

# **Relatório de Controle de Conformidade e Eficiência Operacional dos processos e produtos da Braspag**

**(Serviços de Pagamentos, Processos de segurança, Continuidade de Negócio e  
Gerenciamento de Risco)**

**PARA USO DA**

**ORACLE®**

**2020**

## **Programa de Compliance Segurança e Continuidade do Negócio**

A Braspag mantém avaliações anuais dos seus processos de negócios, da segurança física e lógica dos seus ambientes e dos controles internos, de modo que estejam aderentes com as melhores práticas e requerimentos do setor em que opera.

### **A) PCI DSS**

O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) foi desenvolvido para incentivar e aprimorar a segurança dos dados do titular do cartão e promover ampla adoção das medidas de segurança dos dados do portador do cartão globalmente. O PCI DSS aplica-se para todas as entidades envolvidas no processo de pagamento com cartão, inclusive comerciantes, processadores, adquirentes, emissores e prestadores de serviço.

Os 12 requisitos do PCI DSS basicamente são aplicados em todas as empresas que armazenam, processam ou transmitem dados do titular do cartão e/ou dados de autenticação do portador considerados confidenciais.

A Braspag, por sua vez, está aderente com os 12 requisitos do PCI DSS na sua última versão (3.2.1), onde estes requisitos são verificados periodicamente e validados a cada ano como um fornecedor de serviço de **Nível 1**. Esta validação é realizada por um Assessor Qualificado de Segurança (QSA) devidamente homologado pelo PCI Council.

Abaixo são listados os 12 requisitos:

#### **Construir e manter a segurança de rede e sistemas**

1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão;
2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança;

#### **Proteger os dados do titular do cartão**

3. Proteger os dados armazenados do titular do cartão;
4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas;

#### **Manter um programa de gerenciamento de vulnerabilidades**

5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus;
6. Desenvolver e manter sistemas e aplicativos seguros;

#### **Implementar medidas rigorosas de controle de acesso**

7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio;
8. Identificar e autenticar o acesso aos componentes do sistema;
9. Restringir o acesso físico aos dados do titular do cartão;

#### **Monitorar e testar as redes regularmente**

10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão;
11. Testar regularmente os sistemas e processos de segurança;

#### **Manter uma política de segurança de informações**

12. Manter uma política que aborde a segurança da informação para todas as equipes.

Para mais informações sobre a conformidade da Braspag com esses padrões consulte o Anexo A (Atestado de Conformidade – AoC PCI DSS).

Sobre o PCI-DSS visite: <https://www.pcisecuritystandards.org>.

## **B) CONTINUIDADE DE NEGÓCIOS (ISO 22301)**

Por ser uma empresa líder no seu setor de atuação e com uma rede global que conecta diversas instituições financeiras, comerciantes, parceiros e clientes, a BRASPAG entende a necessidade de estabelecer sistemas com alto índices de disponibilidade. A resiliência dos processos de negócio é uma preocupação contínua da alta gestão, onde as fases de planejamento, treinamento e descoberta de formas eficientes de trabalho são analisadas periodicamente para melhorar como operacionalizamos o nosso negócio.

O Sistema de Continuidade de Negócio (SGCN) da Braspag também está aderente às melhores práticas do setor de tecnologia e desta forma nos posiciona na vanguarda do que fazemos. O SGCN apoia o compromisso da Braspag em fornecer produtos e serviços com a confiabilidade que nossos clientes esperam.

#### **Governança**

O SGCN é mantido em um ciclo anual, por uma equipe experiente, com a missão de garantir a continuidade da operação ("business as usual") em situações adversas.

Pessoas e recursos são alocados com base nos pilares abaixo:

- **Diretrizes corporativas**  
Estrutura estratégica baseada em políticas, papéis e responsabilidades para assegurar a resiliência esperada;
- **Gerenciamento de Crises**  
O processo de gerenciamento de crise é baseado na resposta de emergência e no gerenciamento de incidentes que ameaçam a vida, reputação da marca, clientes,

produtos e serviços da Braspag. Este pilar garante um processo coordenado para comandar uma resposta eficaz a qualquer incidente, inclusive com o gerenciamento da recuperação da força de trabalho e comunicação em momentos adversos.

