

# Certificado

Norma de controle **ISO/IEC 27001:2013**

Nº de reg. do certific. **01 153 1629772/01**

Organização: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Site: **c/o CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Campo de aplicação: Prestação de serviços de Data Center, Cloud & Security oferecidos na Argentina (Buenos Aires), Brasil (Cotia, Curitiba e Rio de Janeiro), Chile (Santiago de Chile), Colômbia (Cali, Colômbia XV e Suba), Equador (Quito) e Peru (Lima).  
Serviços de Data Center: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service - Domain Management, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Third Party Products, Virtual Hosting Enterprise e Virtual Hosting Standard.  
Serviços Gerenciados de Segurança: Advanced Event Correlation, Antivirus, AV+AS, Consulting Services, External Security Testing, External Vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion Prevention System (IPS), IPS (Equipamento Dedicado), Strong Authentication, Virtual Security Standard, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assessment, Web Applications Security Testing e Webfilter.

Statement of Applicability (SoA) 05/07/2022, version 5.

Através de uma auditoria comprovou-se que as exigências da norma ISO/IEC 27001:2013 foram satisfeitas.

Validade: Este certificado é válido juntamente com o certificado principal 01 153 1629772 de 13.12.2022 a 06.12.2025.

15.12.2022



TÜV Rheinland Cert GmbH  
Am Grauen Stein · 51105 Köln

# Certificado

Norma de controle **ISO/IEC 27017:2015**

Nº de reg. do certific. **TUV.27.31150.3875.17/01**

Organização: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil


Site: **c/o CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Campo de aplicação: Serviço de DEC3, (Dynamic Enterprise Computing v3), prestado nos Data Centers de Argentina (Buenos Aires), Brasil (Cotia e Rio de Janeiro), Chile (Santiago de Chile), Colômbia (Colômbia XV) e Perú (Lima).

Através de uma auditoria comprovou-se que as exigências da norma ISO/IEC 27017:2015 foram satisfeitas.

Validade: Este certificado é válido juntamente com o certificado principal TUV.27.31150.3875.17 de 13.12.2022 a 06.12.2025.

15.12.2022



TÜV Rheinland do Brasil Ltda.  
Av. Francisco Matarazzo,  
1400 - 6º andar - São Paulo  
- SP - 05001-903

# Certificado

Norma de controle **ISO/IEC 27018:2019**

Nº de reg. do certific. **TUV.27.1795387.4102.20/01**

Organização: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Site: **c/o CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Campo de aplicação: Serviço de DEC3, (Dynamic Enterprise Computing v3), prestado nos Data Centers de Argentina (Buenos Aires), Brasil (Cotia e Rio de Janeiro), Chile (Santiago de Chile), Colômbia (Colômbia XV) e Perú (Lima).

Através de uma auditoria comprovou-se que as exigências da norma ISO/IEC 27018:2019 foram satisfeitas.

Validade: Este certificado é válido juntamente com o certificado principal TUV.27.1795387.4102.20 de 13.12.2022 a 06.12.2025.

15.12.2022



TÜV Rheinland do Brasil Ltda.  
Av. Francisco Matarazzo,  
1400 - 6º andar - São Paulo  
- SP - 05001-903

# CERTIFICADO

Sistema de gestão para  
**ISO 14001 : 2015**

O organismo de certificação TÜV NORD CERT GmbH confirma por este meio e em resultado da auditoria, avaliação e decisão de certificação de acordo com a norma ISO/IEC 17021-1:2015, que a organização

**Cirion Technologies do Brasil Ltda.**  
**Avenida Eid Mansur, 666, Térreo - Parque São George**  
**06708-070 - Cotia - SP**  
**Brasil**

**com os locais de acordo com o anexo**

opera um sistema de gestão em conformidade com os requisitos da norma ISO 14001 : 2015 e que durante o período de vigência de 3 anos será monitorizada quanto à conformidade.

