCI PTS.

6. DOCUMENTAÇÃO:

6.1. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

ITEM 4 - EQUIPAMENTO POS MÓVEL

ESPECIFICAÇÕES TÉCNICAS
EQUIPAMENTO POS MÓVEL 3G/WIFI

1. CARACTERÍSTICAS GERAIS:

1.1. Terminal deve ser um TRSM (Tamper-Resistant Security Module).
1.2. Terminal deve ser um POS (Point of Sale).
1.3. Terminal deve ter suporte para bobinas termossensíveis com no mínimo 57 mm de largura por 35 mm de espessura.
1.4. Permitir operação totalmente independente de base de apoio através de bateria própria.

2. CARACTERÍSTICAS ESPECÍFICAS:

2.1. PROCESSADOR:
2.1.1. No mínimo microprocessador 32 bits.

2.2. MEMÓRIA:
2.2.1. No mínimo 128 Mb – Ram e 256 Mb – Flash.

2.3. MÓDULO DE COMUNICAÇÃO:
2.3.1. Comunicação sem fio.
2.3.2. Suporte a redes WiFi.
2.3.3. Suporte a rede de telefonia móvel 3G/2G/GSM/GPRS – Quad Band classe 10 (900-1800 mhz e 850-1900 mhz), permitindo downgrade conforme infraestrutura do local.
2.3.4. Capacidade de contingenciamento entre comunicações.

2.4. DISPLAY:
2.4.1. Colorido – no mínimo 240 x 320 pixels.
2.4.2. Capacidade de exibir no mínimo 5 (cinco) linhas de 20 (vinte) caracteres por linha.
2.4.3. Display touchscreen.

2.5. RELÓGIO – CALENDÁRIO:
2.5.1. Autonomia mínima de 5 (cinco) anos devendo manter a data/hora independente do fornecimento de energia para o terminal.
2.5.2. Independente das aplicações Vero/Banrisul.
2.5.3. Gerenciamento automático de ano bissexto.

2.6. TECLADO:
2.6.1. Teclado seguro com no mínimo 15 teclas físicas de 0 (zero) a 9 (nove), entra, anula, cancela e de função.
2.6.2. Tecla entra/enter na cor verde.
2.6.3. Tecla anula/corrige/clear na cor amarela.
2.6.4. Tecla cancela/cancel na cor vermelha.
2.6.5. Tecla contendo o número 1 (um) deve estar posicionada no canto superior esquerdo do teclado numérico.
2.6.6. Identificador tátil identificando o número 5 (no centro do teclado) e as teclas entra/enter, anula/corrige/clear e cancela/cancel.

2.7. LEITOR DE CARTÃO MAGNÉTICO:
2.7.1. Leitor de tarja magnética integrado ao corpo do equipamento capaz de ler as trilhas 1 e 2 conforme padrões ISO7810 e ISO7811.
2.7.2. Possuir identificação visual da posição de passagem do cartão.

2.8. LEITOR DE CARTÃO COM CHIP:
2.8.1. Leitor de SmartCard integrado (IFM).

2.8.2. Apresentar tempo máximo de 11 (onze) segundos para uma transação EMV com algoritmo CDA usando um cartão de testes fornecido pelo Banrisul.
2.8.3. Possuir identificação visual da posição de inserção do cartão.

2.9. LEITOR DE CARTÃO CONTACTLESS:
2.9.1. Possuir leitor ISO14443 A/B e Mifare compatível com Mastercard Paypass M/Chip, Mastercard PayPass Magstripe, Visa Paywave MSD, Visa PayWave QVSDC, Discover Zip, American Express ExpressPay e aplicações NFC.
2.9.2. Possuir o módulo Contactless como parte integrante do equipamento, sem a necessidade de acoplar ou acrescentar posteriormente tal funcionalidade.
2.9.3. Possuir identificação visual de equipamento leitor Contactless.

2.10. INTERFACE EXTERNA:
2.10.1. Possuir interface para conexão de cabo de dados e carga da bateria.

2.11. ALIMENTAÇÃO:
2.11.1. Teclas com funções liga e desliga no próprio terminal.
2.11.2. Possuir conjunto completo de carregador (carregador "tomada" + cabo), com variação de voltagem automática de entrada entre 100 e 240v, no mínimo.
2.11.3. Bateria interna de no mínimo 2500 mAh.
2.11.4. Deve permitir configuração para desativação automática por ociosidade.

3. SOFTWARE:
3.1. O equipamento deve ser compatível e disponibilizado com aplicação de meios de pagamento Vero/Banrisul.
3.2. A aplicação mencionada no item 3.1 deve ser compatível com o marketplace de aplicações da Vero, denominado Vero Store, que é a plataforma responsável pelas atualizações de software da solução de forma remota.
3.3. As especificações técnicas para desenvolvimento e integração referentes aos itens 3.1 e 3.2 serão fornecidas pela Vero/Banrisul após assinatura de NDA.

