O PCI DSS
(Payment Card Industry – Data Security Standard)

O PCI DSS (Payment Card Industry – Data Security Standard) é uma certificação de segurança internacional necessária para todas as empresas que processam, armazenam ou transmitem dados de cartões. Tem como premissa assegurar a proteção de informações confidenciais e garantir a segurança de dados sensíveis em transações financeiras.

A Beeteller possui parceria com a PagSeguro Internet Instituição de Pagamento S.A, inscrita no CNPJ 08.561.701/0001-01, responsável pelo processamento dos pagamentos via cartão de crédito. A PagSeguro possui um mecanismo, utilizado pela Beeteller, que criptografa as informações dos dados do cartão de crédito diretamente no navegador do usuário antes de transmiti-lo pela internet, utilizando uma chave pública, na qual somente o PagSeguro possui acesso à chave privada, sendo este a única parte com possibilidade de decriptar os dados para ser utilizado durante o processamento, armazenamento e transmissão desses mesmos dados.

Dessa forma, a PagSeguro como recebedora dos dados do cartão de crédito possui as certificações PCI DSS, estando em conformidade com o mais alto nível de segurança internacional, conforme certificações abaixo.

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:	PagSeguro Internet Instituição de Pagamento S.A	DBA (doing business as):	PagSeguro/PagBank - Adquirência
Contact Name:	Marcelo Martinez	Title:	Information Security Specialist
Telephone:	+55 (11) 3038-8256	E-mail:	mamartinez@pagbank.com
Business Address:	Av. Brig. Faria Lima, 1384	City:	São Paulo
State/Province:	São Paulo	Country: Brazil	Zip: 01451-001
URL:	https://pagbank.uol.com.br/		

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

Company Name:	Cipher S/A		
Lead QSA Contact Name:	Paulo Rogério de Aguiar Poi	Title:	LATAM, Governance, Risk and Compliance Director
Telephone:	+551140637300 ext.1446	E-mail:	ppoi@cipher.com
Business Address:	Alexandre Dumas, 1658, 02 Floor	City:	São Paulo
State/Province:	São Paulo	Country: Brazil	Zip: 04717-004
URL:	https://www.cipher.com/		

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:	PagSeguro - Acquiring Services

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):

☐ 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.

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:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	PagSeguro is part of the group Universo Online (UOL) offering acquiring services, performing interface amongst merchants, card brands, payment gateways and issuers. The company receives transactions originated from merchants or payment gateways (including its own PagSeguro payment gateway), redirecting them to the payment brands in order to be authorized. PagSeguro then performs the settlement of the transactions, after the conciliation procedures took place.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	As an acquirer, PagSeguro is directly involved at the payment process including POS operation processing. PagSeguro Acquirer is a service provider Level 1 in PCI DSS.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Data Center Glete	1	São Paulo, SP, Brazil
Data Center Tamboré	1	Barueri, SP, Brazil
Safety Room Faria Lima	1	São Paulo, SP, Brazil
Corporate Office, Backoffice and Fraud Prevention Operations	1	São Paulo, SP, Brazil

Part 2d. Payment Applications

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	☒ Yes ☐ No	June 29th,2022
Payware CMS	8.11.49.1.3	Verifone	☒ Yes ☐ No	June 03rd,2022
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	PagSeguro has segragated and dedicated environments for transactions capture and processing for POS transactions.
For example: • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The capturing networks are directly connected to the CDE, where transactions are processed and sent to brands and issuers. No CDE network has direct connection to untrusted networks. Additionally, there are backoffice processes performed on isolated networks, without direct connection to untrusted networks

Does your business use network segmentation to affect the scope of your PCI DSS environment?	☒ Yes ☐ No

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

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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:
IronMountain	Logistics management and secure disposal of backup tapes.
Verifone	Services and Development of Payware System
Tenablei.io	Responsible for vulnerability testing