Seguinte âmbito

**Prestação de serviços de telecomunicações e tecnologia da informação, nas modalidades de hospedagem, gerenciamento e monitoramento de servidores, dados e aplicativos de terceiros; armazenamento e backup de informações; e segurança lógica de dados, direcionados a clientes dos setores público e privado.**

Número do registro do certificado 44 104 21 310002  
Relatório da auditoria - OS 22338

Válido de 2024-04-07  
Válido até 2027-04-06  
Certificação Inicial 2021



A Entidade de Certificação  
da TÜV NORD CERT GmbH

Barueri, 2024-04-03

# ANEXO

do Certificado N° de registro 44 104 21 310002  
ISO 14001 : 2015

**Cirion Technologies do Brasil Ltda.**  
Avenida Eid Mansur, 666, Térreo  
Parque São George  
06708-070 - Cotia - SP  
Brasil

N° de registro do certificado	Localização	Seguinte âmbito
44 104 21 310002-001	Cirion Technologies do Brasil Ltda. Avenida Eid Mansur, 666, Térreo Parque São George 06708-070 - Cotia - SP - Brasil	Prestação de serviços de telecomunicações e tecnologia da informação, nas modalidades de hospedagem, gerenciamento e monitoramento de servidores, dados e aplicativos de terceiros; armazenamento e backup de informações; e segurança lógica de dados, direcionados a clientes dos setores público e privado.
44 104 21 310002-002	Cirion Technologies do Brasil Ltda. Rua Moises Cardoso de Oliveira, 100 Mirim 11705-045 - Praia Grande - SP - Brasil	Prestação de serviços de telecomunicações e tecnologia da informação, nas modalidades de hospedagem, gerenciamento e monitoramento de servidores, dados e aplicativos de terceiros; armazenamento e backup de informações; e segurança lógica de dados, direcionados a clientes dos setores público e privado.

Final da lista



A Entidade de Certificação  
da TÜV NORD CERT GmbH

Barueri, 2024-04-03

# Certificado

Norma de controle **NBR ISO 9001:2015**

Nº de reg. do certific. TUV.09.31150.0043.15

Empresa: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
CNPJ: 72.843.212/0006-56  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

com as suas sucursais conforme anexo

Campo de aplicação: Instalação e Entrada em Operação dos Serviços de Housing e Colocation prestados no Brasil (Cotia, Curitiba e Rio de Janeiro).

Através de uma auditoria comprovou-se que as exigências da norma NBR ISO 9001:2015 foram satisfeitas.

Data da próxima auditoria: 08.06 (dd.mm).

Validade: Este certificado é válido de 07.12.2023 a 06.12.2026.  
Primeira Certificação em 2015

18.10.2023



TÜV Rheinland do Brasil Ltda.  
Av. Francisco Matarazzo,  
1400 - 6º andar - São Paulo  
- SP - 05001-903

# Annex to certificate

Standard

**ISO/IEC 20000-1:2018**

Certificate Registr. No. **01 103 1829771**

No.	Location	Scope
/01	c/o CENTURYLINK COMUNICAÇÕES DO BRASIL LTDA. AVENIDA EID MANSUR 666 PARQUE SÃO GEORGE COTIA - SP 06708-070 Brazil	Data Center services: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service – Domain Management, Dynamic Enterprise Computing, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Virtual Hosting Enterprise y Virtual Hosting Standard.Managed Security Services: Antivirus, AV+AS, Event Correlation, External Security Testing, External vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion Prevention System (IPS), IPS (Dedicated Equipment), Strong Authentication, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assesment, Web Applications Security Testing, Webfilter.
/02	c/o CENTURYLINK COMUNICAÇÕES DO BRASIL LTDA. AVENIDA PEDRO II 329 SÃO CRISTOVÃO RIO DE JANEIRO - RJ 20941-070 Brazil	Data Center services: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service – Domain Management, Dynamic Enterprise Computing, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services

Page 1 of 3

# Annex to certificate

Standard

**ISO/IEC 20000-1:2018**

Certificate Registr. No. **01 103 1829771**

/03

c/o CENTURYLINK  
COMUNICAÇÕES DO BRASIL  
LTDA.  
RUA DO SEMEADOR 350  
CIDADE INDUSTRIAL  
CURITIBA - PR  
81270-050  
Brazil

Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Virtual Hosting Enterprise y Virtual Hosting Standard.Managed Security Services: Antivirus, AV+AS, Event Correlation, External Security Testing, External vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion Prevention System (IPS), IPS (Dedicated Equipment), Strong Authentication, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assesment, Web Applications Security Testing, Webfilter.

Data Center services: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service – Domain Management, Dynamic Enterprise Computing, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Virtual Hosting Enterprise y Virtual Hosting Standard.Managed Security Services: Antivirus, AV+AS, Event Correlation, External Security Testing, External vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion

Page 2 of 3

# Annex to certificate

Standard **ISO/IEC 20000-1:2018**

Certificate Registr. No. **01 103 1829771**

Prevention System (IPS), IPS (Dedicated Equipment), Strong Authentication, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assessment, Web Applications Security Testing, Webfilter.