4. SEGURANÇA / CRIPTOGRAFIA:
4.1. O equipamento deve estar apto a trabalhar com o método de gerenciamento de chaves criptográficas DUKPT conforme definido na norma ANS x9.24-1:2009.
4.2. O equipamento deve suportar a captura e criptografia de PIN e dados utilizando chaves do método DUKPT.
4.3. As chaves DUKPT devem ser armazenadas de acordo com as especificações Vero/Banrisul;
4.4. O equipamento deve possuir quantidade de slots suficientes para suportar a gravação de todas as chaves Vero/Banrisul.
4.5. O equipamento deve suportar a gravação de no mínimo 2 chaves criptográficas 3-des Vero/Banrisul, de no mínimo 16 bytes cada uma, para utilização com o método de gerenciamento de chaves DUKPT (uma para PIN e outra para dados).
4.6. O equipamento deve ser fornecido com a versão vigente do Mapa de Chaves da ABECS devidamente carregado, contendo as chaves Vero/Banrisul e demais autorizadas.
4.7. As chaves criptográficas a serem inseridas nos equipamentos serão geradas e inseridas pelo Banrisul no HSM do fornecedor, através de processo a ser definido posteriormente entre as empresas.
4.8. O Banrisul pode a qualquer momento solicitar formalmente que a empresa destrua as informações referente as suas chaves criptográficas.
4.9. Os equipamentos de teste e homologação devem ser carregados com chaves de testes.
4.10. As chaves de teste não podem ser carregadas no ambiente de produção.
4.11. O fornecedor deverá sempre possuir o Mapa de chaves da ABECS em sua última versão, garantindo assim que, havendo necessidade de manutenção nos equipamentos da Vero, os mesmos possam receber em laboratório sempre o Mapa de chaves da ABECS mais recente.

5. CERTIFICAÇÕES:
5.1. Referente ao módulo leitor de certificação EMV 4.0 (ou superior) nível 1:
5.1.1. CONTATO:
5.1.1.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.

5.1.1.2. Carta declaratória comprovando homologação TQM (Terminal Quality Management).
5.1.2. SEM CONTATO:
5.1.2.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.2.2. Carta declaratória comprovando homologação/certificação TQM (Terminal Quality Management).
5.1.2.3. Carta declaratória comprovando homologação/certificação kernel Visa (msd e qvsdc, versão vcps 2.1 ou superior).
5.1.2.4. Carta declaratória comprovando homologação/certificação kernel MasterCard (magstripe e m/chip, versão mci 3.0 ou superior).
5.1.2.5. Carta declaratória comprovando homologação/certificação kernel Discover.
5.1.2.6. Constar na lista vigente de leitores aprovados pela EMVco Type Approval Contactless Level 1 (EMV 2.0 ou superior) a ser comprovado através de cópia do certificado.
5.2. Referente ao núcleo (kernel) EMV com certificação EMV 4.0 (ou superior) nível 2: carta declaratória identificando o kernel EMV de forma que permita a consulta na seção “emv type approved level 2 application kernels” no site www.emvco.com.
5.3. Ainda referente a certificação EMV 4.0 nível 2, deve possuir as seguintes características relacionadas ao kernel da aplicação EMV, presentes na emvco letter of approval - terminal level 2:
- terminal type: 22
- manual key entry: yes
- magnetic stripe: yes
- ic with contacts: yes
- plaintext pin for icc verification: yes
- online enciphered pin: yes
- signature (paper): yes
- offline enciphered pin: yes
- no cvm: yes
- sda: yes
- dda: yes
- cda: yes
- goods: yes
- services: yes
- cash back: yes
- numeric keys: yes
- alpha and special char keys: yes
- command keys: yes
- function keys: yes
- print, attendant: yes
- display, attendant: yes
- code table 1: yes

5.4. Referente a certificação PCI Security Standards Council: carta declaratória identificando o equipamento, versão de firmware e versão de hardware, de forma que permita a sua identificação no site do “pci security standards – pin transaction security devices”, versão 3.0 ou superior, do tipo on-line e off-line (https://www.pcisecuritystandards.org).
5.5. Referente à certificação da Associação Brasileira de Empresas de Cartões de Crédito (ABECS): o equipamento deve ser homologado pelo comitê ABECS, sendo possível identificá-lo junto ao site da ABECS em http://www.abecs.org.br.
5.6. Referente à certificação Anatel: o equipamento deve possuir carta declaratória da Anatel comprovando que as interfaces de rede contidas no equipamento foram homologadas.
5.7. Referente certificação PCI PIN Security, a empresa deverá apresentar atestado de conformidade emitido por entidade competente, sendo possível identificá-lo junto aos sites PCI ou das bandeiras.
5.8. Certificado PCI PTS.