- **Gerenciamento de Continuidade de Negócio**

Este pilar possui esforços alocados na continuidade e recuperação dos processos do negócio. São identificados processos críticos do negócio e estabelecidas as opções de recuperação. É garantida a viabilidade dos planos através dos processos documentados, treinamentos e exercícios de continuidade.

- **Planos de desastre**

Os planos de desastre são esforços concentrados na recuperação de sistemas e serviços da Braspag. Este pilar avalia toda criticidade e recuperação dos produtos e garante que os planos necessários estejam em vigor e disponíveis para atingir um alto padrão de operação e disponibilidade.

O SGCN segue a estratégia estabelecida de avaliação, planejamento, exercício e treinamento definido na política corporativa da Braspag. Todo programa é baseado nas orientações regulatórias e padrões da indústria, incluindo:

- Organização Internacional de Normalização ISO 22301 - Gerenciamento de Continuidade de Negócios;
- Disaster Recovery Institute International (DRII).

As atividades de desempenho do SGCN, incluindo o processo de gerenciamento de risco, são analisadas e aprovadas pela alta direção em apoio à estratégia do programa.

A garantia independente do Programa é assegurada por auditores internos, externos e consultores através de uma programação regular de avaliação e melhoria.

Para mais informações sobre a conformidade da Braspag, consulte o Anexo B (Certificado de Conformidade ISO 22301).

## **ANEXO A**



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

June 2018

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

#### Part 1. Service Provider and Qualified Security Assessor Information

##### Part 1a. Service Provider Organization Information

Company Name:	Braspag Tecnologia em Pagamento Ltda		DBA (doing business as):	Braspag		
Contact Name:	Atila Duarte		Title:	Compliance Manager		
Telephone:	+55 21 990321225		E-mail:	aduarte@braspag.com.br		
Business Address:	Marechal Câmara Avenue, 160 9° floor		City:	Rio de Janeiro		
State/Province:	Rio de Janeiro	Country:	Brazil		Zip:	06455-030
URL:	http://www.braspag.com.br					

##### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Foregenix Ltd				
Lead QSA Contact Name:	Leonardo Lima Ferla	Title:	QSA		
Telephone:	+44 845 309 6232	E-mail:	lferla@foregenix.com		
Business Address:	1st Floor 8-9 High Street	City:	Marlborough		
State/Province:	Wiltshire	Country:	United Kingdom	Zip:	SN8 1AA
URL:	http://www.foregenix.com				

DS  
AND:

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) assessed: Authorisation (Pagador), Fraud Prevention (Antifraude), Meu CheckOut | Cartao Protegido, Backup

Type of service(s) assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

#### Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☐ POS / card present
- ☒ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):  
Fraud Prevention

☐ Account Management

☐ Fraud and Chargeback

☒ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

DS  
AND:



**Part 2a. Scope Verification** *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) not assessed: Not Applicable

Type of service(s) not assessed:

**Hosting Provider:**

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

**Managed Services (specify):**

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

**Payment Processing:**

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

Not Applicable

DS  
AND:

## Part 2b. Description of Payment Card Business

DS  
AND:

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Braspag Tecnologia em Pagamento Ltda (Braspag) is a level 1 service provider, located in the city of Rio de Janeiro (Brazil), operating as a payment gateway for e-commerce transactions.

Braspag is responsible for processing card-not-present transactions (internet orders) and forwarding them to acquirers (Cielo, GetNet and Rede). Also, Braspag is capable to provide settlement, fraud prevention and merchant services through a web portal to their clients.