2021-09-13



TÜV Rheinland Cert GmbH  
Am Grauen Stein · 51105 Köln

Page 3 of 3



CERTIFICAÇÃO DE CONFORMIDADE

# Cirion – SAOI – São Paulo – Brasil

Atendeu completamente aos requisitos exigidos pelo  
Payment Card Industry Data Security Standard (PCI-DSS).

Categoria: Payment Card Processor

05/04/2024

EMIÇÃO DE CERTIFICADO

Junho /2016

CERTIFICADO DE PCI-DSS DESDE

05/04/2025

VALIDADE DO CERTIFICADO

4.0

VERSÃO

# Certificado

Norma de controle **ISO 22301:2019**

Nº de reg. do certific. **01 195 2129794/01**

Organização: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Site: c/o **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Campo de aplicação: Business Continuity Management System (BCMS) that offers support to the Data Center, Cloud & Security services provided at the SAO1 Data Center in São Paulo, Brazil.  
Data Center Services: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service - Domain Management, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Third Party Products, Virtual Hosting Enterprise and Virtual Hosting Standard.  
Managed Security Services: Advanced Event Correlation, Antivirus, AV+AS, Consulting Services, External Security Testing, External Vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion Prevention System (IPS), IPS (Specific Purpose Equipment), Strong Authentication, Virtual Security Standard, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assessment, Web Applications Security Testing and Webfilter.

Através de uma auditoria comprovou-se que as exigências da norma ISO 22301:2019 foram satisfeitas.  
Validade: Este certificado é válido juntamente com o certificado principal 01 195 2129794 de 19.10.2023 a 13.09.2024.

24.10.2023



TÜV Rheinland Cert GmbH  
Am Grauen Stein · 51105 Köln

# Certificado

Norma de controle **ISO/IEC 27701:2019**

Nº de reg. do certific. **74 251 0110/01**

Site: **CIRION TECHNOLOGIES DO BRASIL LTDA**  
AVENIDA EID MANSUR 666  
PARQUE SÃO GEORGE  
COTIA - SP  
06708-070  
Brasil

Campo de aplicação: Prestação de serviços de Data Center, Cloud & Security oferecidos no Data Center SAO1 em São Paulo, Brasil, como processador de DP e em processos de suporte como controlador de DP.  
Serviços de Data Center: Backup, Colocation, Consulting Services, Database Management, DEC 3 (Dynamic Enterprise Computing v3), DNS Service - Domain Management, Hosting, Housing, Load Balancing Enterprise, Load Balancing Standard, Management, Microsoft Active Directory Management, Microsoft Exchange Management, Microsoft Terminal Services Management, Office Space, On Site Assistance, On Site Operations, Operating System Management, Other Application Management, SAP Basis Management, SAP Other, SAP Portal Management, Storage, Third Party Products, Virtual Hosting Enterprise e Virtual Hosting Standard.  
Serviços Gerenciados de Segurança: Advanced Event Correlation, Antivirus, AV+AS, Consulting Services, External Security Testing, External Vulnerability Assessment, Firewall & UTM, Internal Security Testing, Internal Vulnerability Assessment, Intrusion Prevention System (IPS), IPS (Equipamento Dedicado), Strong Authentication, Virtual Security Standard, VPN IPSEC Client-to-Site, VPN IPSEC Site-to-Site, VPN SSL, Web Application Vulnerability Assessment, Web Applications Security Testing e Webfilter.

Declaração de Aplicabilidade de 01/08/2023, versão 50.

Através de uma auditoria comprovou-se que as exigências da norma ISO/IEC 27701:2019 foram satisfeitas.

Validade: Este certificado é válido juntamente com o certificado principal 74 251 0110 de 10.10.2023 a 30.10.2025.

24.10.2023

TÜV Rheinland of North America, Inc.  
295 Foster Street, Suite 100,  
Littleton, MA 01460



19 January 2024

Rodrigo de Oliveira  
Director Sales Engineering  
Cirion Technologies do Brasil LTDA  
Alameda Vicente Pinzon, 51 – 4º andar  
São Paulo, SP 04547-130  
Brazil

Re: Tier III Certification of Design Documents for the Cirion Technologies do Brasil LTDA – Cotia DC-6 to DC-13 and TH03A in Cotia, Brazil

Dear Rodrigo de Oliveira,

Uptime Institute Professional Services is pleased to announce the Tier Certification of Design Documents for the mutually dependent data centers of Cirion Technologies do Brasil LTDA – Cotia DC-6 to DC-13 and TH03A as fulfilling Tier III Concurrently Maintainable criteria. This Certification is based upon the design documentation submitted between 10 August and 15 December 2023.