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

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:	PagSeguro - Acquiring Services

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.2.3 - This requirement are not applicable, as not have any wireless networks connected with their cardholder data environment. 1.4 - This requirement are not applicable, as no mobile devices acessing CDE directly.
Requirement 2:	☐	☒	☐	2.1.1 - This requirement are not applicable, because does not have wireless environment connected to CDE. 2.6 - This requirement are not applicable. The company is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1 - This requirement are not applicable, as no disk encryption are used in environment.
Requirement 4:	☐	☒	☐	4.1.1 - This requirement are not applicable, as not have any wireless networks connected with their cardholder data environment.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6 - This requirement are not applicable, as there hane been no significant changes in your environment in the last year.
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	8.1.5 - This requirement are not applicable, because no vendors IDs to access, support or maintain systems. 8.5.1 - This requirement are not applicable. The company is not a shared hosting provider.
Requirement 9:	☒	☐	☐	
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.2.3 - This requirement are not applicable, as there have been no significant changes in your environment in the last year.
Requirement 12:	☐	☒	☐	12.9 - This requirement are not applicable. The company is not a shared hosting provider.
Appendix A1:	☐	☐	☒	These requirements are not applicable. PagSeguro's hosted shared provider as not in scope for certification.
Appendix A2:	☐	☐	☒	These requirements are not applicable. because PagSeguro does not use early SSL/TLS.

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:	July 03th, 2023	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated July 03th, 2023**.**

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):**

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby PagSeguro - Adquirência has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** 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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Tanable.IO

Part 3b. Service Provider Attestation

DocuSigned by:

Gustavo De Almeida Sartori

C74776FEB6B54DA...

Signature of Service Provider Executive Officer ↑

DocuSigned by:

Sadami Ikegami

7CB342A81921445...

Date: July 03th, 2023

Service Provider Executive Officer Name: Gustavo De Almeida Sartori | Sadami Ikegami

Title: General Security Manager | Chief Risk Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Project Manager and Lead Assessor

Janaina Devus Creazzo

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* July 03th, 2023
Duly Authorized Officer Name: Janaina Devus Creazzo	*QSA Company:* CIPHER S/A

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

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Marcelo Martinez - Information Security Assessor

---

[1] 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.

[2] 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.

[3] 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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	

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:	PagSeguro Internet Instituição de Pagamento S.A		DBA (doing business as):		PagSeguro/PagBank	
Contact Name:	Marcelo Martinez		Title:		Information Security Specialist	
Telephone:	+55 11 3038-8256		E-mail:		mamartinez@pagbank.com	
Business Address:	Av Brig. Faria Lima, 1384		City:		São Paulo	
State/Province:	São Paulo	Country:	Brazil		Zip:	01451-001
URL:	https://www.pagbank.com/					

Part 1b. Qualified Security Assessor Company Information (if applicable)				
Company Name:	CIPHER S/A			
Lead QSA Contact Name:	Paulo Rogério de Aguiar Poi	Title:	GRC LATAM Director	
Telephone:	+551140637300 ext.1446	E-mail:	ppoi@cipher.com	
Business Address:	Alexandre Dumas, 1658, 02 Floor	City:	São Paulo	
State/Province:	São Paulo	Country:	Brazil	Zip: 04717-004
URL:	https://www.cipher.com/			

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:	PagSeguro Gateway

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POS / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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):		

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.