### Authorisation processing transactions

Also known as Pagador, Cartao Protegido and Meu CheckOut

As part of authorization processing transactions, Braspag receives over the internet (by a secure connection with HTTPS with TLS 1.2 encrypted with AES-256) CHD (Name, PAN and Expiry) and SAD (CVV2, CVC2 and CID) by an in-scope system (Pagador). The received requests are forwarded to acquirers using a secure private connection (X.25 or MPLS) or by an acquirer's web service (out-of-scope) by HTTPS (TLS v1.2 or higher encrypted by AES-256).

For this process, Braspag stores truncated PAN (first 6 and last 4 digits visible only), PAN (encrypted with RSA-2048), Name and Expiry in a database server. For all encrypted PAN stored, Braspag generates and stores (in an in-scope database) a token (pseudo-random 128-bits GUID not derived from PAN). This token is shared with Braspag's clients (merchants) and may be used for recurring transactions that do not require Card Security Code (per agreement with Braspag's client and acquirer).

### Fraud Prevention process

As part of fraud prevention, Braspag receives over the internet (by a secure connection with HTTPS with TLS 1.2 encrypted with AES-256) CHD (Name, PAN and Expiry) and SAD (CVV2, CVC2 and CID) by an in-scope system (Pagador). Pagador forwards (over the internet, using HTTPS, to an out-of-scope web service managed by the fraud prevention service provider) CHD (Name, PAN and Expiry) to a service provider (ACI or CyberSource) responsible for analyzing sent information and returning a risk score.

	<p>For this purpose, Braspag stores in an in-scope database server Name, PAN and Expiry, where PAN is encrypted with RSA-2048.</p> <p><b>Backup process</b></p> <p>Backup process is performed daily and stores CHD (Name, PAN and Expiry) in an Azure Storage (Blob) (PAN is encrypted with RSA-2048).</p>
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	<p>Not Applicable.</p> <p>Besides the services described above and covered by this assessment, Braspag has no other service that they can impact the security of the cardholder data.</p>

### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Data Center	6	<p>Campinas, SP, Brazil (2)</p> <p>Dallas and San Antonio, Texas, US (2)</p> <p>Rio de Janeiro, RJ, Brazil (1)</p> <p>Sao Paulo, SP, Brazil (1)</p>
Office	1	<p>Rio de Janeiro, RJ, Brazil (1)</p>

### Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
SiTef	6.2.8.1	Software Express	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	28/10/2019

### Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- Connections into and out of the cardholder data environment (CDE).

The scope of the assessment was the Braspag's scope, which is comprised of six (6) in-scope data centers (AMT, Mandic and Microsoft Azure (4)), where the following in-scope technologies are placed.

- Application servers

- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

- Asymmetric encryption keys (RSA)
- Backup solution
- Database servers
- EFT application
- Endpoint protection solution
- File Integrity Monitoring (FIM)
- Hash algorithms (SHA, NTLM)
- Intrusion Prevent System (IPS)
- IaaS technologies provided by MS Azure
- LDAP servers
- Linux Operating Systems
- MS Windows Operating Systems
- PaaS technologies provided by MS Azure
- Physical OTP (One Time Password)
- Private links (X.25 and MPLS)
- Stateful firewalls
- Switch Layer 2
- Symmetric encryption (AES and Blowfish)
- Syslog solution
- TLS connections
- Unified Threat Management (UTM)
- Virtualization solution
- Vulnerability scanner solution
- Web application servers
- Web application vulnerability scanning

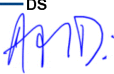
In addition, the following connections in and out are present in the CDE:

- Private connections with acquirers (X.25 and MPLS)

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

☒ Yes ☐ No


  
DS

## Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

☐ Yes ☒ No

### If Yes:

Name of QIR Company:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

☒ Yes ☐ No

### If Yes:

Name of service provider:	Description of services provided:
ACI	Fraud prevention service provider
AMT	Hosting provider
Cyber Source	Fraud prevention service provider
Mandic	Hosting provider
Microsoft Azure	Cloud service provider

*Note: Requirement 12.8 applies to all entities in this list.*

DS  
AND:

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Authorisation (Pagador), Fraud Prevention (Antifraude), Meu CheckOut   Cartao Protegido, Backup		
PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1: No wireless network in-scope 2.6: Braspag is not a shared hosting provider
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1: No disk encryption technology in-scope 3.6: No shared keys process with customers 3.6.2: No shared keys process with customers 3.6.6: No manual clear-text cryptographic keys
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1: No wireless network in-scope
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5: No service provider with access to scope 8.2.2: Just face-to-face password reset process 8.5.1: No remote access to customer premises
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.9: No POS devices in-scope

				<b>9.9.1: No POS devices in-scope</b> <b>9.9.2: No POS devices in-scope</b> <b>9.9.3: No POS devices in-scope</b>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>12.3.9: No service provider with access to scope</b>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>A.1.1: Braspag is not a shared hosting provider</b> <b>A.1.2: Braspag is not a shared hosting provider</b> <b>A.1.3: Braspag is not a shared hosting provider</b> <b>A.1.4: Braspag is not a shared hosting provider</b>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>A.2.1: No POS devices in-scope</b> <b>A.2.2: No SSL or early TLS implementation</b> <b>A.2.3: No SSL or early TLS implementation</b>

DS  
AND:



## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	16 May 2019
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

DS  


## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 16 May 2019.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby Braspag Tecnologia em Pagamento Ltda has demonstrated full compliance with the PCI DSS.</p>				
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby Braspag Tecnologia em Pagamento Ltda has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" data-bbox="397 1075 1432 1209"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met		
Affected Requirement	Details of how legal constraint prevents requirement being met				

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Qualys and Trustwave

**DocuSigned by:**

**Part 3b. Service Provider Attestation**

*Alina Duarte*

17/5/2019 | 12:07 BRT

9C7A5950A7344C4...

Signature of Service Provider Executive Officer ↑

Date: **16 May 2019**

Service Provider Executive Officer Name: Atila Duarte

Title: **Compliance Manager**

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:

*The lead QSA (Leonardo Lima Ferla) assessed this entity against PCI-DSS v3.2.1 and reviewed evidence as part of the validation step and prepared the Report on Compliance. The QSA did not execute any other function.*

*Leonardo Lima Ferla*

Signature of Duly Authorized Officer of QSA Company ↑

Date: **16 May 2019**

Duly Authorized Officer Name: Leonardo Lima Ferla

QSA Company: **Foregenix Ltd**

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

If an ISA(s) If no ISA in the assessment, then simply include Not Applicable here.  
with this assessment, identify the ISA personnel and describe the role performed:

The involved ISA (Gabriel Carvalhal) supported the lead QSA related to PCI-DSS requirement testing procedures, such as system examinations, document reviews and process observation. Also, ISA is the point of contact of all PCI-DSS projects in Braspag.

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



DS  
AMD:

## **ANEXO B**

# Certificate of Registration

## BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2012

This is to certify that:

Braspag Tecnologia e Pagamentos Ltda.  
Av. Marechal Câmara, nº 160 - 9º Andar  
Ed. Le Bourguet  
Rio de Janeiro  
Rio de Janeiro  
20020-080  
Brasil

Holds Certificate Number:

BCMS 632357

and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2012 for the following scope:

**The Business Continuity Management System of payment solutions services supported by the technological infrastructure, including the development, monitoring and information security of Braspag Tecnologia e Pagamentos Ltda., located at Avenida Marechal Câmara, 160 - 9th Floor, Downtown, Rio de Janeiro, RJ, Brazil.**

**O Sistema de Gestão de Continuidade de Negócios dos serviços de soluções de pagamentos suportado pela infraestrutura tecnológica, incluindo desenvolvimento, monitoramento e segurança da informação da Braspag Tecnologia e Pagamentos Ltda, localizada na Avenida Marechal Câmara, 160 - Ed. Le Bourget, 9º Andar, Centro, Rio de Janeiro, RJ, Brasil.**



For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2015-03-29

Latest Revision Date: 2018-03-09

Effective Date: 2018-03-29

Expiry Date: 2021-03-28

Page: 1 of 1



...making excellence a habit.™