This Certification is the combination of the mutually dependent data centers of the CenturyLink Comunicações do Brasil Ltda – São Paulo Datacenters DC-6, DC-7, DC-8, DC-9, DC-10, DC-11, and DC-12 and the Cirion Technologies Do Brasil LTDA – Cotia DC-13 and TH03A, and supersedes the Tier III Certification of Design Documents for CenturyLink Comunicações do Brasil Ltda – São Paulo Datacenters DC-6, DC-7, DC-8, DC-9, DC-10, DC-11, and DC-12 with 30 August 2023 expiry.

This Certification recognizes the Cirion Technologies do Brasil LTDA – Cotia DC-6 to DC-13 and TH03A design as supporting any planned work on the site infrastructure without disrupting operations, as limited by the stated IT capacity of 2,715 kilowatts (kW). This includes 245 kW of alternating current (AC) load in DC-6; 96 kW of AC load in DC-7; 96 kW of AC load in the DC-8; 209 kW of AC load in DC-9; 143 kW of AC load in DC-10; 256 kW of AC load in DC-11; 270 kW of AC load in DC-12; 1,200 kW of AC load in DATA HALL 13; and 200 kW of direct current (DC) load in TELEHOUSE.

Tier III Concurrently Maintainable criteria are founded on the capability to complete planned facility maintenance or modifications on a scheduled basis; equipment failures or distribution path faults may lead to unplanned outages. Certain operator errors, such as procedural errors during reconfiguration of the redundant computer room or site infrastructure equipment, may also impact the critical load.

This Tier Certification is based on the 100% design documents as submitted for review and makes no assurances as to the constructed environment. This Tier Certification is valid until the design is modified, including any changes to the capacity components or distribution paths depicted in the design identified above and submitted for review. This Certification is subject to the limitations set forth in Schedule I, attached hereto and incorporated herein.

The Tier III Certification of Design Documents award is valid until 19 January 2026 subject to the limitations and extension request process set forth in the attached Schedule I.

Congratulations on this achievement.

Sincerely,

A handwritten signature in black ink, appearing to read "Christopher Brown".

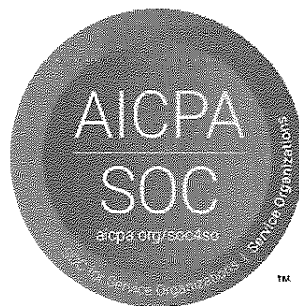
Christopher Brown  
Chief Technical Officer



## **Service Organization Control 1 Report**

### **Description of System – CenturyLink**

For the Period 1 November 2018 through 31 October 2019



## Contents

<b>Section I – CenturyLink’s Management Assertion .....</b>	<b>2</b>
<b>Section II – Independent Service Auditor’s Report .....</b>	<b>4</b>
<b>Section III – Description of Controls provided by CenturyLink.....</b>	<b>8</b>
Operations overview.....	8
Relevant Aspects of Entity Level Controls.....	9
Control Activities.....	12
<b>Section IV – Description of Control Objectives, Controls, Tests and Results of Tests .....</b>	<b>44</b>
Testing Performed and Results of Tests of Entity Level Controls .....	44
Testing of Information Produced by the Entity.....	44
Control Objectives and Related Controls for Systems and Applications.....	44
Organization and Management .....	45
Change Management –Service Delivery Process .....	48
Change Management – Changes to CenturyLink environment.....	50
Change Management – Changes to SAP Customer environment ...	53
Physical Access and Environmental Security.....	57
Logical Access – Privilege Access to Customer Servers .....	61
Access.....	62
Logical Access – Access to Customer Servers (Operating Systems).....	62
Logical Access – Access to Customer Servers (Databases).....	65
Logical Access – Access to Customer Servers (SAP Application) ..	67
Logical Access – Restriction to Other Customer Organization.....	69
Logical Access – Access to Central Infrastructure Tools.....	73
Computer Operations – Event Management .....	76
Computer Operations – Incident Resolution.....	77
Computer Operations - Backup Management .....	79
<b>Section V – Other Information Provided by CenturyLink.....</b>	<b>82</b>
1. Contingency Plan for Critical Tools.....	82
2. Infrastructure Description .....	83
3. Certifications and compliance.....	99