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:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	PagSeguro receives transactions containing the PAN, expiration date, card validation code, PIN, PIN Block and the full track data, however it only stores the truncated version of the PAN, hashed version of the PAN, Expiration Date and Cardholder Name.
	About the PagSeguro (PagBank) product/environment, the first transaction received, when the customer subscribes to a plan, receives the PAN, card Expiration date, and cardholder name, this information is sent to the payment-token-hub application that is used to generate a token with card data (without the CVV), which will be used in recurring charges. The CVV can be requested at the time of signing the plan for validation, not being stored.
	PagSeguro is a Level 1 Service Provider.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	PagSeguro transmits cardholder data and sensitive authentication data through encrypted channels, however they not store cardholder data, once only the truncated and hashed version of the PAN are store.
	It is important to remind that the hashed version of the PAN is generated using a random salt value, which is stored in a segregated environment.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Office Faria Lima	1	São Paulo, SP, Brazil
Data Center Glete	1	São Paulo, SP, Brazil
Data Center Tamboré	1	Barueri, SP, Brazil

Part 2d. Payment Applications

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	☒ Yes ☐ No	June 29th, 2022
Payware CMS	8.11.49.1.3	Verifone	☒ Yes ☐ No	June 03rd, 2022
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	UOL's PagSeguro is a payment platform that performs transactions with card-present for POS terminals and with card-not-present for e-commerce and mobile. The company captures transactions and
For example:	
• *Connections into and out of the cardholder data environment (CDE).*	

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	transmits them to acquirers using certified payment applications. The Product PagBank PagSeguro Subscriptions is a set of APIs with that offers to customers the sheduling engine that allows automatic recurring billing after signing a plan to purchase products or services. PagSeguro receives transactions containing the PAN, expiration date, card validation code, PIN and the full track data, however it only stores the truncated version of the PAN, hashed version of the PAN, Expiration Date and Cardholder Name.
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

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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:
IronMountain	Logistics management and secure disposal of backup tapes.
Teleperformance	Backoffice management and Call Center
Tenablei.io	Responsible for vulnerability testing
AWS	Cloud Service Provider in scope

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

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:	PagSeguro Gateway

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.2.3 - This requirement are not applicable, as not have any wireless networks connected with their cardholder data environment. 1.4 - This requirement are not applicable, as no mobile devices acessing CDE directly.
Requirement 2:	☐	☒	☐	2.1.1 - This requirement are not applicable, because does not have wireless environment connected to CDE. 2.6 - This requirement are not applicable. The company is not a shared hosting provider.
Requirement 3:	☒	☐	☐	
Requirement 4:	☐	☒	☐	4.1.1 - This requirement are not applicable, as not have any wireless networks connected with their cardholder data environment.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6 - This requirement are not applicable, as there hane been no significant changes in your environment in the last year.
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	8.1.5 - This requirement are not applicable, because no vendors IDs to access, support or maintain systems. 8.5.1 - This requirement are not applicable. The company is not a shared hosting provider.
Requirement 9:	☒	☐	☐	
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	12.9 - This requirement are not applicable. The company is not a shared hosting provider.
Appendix A1:	☐	☐	☒	These requirements are not applicable. PagSeguro hosted shared provider as not in scope for certification
Appendix A2:	☐	☐	☒	These requirements are not applicable, because MOIP does not use early TLS/SSL

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:	July 03th, 2023
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes ☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated July 03th, 2023**.**

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby PagSeguro Internet Instituição de Pagamento S.A has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** 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. *If checked, complete the following:* <table><tr><th>Affected Requirement</th><th>Details of how legal constraint prevents requirement being met</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Tenable.IO

Part 3b. Service Provider Attestation

DocuSigned by:

Gustavo De Almeida Sartori
C74776FEB6B54DA...

DocuSigned by:

Sadami Ikegami
7CB342A81921445...

Signature of Service Provider Executive Officer ↑	*Date:* July 03th, 2023
Service Provider Executive Officer Name: Gustavo De Almeida Sartori | Sadami Ikegami	*Title:* General Security Manager | Chief Risk Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Project Manager and Lead Assessor

Janaina Devus Creazzo

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* July 03th, 2023
Duly Authorized Officer Name: Janaina Devus Creazzo	*QSA Company:* CIPHER S/A

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

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Marcelo Martinez - Information Security Assessor

---

[1] 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.

[2] 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.

[3] 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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	