6. DOCUMENTAÇÃO:

6.1. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e

requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

ITEM 5 - EQUIPAMENTO SMARTPOS

ESPECIFICAÇÕES TÉCNICAS
EQUIPAMENTO SMARTPOS ANDROID 4G/WIFI

1. CARACTERÍSTICAS GERAIS:

1.1. Terminal deve ser um TRSM (Tamper-Resistant Security Module).
1.2. Terminal deve ser um POS (Point of Sale), operando com aplicação homologada pela Vero/Banrisul.
1.3. Terminal deve ter suporte para bobinas termossensíveis com no mínimo 57 mm de largura por 35 mm de espessura.

2. CARACTERÍSTICAS ESPECÍFICAS:

2.1. PROCESSADOR:
2.1.1. No mínimo microprocessador Quadcore 32 bits.

2.2. MEMÓRIA:
2.2.1. No mínimo 1 Gb – Ram e 8 Gb – Flash.

2.3. MÓDULO DE COMUNICAÇÃO:
2.3.1. Comunicação sem fio.
2.3.2. Suporte a redes WiFi.
2.3.3. Suporte a rede de telefonia móvel, no mínimo 3G/2G/GSM/GPRS – Quad Band classe 10 (900-1800 mhz e 850-1900 mhz), permitindo downgrade conforme infraestrutura do local.
2.3.4. Capacidade de contingenciamento entre comunicações.

2.4. DISPLAY:
2.4.1. Touchscreen – colorido – no mínimo 800 x 480 pixels.

2.5. RELÓGIO – CALENDÁRIO:
2.5.1. Autonomia mínima de 5 (cinco) anos devendo manter a data/hora independente do fornecimento de energia para o terminal.
2.5.2. Independente das aplicações Vero/Banrisul.
2.5.3. Gerenciamento automático de ano bissexto.

2.6. TECLADO:
2.6.1. Teclado seguro com no mínimo 15 teclas físicas e/ou virtuais – de 0 (zero) a 9 (nove), entra, anula, cancela e de função.
2.6.2. Tecla entra/enter na cor verde.
2.6.3. Tecla anula/corrige/clear na cor amarela.
2.6.4. Tecla cancela/cancel na cor vermelha.
2.6.5. Tecla contendo o número 1 (um) deve estar posicionada no canto superior esquerdo do teclado numérico.
2.6.6. Para teclado físico deve possuir identificador tátil identificando o número 5 (no centro do teclado) e as teclas entra/enter, anula/corrige/clear e cancela/cancel.
2.6.7. Para teclado virtual, na ausência de teclado físico, deve obrigatoriamente possuir película com os mesmos identificadores táteis de um teclado físico, de acordo com o padrão sugerido pela ABECS.

2.7. LEITOR DE CARTÃO MAGNÉTICO:
2.7.1. Leitor de tarja magnética integrado ao corpo do equipamento capaz de ler as trilhas 1 e 2 conforme padrões ISO7810 e ISO7811.
2.7.2. Possuir identificação visual da posição de passagem do cartão.

2.8. LEITOR DE CARTÃO COM CHIP:
2.8.1. Leitor de SmartCard integrado (IFM).

2.8.2. Apresentar tempo máximo de 11 (onze) segundos para uma transação EMV com algoritmo CDA usando um cartão de testes fornecido pelo Banrisul.
2.8.3. Possuir identificação visual da posição de inserção do cartão.

2.9. LEITOR DE CARTÃO CONTACTLESS:
2.9.1. Possuir leitor ISO14443 A/B e Mifare compatível com Mastercard Paypass M/Chip, Mastercard PayPass Magstripe, Visa Paywave MSD, Visa PayWave QVSDC, Discover Zip, American Express ExpressPay e aplicações NFC.
2.9.2. Possuir o módulo Contactless como parte integrante do equipamento, sem a necessidade de acoplar ou acrescentar posteriormente tal funcionalidade.
2.9.3. Possuir identificação visual de equipamento leitor Contactless.

2.10. INTERFACE EXTERNA:
2.10.1. Possuir interface para conexão de cabo de dados e carga da bateria.

2.11. ALIMENTAÇÃO:
2.11.1. Teclas com funções liga e desliga no próprio terminal.
2.11.2. Possuir conjunto completo de carregador (carregador "tomada" + cabo), com variação de voltagem automática de entrada entre 100 e 240v, no mínimo.
2.11.3. Bateria interna de no mínimo 3400 mAh.
2.11.4. Deve permitir configuração para desativação automática por ociosidade.

3. SOFTWARE:
3.1. Sistema Operacional Android versão mínima 5.0 ou superior.
3.2. O equipamento deve ser compatível e disponibilizado com aplicação de meios de pagamento Vero/Banrisul.
3.3. A aplicação mencionada no item 3.2 deve ser compatível com o marketplace de aplicações da Vero, denominado Vero Store, que é a plataforma responsável pelas atualizações de software da solução de forma remota.
3.4. As especificações técnicas para desenvolvimento e integração referentes aos itens 3.2 e 3.3 serão fornecidas pela Vero/Banrisul após assinatura de NDA.
3.5. Deve ser possível atualizar remotamente, via Vero Store, o sistema operacional, firmwares, kernels, entre outros componentes de responsabilidade do fabricante do equipamento.