## Section I - CenturyLink's Management Assertion

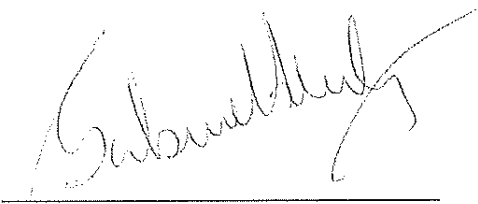
13 December 2019

We have prepared the description of CenturyLink's Data Center Operations system entitled, "Description of Controls provided by CenturyLink" (Description) for hosting user entities' systems throughout the period 1 November 2018 to 31 October 2019 for user entities of the system during some or all of the period 1 November 2018 to 31 October 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

We confirm, to the best of our knowledge and belief, that:

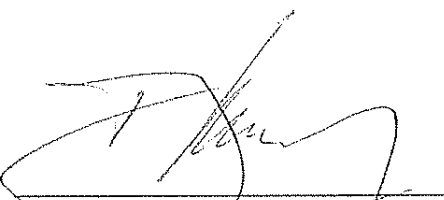
- a. The Description fairly presents the Data Center Operations system (System) made available to user entities of the System during some or all of the period 1 November 2018 to 31 October 2019 for hosting user entities' systems as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:
  - (1) Presents how the System made available to user entities of the system was designed and implemented, including, if applicable:
    - The types of services provided.
    - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System.
    - The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
    - How the System capture and address significant events and conditions
    - The process used to prepare reports and other information for user entities.
    - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
    - The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
    - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

- (2) Includes relevant details of changes to the System during the period covered by the Description.
  - (3) Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Services that each individual user entity of the system and its user auditor may consider important in the user entity's own particular environment.
- b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the 1 November 2018 to 31 October 2019 to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of CenturyLink's controls throughout the period the 1 November 2018 to 31 October 2019. The criteria we used in making this assertion were that:
- (1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.
  - (2) The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
  - (3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



---

**Gabriel del Campo**  
VP Data Center LATAM  
CenturyLink Communications, Latin America



---

**Leonardo Barbero**  
Senior VP Product and Marketing LATAM  
CenturyLink Communications, Latin America



Building a better  
working world

Pistrelli, Henry Martín y Asociados S.R.L.  
25 de mayo 487 - C1002ABI  
Buenos Aires - Argentina

Tel: +54 11 4318 1600  
Fax: +54 11 4510 2220  
ey.com

## Section II – Independent Service Auditor's Report

To: CenturyLink Data Center Outsourcing & Security Services Vice Presidency

### *Scope*

We have examined CenturyLink's description entitled Section III - Description of Controls provided by CenturyLink (Description) related to the Data Centers in Buenos Aires (Argentina), Santiago (Chile), Lima (Perú), Rio de Janeiro (Brazil), São Paulo (Brazil), Carcelén (Quito, Ecuador), Cali (Colombia) and Bogotá (Colombia) throughout the period 1 November 2018 to 31 October 2019 and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in CenturyLink's Management Assertion (Assertion). The Control Objectives and controls included in the Description are those that management of CenturyLink believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of CenturyLink's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in Section V - Other Information Provided by CenturyLink is presented by management of CenturyLink to provide additional information and is not a part of CenturyLink's Description. Information about CenturyLink's Contingency Plan for Critical Tools and Infrastructure Description has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and, accordingly we express no opinion on it.

### *CenturyLink's responsibilities*

CenturyLink has provided the accompanying assertion titled, CenturyLink's Management Assertion (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. CenturyLink is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

#### *Service auditor's responsibilities*

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Our examination was also performed in accordance with International Standard on Assurance Engagements 3402 *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period 1 November 2018 to 31 October 2019. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in the Assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

#### *Quality Control Requirements*

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

#### *Compliance with Independence and Other Ethical Requirements*

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

*Inherent limitations*

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in hosting user entities' systems. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

*Description of tests of controls*

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying Section IV – Control Objectives, Controls, Tests and Results of Tests (Description of Tests and Results).

*Opinion*

In our opinion, in all material respects, based on the criteria described in the Assertion:

- a. The Description fairly presents the System that was designed and implemented throughout the period 1 November 2018 to 31 October 2019.
- b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period 1 November 2018 to 31 October 2019, and user entities applied the complementary controls assumed in the design of CenturyLink's controls throughout the period 1 November 2018 to 31 October 2019.
- c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period 1 November 2018 to 31 October 2019 if user entity controls assumed in the design of CenturyLink's controls operated effectively throughout the period 1 November 2018 to 31 October 2019.

*Restricted use*

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of CenturyLink, user entities of CenturyLink's System during some or all of the period 1 November 2018 to 31 October 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

13 December 2019

PISTRELLI, HENRY MARTIN ASESORES S.R.L.

C.P.C.E.C.A.B.A. T° 1 F° 12



Pablo A. Dandois  
Socio

Contador Público Nacional (U.B.A.)  
C.P.C.E.C.A.B.A. T° 205 - F° 152

### Section III – Description of Controls provided by CenturyLink

#### Operations overview

CenturyLink provides local, national and global communications services to enterprise, government and carrier customers. CenturyLink's comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; Data Center and cloud-based solutions. CenturyLink serves customers in more than 450 markets in 45 countries over a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities. For more information, please visit [www.CenturyLink.com](http://www.CenturyLink.com).

The following services are offered as part of the Data Center business line: managed services, hosting, housing, office space, storage utilities, security solutions, backbone Data Center, monitoring and mail & messaging. To support its transactions in the different Latin American countries, CenturyLink has Data Center facilities at the following locations:

#### ARGENTINA

Buenos Aires (Artigas) (\*)  
Mendoza  
Córdoba  
Rosario

#### ECUADOR

Guayaquil  
Quito  
Quito Carcelén (\*)

#### BRAZIL

São Paulo (Cotia) (\*)  
Curitiba  
Rio de Janeiro (\*)

#### PERU

Lima (Surco) (\*)

#### CHILE

Santiago (\*)

#### VENEZUELA

Caracas

#### COLOMBIA

Bogotá (Colombia XV) (\*)  
Bogotá (SUBA)  
Cali (\*)

(\*) Data Centers covered by this report.



São Paulo, Jan 2, 2024.

Dear,

We have received your request for information regarding material change in internal control related to the ISAE3402. Ernst & Young Auditors prepared the latest Type II ISAE 3402 for these services and the report is dated 12/14/2023. This report includes tests of operating effectiveness for the period ending November 1, 2022 to October 31, 2023.

Cirion Technologies recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness, as well as material change to its internal controls. As of 01/02/2024, I am not aware of any material change in our control environment that would adversely affect the Auditor's Opinion reached in the November 1, 2022 to October 31, 2023 report for the above named ISAE 3402.

You should also be aware that Cirion Technologies, as a normal part of its operations, continually updates its services and technology as appropriate. In addition, the controls for all of Cirion Technologies were designed with certain responsibilities required of the system users (See User Control Considerations in the ISAE 3402 report). Cirion Technologies controls must always be evaluated in conjunction with an assessment of the strength of these user controls.

Finally, in order to conclude upon the design and effectiveness of internal controls for Cirion Technologies, you must read the current ISAE 3402 report. This letter is not intended to be a substitute for the ISAE 3402 report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Nelma Santos", with a stylized flourish at the end.

**Nelma Santos**

Regional Processes Manager  
Data Center, Cloud & Security





## **System and Organization Controls 2 (SOC 2) Type 2 Report**

### **Description of the CenturyLink Housing, Hosting and DEC 3 Services System Relevant to Security and Availability**

For the Period November 1, 2020 through October 31, 2021



## Contents

<b>Section I - CenturyLink's Management Assertion .....</b>	<b>2</b>
<b>Section II - Independent Service Auditor's Report .....</b>	<b>4</b>
<b>Section III – Description of the CenturyLink Housing, Hosting and DEC3 Services System relevant to Security and Availability .....</b>	<b>8</b>
A) Services Overview .....	8
B) Service Commitments and System Requirements .....	10
C) Relevant Aspects of Internal Controls .....	11
D) Applicable Trust Services Criteria .....	23
E) Complementary User Entity Controls .....	24
<b>Section IV – Description of Criteria, CenturyLink Controls, Test and Results of Tests .....</b>	<b>25</b>
Testing Performed and Results of Tests of Entity Level Controls .....	25
Testing of Information Produced by the Entity .....	25
Criteria and Related Controls .....	25
Subsection A .....	26
Subsection B .....	46
<b>Section V – Other Information Provided by CenturyLink .....</b>	<b>75</b>
1. Contingency Plan for Critical Tools .....	75
2. Infrastructure Description .....	76
3. Certifications and Compliance .....	83

## Section I - CenturyLink's Management Assertion

December 16th, 2021

We have prepared the accompanying "Description of the CenturyLink Housing, Hosting and DEC 3 Services System relevant to Security and Availability" (Description) of CenturyLink (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Housing, Hosting and DEC 3 Services and their supporting Data Centers located in São Paulo (Brazil), Bogotá (Colombia), Cali (Colombia) and Lima (Peru) that may be useful when assessing the risks arising from interactions with the System throughout the period 1 November 2020 to 31 October 2021, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of CenturyLink's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

- a.** The Description presents the CenturyLink Housing, Hosting and DEC 3 Services system that was designed and implemented throughout the period 1 November 2020 to 31 October 2021 in accordance with the Description Criteria.
- b.** The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls assumed in the design of CenturyLink's controls throughout the period 1 November 2020 to 31 October 2021.