4. SEGURANÇA / CRIPTOGRAFIA:
4.1. O equipamento deve estar apto a trabalhar com o método de gerenciamento de chaves criptográficas DUKPT conforme definido na norma ANS x9.24-1:2009.
4.2. O equipamento deve suportar a captura e criptografia de PIN e dados utilizando chaves do método DUKPT.
4.3. As chaves DUKPT devem ser armazenadas de acordo com as especificações Vero/Banrisul;
4.4. O equipamento deve possuir quantidade de slots suficientes para suportar a gravação de todas as chaves Vero/Banrisul.
4.5. O equipamento deve suportar a gravação de no mínimo 2 chaves criptográficas 3-des Vero/Banrisul, de no mínimo 16 bytes cada uma, para utilização com o método de gerenciamento de chaves DUKPT (uma para PIN e outra para dados).
4.6. O equipamento deve ser fornecido com a versão vigente do Mapa de Chaves da ABECS devidamente carregado, contendo as chaves Vero/Banrisul e demais autorizadas.
4.7. As chaves criptográficas a serem inseridas nos equipamentos serão geradas e inseridas pelo Banrisul no HSM do fornecedor, através de processo a ser definido posteriormente entre as empresas.
4.8. O Banrisul pode a qualquer momento solicitar formalmente que a empresa destrua as informações referente as suas chaves criptográficas.
4.9. Os equipamentos de teste e homologação devem ser carregados com chaves de testes.
4.10. As chaves de teste não podem ser carregadas no ambiente de produção.
4.11. O fornecedor deverá sempre possuir o Mapa de chaves da ABECS em sua última versão, garantindo assim que, havendo necessidade de manutenção nos equipamentos da Vero, os mesmos possam receber em laboratório sempre o Mapa de chaves da ABECS mais recente.
4.12. O equipamento não deve permitir a carga de aplicações que não sejam assinadas e autorizadas pela Vero/Banrisul.

4.13. O equipamento deve possuir proteções contra liberação de root no sistema operacional.
4.14. O equipamento deve possuir proteções contra captura de tela via sistema operacional.
4.15. O equipamento deve possuir mecanismos de segurança para garantir que comunique apenas com o marketplace indicado/configurado pela Vero/Banrisul;
4.16. O sistema operacional do equipamento deve ser baseado, no mínimo, em Android 5.0 e permitir futuras atualizações do sistema, de forma remota.

5. CERTIFICAÇÕES:
5.1. Referente ao módulo leitor de certificação EMV 4.0 (ou superior) nível 1:
5.1.1. CONTATO:
5.1.1.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.1.2. Carta declaratória comprovando homologação TQM (Terminal Quality Management).
5.1.2. SEM CONTATO:
5.1.2.1. Carta declaratória identificando o componente aprovado no site www.emvco.com.
5.1.2.2. Carta declaratória comprovando homologação/certificação TQM (Terminal Quality Management).
5.1.2.3. Carta declaratória comprovando homologação/certificação kernel Visa (msd e qvsdc, versão vcps 2.1 ou superior).
5.1.2.4. Carta declaratória comprovando homologação/certificação kernel MasterCard (magstripe e m/chip, versão mci 3.0 ou superior).
5.1.2.5. Carta declaratória comprovando homologação/certificação kernel Discover.
5.1.2.6. Constar na lista vigente de leitores aprovados pela EMVco Type Approval Contactless Level 1 (EMV 2.0 ou superior) a ser comprovado através de cópia do certificado.
5.2. Referente ao núcleo (kernel) EMV com certificação EMV 4.0 (ou superior) nível 2: carta declaratória identificando o kernel EMV de forma que permita a consulta na seção “emv type approved level 2 application kernels” no site www.emvco.com.
5.3. Ainda referente a certificação EMV 4.0 nível 2, deve possuir as seguintes características relacionadas ao kernel da aplicação EMV, presentes na emvco letter of approval - terminal level 2:
- terminal type: 22
- manual key entry: yes
- magnetic stripe: yes
- ic with contacts: yes
- plaintext pin for icc verification: yes
- online enciphered pin: yes
- signature (paper): yes
- offline enciphered pin: yes
- no cvm: yes
- sda: yes
- dda: yes
- cda: yes
- goods: yes
- services: yes
- cash back: yes
- numeric keys: yes
- alpha and special char keys: yes
- command keys: yes
- function keys: yes
- print, attendant: yes
- display, attendant: yes
- code table 1: yes

5.4. Referente a certificação PCI Security Standards Council: carta declaratória identificando o equipamento, versão de firmware e versão de hardware, de forma que permita a sua identificação no site do “pci security standards – pin transaction security devices”, versão 3.0 ou superior, do tipo on-line e off-line (https://www.pcisecuritystandards.org).
5.5. Referente à certificação da Associação Brasileira de Empresas de Cartões de Crédito (ABECS): o equipamento deve ser homologado pelo comitê ABECS, sendo possível identificá-lo junto ao site da ABECS em http://www.abecs.org.br.
5.6. Referente à certificação Anatel: o equipamento deve possuir carta declaratória da Anatel comprovando que as interfaces de rede contidas no equipamento foram homologadas.