- c. The CenturyLink controls stated in the Description operated effectively throughout the period 1 November 2020 to 31 October 2021 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls assumed in the design of CenturyLink's controls throughout the period 1 November 2020 to 31 October 2021.

*Gabriel del Campo*  
Gabriel del Campo (16 de December de 2021 12:07 GMT-3)

---

Gabriel Del Campo  
VP Data Center LATAM  
CenturyLink Communications, Latin America



Pistrelli, Henry Martin y Asociados S.R.L.  
25 de mayo 487 - C1002ABI  
Buenos Aires, Argentina

Tel: (54-11) 4318-1600/4311-6644  
Fax: (54-11) 4510-2220  
ey.com

## Section II - Independent Service Auditor's Report

To: CenturyLink Data Center, Cloud & Security Services Vice Presidency

### Scope

We have been engaged to report on CenturyLink's accompanying "Description of the CenturyLink Housing, Hosting and DEC 3 Services System relevant to Security and Availability" of its Housing, Hosting and DEC 3 Services system for the Data Centers in Bogotá (Colombia), Cali (Colombia), Lima (Perú) and São Paulo (Brazil) throughout the period 1 November 2020 to 31 October 2021 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period 1 November 2020 to 31 October 2021 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The Description also indicates that CenturyLink's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of CenturyLink's controls are suitably designed and operating effectively, along with related controls at the service organization. Our procedures did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in the accompanying "Other Information Provided by CenturyLink" is presented by management of CenturyLink to provide additional information and is not part of CenturyLink's Description. Such information has not been subjected to the procedures applied in our engagement and, accordingly we express no opinion on it.

### CenturyLink's responsibilities

CenturyLink is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. CenturyLink has provided the accompanying assertion titled, CenturyLink's Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. CenturyLink is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the



trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system (5) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

### ***Our responsibilities***

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our procedures.

Our engagement was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria throughout the period 1 November 2020 to 31 October 2021. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- performing procedures to obtain evidence about whether the description is presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Our engagement also included performing such other procedures as we considered necessary in the circumstances.



### ***Our independence and quality control***

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

We apply International Standard on Quality Control 1 and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

### ***Inherent limitations***

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

### ***Description of tests of controls***

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying "Description of Criteria, CenturyLink Controls, Test and Results of Tests" (Description of Tests and Results).

### ***Opinion***

In our opinion, in all material respects:

- a. the Description presents the CenturyLink Housing, Hosting and DEC 3 Services system that was designed and implemented throughout the period 1 November 2020 to 31 October 2021 in accordance with the Description Criteria.
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and user entities applied the controls assumed in the design of CenturyLink's controls throughout the period 1 November 2020 to 31 October 2021.
- c. the controls stated in the description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 1 November 2020 to 31 October 2021, if user entity controls assumed in the design of CenturyLink's controls operated effectively throughout the period 1 November 2020 to 31 October 2021.



### ***Restricted use***

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of CenturyLink, user entities of CenturyLink's Housing, Hosting and DEC 3 Services system during some or all of the period 1 November 2020 to 31 October 2021 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

December 16th, 2021

C.A.B.A, Buenos Aires

PISTRELLI, HENRY MARTIN ASESORES  
S.R.L.  
C.P.C.E.C.A.B.A. T° 1 F° 12

  
Pablo Dandois (16 de December de 2021 17:23 GMT-3)

Pablo A. Dandois  
Socio  
Contador Público Nacional (U.B.A.)  
C.P.C.E.C.A.B.A. T° 205 - F° 152

### **Section III – Description of the CenturyLink Housing, Hosting and DEC3 Services System relevant to Security and Availability**

#### **A) Services Overview**

##### About CenturyLink

CenturyLink provides local, national and global communications services to enterprise, government and carrier customers. CenturyLink's comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; data center and cloud-based solutions. CenturyLink serves customers in more than 450 markets in 45 countries over a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities. For more information, please visit [www.lumen.com](http://www.lumen.com).