5.7. Referente certificação PCI PIN Security, a empresa deverá apresentar atestado de conformidade emitido por entidade competente, sendo possível identificá-lo junto aos sites PCI ou das bandeiras.
5.8. Referente ao certificado Software-based PIN Entry on COTS (SPoC): a critério da Vero/Banrisul, poderá ser solicitado atestado de conformidade com o PCI SSC, sendo possível identificá-lo no site deste órgão https://www.pcisecuritystandards.org.
5.9. Certificado PCI PTS.

6. DOCUMENTAÇÃO:
6.1. Todos os processos relacionados com a gestão do ciclo de vida de chaves e ciclo de vida de equipamentos, incluindo processos de comunicação e substituição de chaves em caso de suspeita de comprometimento devem estar documentados e, sempre que solicitado pelo banco, deve ser disponibilizada tal documentação de forma que se comprove o atendimento aos requisitos deste edital e requisitos de segurança das bandeiras capturadas pela Vero. Tais processos podem ser auditados a qualquer momento pela Vero.

UNIDADE/ÁREA: BANRISUL CARTÕES S.A. / GERÊNCIA DE SOLUÇÕES DE CAPTURA.
GESTOR: HUMBERTO SKUERESKY SIEBEN DA SILVA.
ÚLTIMA ATUALIZAÇÃO: 15/08/2019.

ACORDO DE CONFIDENCIALIDADE E SIGILO

Banrisul Cartões S.A., com sede na Rua Caldas Júnior, 120, 11º andar, em Porto Alegre, RS, inscrita no CNPJ sob o nº 92.934.215/0001-06, por seu representante legal no fim assinado, doravante denominado **BANRISUL CARTÕES**,
e
(nome fantasia ou razão social), com sede na (--Endereço da empresa --), nº....., Bairro ....., em ..... -...., CEP .....-....., inscrita no CNPJ sob o n° ....., por seu representante legal no fim assinado, doravante denominada **Nome Fantasia ou Razão Social**.

Por este **ACORDO DE CONFIDENCIALIDADE**, as partes acima nomeadas e qualificadas resolvem firmar o presente, conforme cláusulas e condições as seguir.

CLÁUSULA PRIMEIRA - DO OBJETO
O presente **ACORDO DE CONFIDENCIALIDADE E SIGILO**, define os direitos, obrigações e responsabilidades das Partes em relação à **Segurança da Informação**, **à confidencialidade e aos ativos** envolvidos e necessários referente a uma possível parceria comercial entre as Partes.

CLÁUSULA SEGUNDA - DAS DEFINIÇÕES
Ativo - Qualquer coisa que tenha valor para as Partes, englobando:

- Os ativos de informação, tais como, mas não se limitando a, base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
- Os ativos de software, tais como, mas não se limitando a, aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- Os ativos físicos, tais como, mas não se limitando a, equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
- Os serviços, tais como, mas não se limitando a, serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;
- As pessoas e suas qualificações, habilidades e experiências;
- Os intangíveis, tais como, mas não se limitando a, reputação e a imagem da Parte.

Confidencialidade - Garantia de que a **informação** é acessível somente a Pessoas Autorizadas.

Informação - Significa toda e qualquer informação de natureza, mas não se limitando a, comercial, técnica, financeira, jurídica, operacional ou mercadológica sobre, mas sem se limitar a, análises, amostras, componentes, contratos, cópias, croquis, dados, definições, desenhos, diagramas, documentos, equipamentos, especificações, estatísticas, estudos, experiências, resultados de testes e pesquisas, conhecimento adquirido ou novo conhecimento, a partir de informações confidenciais reveladas, tendências, fluxogramas, fórmulas, fotografias, ideias, instalações, invenções, mapas, métodos e metodologias, modelos, pareceres, pesquisas, planos ou intenções de negócios, plantas ou gráficos,

práticas, preços, custos e outras informações comerciais, processos, produtos atuais e futuros, programas de computador, projetos, testes ou textos, repassada na forma escrita, oral, armazenada em qualquer mídia tangível ou intangível.

Informações Confidenciais ou Sigilosas - São aquelas informações que a Parte Divulgadora deseja proteger contra o uso ilimitado, comunicação e ou divulgação indiscriminada ou competição e que sejam designadas como tal, especialmente para fins de execução de projetos da **BANRISUL CARTÕES**.

INFORMAÇÃO PÚBLICA - Trata-se da informação identificada pela Parte Divulgadora com a expressão "**INFORMAÇÃO PÚBLICA**" ou que:

- Seja do conhecimento da Parte Receptora à época em que lhe for comunicada, desde que possa ser comprovado tal conhecimento prévio;
- Antes de ser revelada, tenha se tornado do conhecimento do público através de fatos outros que não atos ilícitos praticados por uma das Partes ou por seus representantes ou empregados;
- Tenha sido recebida legitimamente de terceiro sem restrição à revelação e sem violação à obrigação de sigilo direta ou indiretamente para com a Parte que as houver revelado;
- Tenha tido a divulgação autorizada por escrito pela Parte Divulgadora;
- Tenha sido desenvolvida de forma independente por empregados ou por empresas do mesmo grupo da Parte Receptora, sem utilização direta ou indireta de **Informações Confidenciais**, desde que passível de comprovação;

Toda e qualquer informação que não se enquadre nas hipóteses previstas acima deverá ser considerada **Confidencial** e mantida sob sigilo pela Parte Receptora até que venha a ser autorizado, expressamente pela Parte Divulgadora, a tratá-la diferentemente.

Parte - Expressão utilizada para referir genericamente os signatários deste **ACORDO DE CONFIDENCIALIDADE E SIGILO**.

Parte Receptora - É a Parte que recebe as **Informações Confidenciais**.

Parte Divulgadora - É a Parte que divulga as **Informações Confidenciais**.

Pessoa Autorizada - Agentes, representantes, especialistas, prestadores de serviços, internos ou externos, ou empregados dos signatários deste **ACORDO DE CONFIDENCIALIDADE E SIGILO** e aqueles autorizados formalmente a transmitir ou receber informações.

Sigilo - Condição nas quais dados sensíveis são mantidos em sigilo e divulgado apenas para as Pessoas Autorizadas.

Sigilo Bancário – Tratamento da informação em conformidade com a **Lei Complementar 105**, de 10 de janeiro de 2001.

CLÁUSULA TERCEIRA

Todas as informações relacionadas ao objeto deste **ACORDO,** conforme referido na **cláusula primeira**, que forem transmitidas pela **Parte Divulgadora** à **Parte Receptora** ou que vierem a ser descobertas no decorrer do presente projeto (novo conhecimento), devem ser consideradas e protegidas pela **Parte Receptora** como **confidenciais**, exceto se antes da divulgação for esclarecido expressamente que não são confidenciais.

CLÁUSULA QUARTA
As informações da Parte Divulgadora devem ser tratadas como confidenciais e serem protegidas pela Parte Receptora por período indeterminado, até ordem em contrário.

CLÁUSULA QUINTA - DAS AUTORIZAÇÕES PARA ACESSO ÀS INFORMAÇÕES CONFIDENCIAIS
Para alcançar a condição de Pessoa Autorizada, os agentes, representantes, especialistas, prestadores de serviços, internos ou externos, empregados das Partes, envolvidos, direta ou indiretamente, com a execução do projeto referido na **cláusula primeira**, deverão ser devidamente instruídos sobre a proteção e manutenção da Confidencialidade e Sigilo das Informações Confidenciais, bem como a legislação pertinente ao sigilo bancário, devendo ainda ter conhecimento do teor deste **ACORDO DE CONFIDENCIALIDADE E SIGILO**.

Parágrafo Primeiro: Concomitantemente, as Partes tomarão todas as providências para minimizar o risco de revelação de **Informações Confidenciais**, assegurando-se de que somente Pessoas Autorizadas tenham acesso a tais informações, na estrita medida do necessário.

Parágrafo Segundo: Em qualquer caso, as Partes serão responsáveis por toda infração ao presente **ACORDO DE CONFIDENCIALIDADE E SIGILO** que venha a ser cometida por qualquer Pessoa sob sua responsabilidade (Autorizada ou não) e tomará todas as providências, inclusive judiciais, necessárias para impedi-los de revelar ou utilizar, de forma proibida ou não autorizada, as **Informações Confidenciais**.

Parágrafo Terceiro: Cada Parte fará a gestão das inclusões e exclusões de seus prepostos na condição de **Pessoa Autorizada**, devendo comunicar imediatamente à outra Parte as mudanças ocorridas.

CLÁUSULA SEXTA - DO USO
As **INFORMAÇÕES CONFIDENCIAIS** reveladas ou que vierem a ser conhecidas serão utilizadas exclusivamente, para os fins de execução do projeto referido na **cláusula primeira**. Em hipótese alguma, poderão ser utilizadas para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para uso de terceiros, salvo acordo entre as partes, expresso e por escrito, em contrário.

A Parte Receptora concorda que:

a) Quaisquer informações confidenciais divulgadas de acordo com este instrumento devem ser usadas pela Parte Receptora tão somente com o propósito para o qual foram divulgadas;
b) Quaisquer informações confidenciais divulgadas de acordo com este instrumento permanecem em qualquer instância de propriedade da Parte Divulgadora;
Exceto nos casos de Informações Públicas e determinação judicial, a Parte Receptora não poderá usar, distribuir, divulgar ou disseminar informações confidenciais a quem quer que seja, salvo a seus empregados, incluindo os de sua controladora, subsidiárias controladas ou afiliadas, que necessitem ter conhecimento de tais informações ao alcance do propósito para o qual foram divulgadas.

CLÁUSULA SÉTIMA - DA NÃO DIVULGAÇÃO

As Informações Confidenciais deverão obrigatoriamente ser protegidas pela Parte Receptora por todos os meios possíveis, devendo a elas serem atribuídas no mínimo o mesmo grau de zelo das Informações Confidenciais próprias, sendo dever da Parte Receptora dar conhecimento das obrigações aqui assumidas a todos os seus empregados, colaboradores e demais pessoas que a elas tenham acesso, evidenciando que a divulgação das Informações Confidenciais, sem autorização expressa da Parte Divulgadora, é motivo suficiente para sujeição às penalidades legais e contratuais.

Parágrafo Primeiro : Todos os empregados da (razão social ou nome fantasia da empresa) que participarem do projeto e tiverem acesso às informações confidenciais deverão assinar o **TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO** contido no Anexo I deste instrumento.

Parágrafo Segundo: Sempre que solicitado, a (razão social ou nome fantasia da empresa) deverá disponibilizar à **BANRISUL CARTÕES o TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO**, devidamente assinado, conforme previsto no parágrafo anterior.

CLÁUSULA OITAVA - DA GUARDA DE INFORMAÇÕES CONFIDENCIAIS
A Parte Receptora deverá manter procedimentos administrativos adequados à preservação de extravio ou perda de quaisquer Informações Confidenciais, principalmente os que impeçam a divulgação ou a utilização por seus agentes, funcionários, consultores e representantes, ou ainda, por terceiros não envolvidos com a execução do projeto referido na **cláusula primeira**.

CLÁUSULA NONA - DAS CÓPIAS
As Partes comprometem-se a não efetuar nenhuma gravação ou cópia das Informações Confidenciais recebidas.

CLÁUSULA DÉCIMA - DA PROPRIEDADE
O presente **ACORDO DE CONFIDENCIALIDADE E SIGILO** não implica a concessão, pela Parte Divulgadora à Parte Receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

Parágrafo Primeiro: Todas as anotações, compilações e resultados dos trabalhos desenvolvidos no decorrer do presente projeto (novo conhecimento), serão também consideradas **Informações Confidenciais**, e serão havidos como de propriedade da Parte Divulgadora, não cabendo à outra Parte nenhum direito, salvo acordo entre as mesmas, expresso e por escrito, em contrário.

CLÁUSULA DÉCIMA PRIMEIRA - DA VIOLAÇÃO
As Partes informarão a outra Parte imediatamente sobre qualquer revelação não autorizada, esbulho ou mau uso, por qualquer pessoa, de qualquer **INFORMAÇÃO CONFIDENCIAL**, assim que tomarem conhecimento, devendo ser adotadas todas as providências necessárias para evitar qualquer violação futura de **Informações Confidenciais**, não se afastando a possibilidade de serem aplicadas as penalidades aqui previstas a Parte que tenha dado causa.

CLÁUSULA DÉCIMA SEGUNDA - DO RETORNO DE INFORMAÇÕES CONFIDENCIAIS

A pedido da Parte Divulgadora, a Parte Receptora deverá restituir imediatamente o documento (ou outro suporte) que contiver Informações Confidenciais.
A Parte Receptora deverá restituir espontaneamente a Parte Divulgadora as Informações Confidenciais que deixarem de ser necessárias, não guardando para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.

Quando solicitado, a Parte Receptora deverá prontamente emitir uma declaração assinada por seu representante legal, confirmando que toda **INFORMAÇÃO CONFIDENCIAL** foi restituída ou inteiramente destruída, comprometendo-se de que não foram retidas quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de ser considerada falta gravíssima, conforme previsto no presente **ACORDO** e ainda podendo ser a (razão social ou nome fantasia da empresa) responsabilizada por perdas e danos que porventura vierem a existir.

CLÁUSULA DÉCIMA TERCEIRA - DAS PENALIDADES
O descumprimento de qualquer cláusula do presente **ACORDO DE CONFIDENCIALIDADE E SIGILO** será considerado falta gravíssima e sujeitará a Parte que o descumpriu ao pagamento ou recomposição de todas as perdas, danos e lucros cessantes sofridos pela outra Parte, inclusive as de ordem moral, concorrencial, bem como as de responsabilidade civil e criminal respectivas, que serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA DÉCIMA QUARTA - DO PRAZO DE VIGÊNCIA
O presente **ACORDO DE CONFIDENCIALIDADE E SIGILO** terá a vigência da duração do projeto referido na **cláusula primeira**. Não obstante o termo final de validade deste instrumento, todas as obrigações aqui previstas, relacionadas às Informações já divulgadas, continuarão a ser observadas, notadamente a preservação da confidencialidade por período indeterminado.

CLÁUSULA DÉCIMA QUINTA - DA PUBLICIDADE
Todas as declarações, anúncios públicos e/ou divulgações relativas ao projeto referido na **cláusula primeira** e a este **ACORDO DE CONFIDENCIALIDADE E SIGILO** deverão ser previamente comunicados e coordenados por ambas as Partes, dependendo do prévio e mútuo consentimento das mesmas.

CLÁUSULA DÉCIMA SEXTA - REVELAÇÃO POR ORDEM JUDICIAL
Caso uma das Partes seja obrigada a revelar qualquer **INFORMAÇÃO CONFIDENCIAL** em virtude de ordem judicial, a mesma avisará a outra Parte imediatamente, para que a esta seja dada a oportunidade de opor-se à revelação. Caso a oposição da Parte não seja bem sucedida, a Parte oposta somente poderá fazer a revelação na extensão exigida pela ordem judicial em questão e deverá exercer todos os esforços razoáveis para obter garantias confiáveis de que tais Informações Confidenciais tenham tratamento sigiloso.

CLÁUSULA DÉCIMA SÉTIMA – DISPOSIÇÕES GERAIS
Parágrafo Primeiro: Falhas ou atrasos de qualquer uma das Partes no exercício de qualquer direito, poder ou privilégio não devem ser considerados como desistência, novação ou modificação dos direitos previstos neste **ACORDO DE CONFIDENCIALIDADE E SIGILO**.

Parágrafo Segundo: Fica entendido que este **ACORDO DE CONFIDENCIALIDADE E SIGILO** não pretende e não vai obrigar as Partes a celebrar outros acordos ou contratos, ou

ainda a realizar qualquer negócio, ficando, certo e ajustado que as Partes não têm exclusividade no recebimento das informações confidenciais a serem divulgadas.

Parágrafo Terceiro: Inobstante do ora ajustado a **BANRISUL CARTÕES** poderá estabelecer, a qualquer momento e a seu critério, parcerias com outras empresas - públicas ou privadas - para execução de projeto similar ao presente.

Parágrafo Quarto: Nada que esteja contido neste **ACORDO DE CONFIDENCIALIDADE E SIGILO** deve ser tomado como garantia ou conferência de direitos de licença de uso das informações confidenciais divulgadas à parte Receptora.

Parágrafo Quinto: Qualquer aditamento a este **ACORDO DE CONFIDENCIALIDADE E SIGILO** deve ser por escrito e assinado por seus representantes legais.

CLÁUSULA DÉCIMA OITAVA - DO FORO
Este **ACORDO DE CONFIDENCIALIDADE E SIGILO** é extensivo aos sucessores das Partes, subsidiárias, controladas e afiliadas, e celebrado segundo as leis brasileiras, fincando eleito o Foro da Comarca de Porto Alegre, Estado do Rio Grande do Sul, como competente para dirimir quaisquer dúvidas oriundas do presente instrumento.

E, por estarem assim justas e de acordo, as Partes firmam o presente Instrumento em 2 (duas) vias de idêntico teor e forma, perante as testemunhas abaixo identificadas e assinadas, para que surta efeitos jurídicos.

Porto Alegre, xx de xxxxxx de 2019.

_____
Banrisul Cartões S.A.

_____
Empresa
(COLOCAR O NOME DA EMPRESA E CARIMBAR COM O NOME DO REPRESENTANTE LEGAL)

Testemunhas:

_____
Nome:
RG:
CPF:

_____
Nome:
RG:
CPF:

ANEXO AO ACORDO DE CONFIDENCIALIDADE E SIGILO

TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO

Eu, «Nome», «Estado_Civil», «Profissão», <<filiação>>, portador(a) da Cédula de Identidade nº «CI», CPF/MF nº «CPF», domiciliado(a) na «Endereço», usuário do endereço eletrônico <<e-mail>>, na condição empregado da(s) empresa <<empresa>>, ..., inscrita no CNPJ/MF sob nº, com endereço na Rua....., em (cidade)/UF..... assino o presente Termo de Sigilo em relação às informações confidenciais, conteúdos e materiais, do projeto <<...>> obrigando-me a guardar sigilo, não revelando o seu conteúdo a quaisquer pessoas que não os representantes legais da referida empresa.

Todas as informações a mim disponibilizadas na realização do referido projeto são para fins relacionados única e exclusivamente às minhas atividades profissionais, sendo expressamente proibido o uso dessas informações para outros fins.

Estou ciente que descumprindo os compromissos por mim assumidos neste Termo de Sigilo, estarei sujeito às penalidades aplicáveis, como medidas administrativas e/ou disciplinares internas, e/ou, ainda, ações penais, cíveis e/ou trabalhista previstas em lei.

«Local», «Dia» de «Mês» de «Ano».

_____

«Nome», «Matrícula».