The following services are offered as part of the Data Center business line: Cloud Services, Cloud Security Services, Managed Services, Infrastructure Services, Security Services, Hosting, Housing. To support its transactions in the different Latin American countries, CenturyLink has Data Center facilities at the following locations:

##### ARGENTINA

Buenos Aires (Artigas)  
Mendoza  
Córdoba  
Rosario

##### ECUADOR

Guayaquil  
Quito  
Quito (Carcelén)

##### BRAZIL

São Paulo (Cotia) (\*)  
Curitiba  
Rio de Janeiro

##### PERU

Lima (Surco) (\*)

##### CHILE

Santiago (Huechuraba)

##### VENEZUELA

Caracas

##### COLOMBIA

Bogotá (Colombia XV) (\*)  
Bogotá (SUBA)  
Cali (Santa Mónica) (\*)

(\*) Data Centers covered by this report.



São Paulo, Jan 02, 2024.

Dear,

We have received your request for information regarding material change in internal control related to the ISAE3402. Ernst & Young Auditors prepared the latest Type II ISAE 3402 for these services and the report is dated 12/19/2022. This report includes tests of operating effectiveness for the period ending November 1, 2022 to October 31, 2023.

Cirion Technologies recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness, as well as material change to its internal controls. As of 01/02/2024, I am not aware of any material change in our control environment that would adversely affect the Auditor's Opinion reached in the November 1, 2022 to October 31, 2023 report for the above named ISAE 3402.

You should also be aware that Cirion Technologies, as a normal part of its operations, continually updates its services and technology as appropriate. In addition, the controls for all of Cirion Technologies were designed with certain responsibilities required of the system users (See User Control Considerations in the ISAE 3402 report). Cirion Technologies controls must always be evaluated in conjunction with an assessment of the strength of these user controls.

Finally, in order to conclude upon the design and effectiveness of internal controls for Cirion Technologies, you must read the current ISAE 3402 report. This letter is not intended to be a substitute for the ISAE 3402 report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Nelma Santos", with a stylized flourish at the end.

**Nelma Santos**

Regional Processes Manager  
Data Center & Security





## **System and Organization Control 3 (SOC 3) Report**

### **Report of the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System Relevant to Security and Availability**

For the Period November 1, 2022 through October 31, 2023



## Contents

<b>Section I - Report of Independent Accountants .....</b>	<b>2</b>
<b>Section II - Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing and DEC3 Services system Based on the Trust Services Criteria for Security and Availability.....</b>	<b>4</b>
<b>Attachment A – Description of Cirion Technologies Housing, Hosting and DEC3 Services System.....</b>	<b>5</b>
<b>Attachment B – Principal Service Commitments and System Requirements .....</b>	<b>13</b>



Pistrelli, Henry Martin y Asociados S.R.L.  
25 de mayo 487 - C1002AB1  
Buenos Aires, Argentina

Tel: (54-11) 4318-1600/4311-6644  
Fax: (54-11) 4510-2220  
ey.com

## Section I - Report of Independent Accountants

To: Cirion Technologies Data Center, Cloud & Security Services Vice Presidency

### *Scope:*

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing and DEC 3 Services system Based on the Trust Services Criteria for Security and Availability (Assertion), that Cirion Technologies' controls over the Cirion Technologies Hosting, Housing/Colocation and DEC 3 Services System (System) were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### *Management's Responsibilities*

Cirion Technologies' management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

### *Our Responsibilities*

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Cirion Technologies' relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Cirion Technologies' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.



*Inherent limitations:*

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Cirion Technologies' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

*Opinion:*

In our opinion, Cirion Technologies' controls over the system were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

December 19th, 2023

C.A.B.A, Buenos Aires

PISTRELLI, HENRY MARTIN ASESORES  
S.R.L.  
C.P.C.E.C.A.B.A. T° 1 F° 12

  
Pablo Dandois (19 de dezembro de 2023 15:13 GMT-3)

Pablo A. Dandois  
Socio  
Contador Público Nacional (U.B.A.)  
C.P.C.E.C.A.B.A. T° 205 - F° 152



**Section II - Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services system Based on the Trust Services Criteria for Security and Availability**

December 19th, 2023

We, as management of, Cirion Technologies are responsible for:

- Identifying the Cirion Technologies Hosting, Housing/Colocation and DEC 3 Services System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

*Gabriel del Campo*  
Gabriel del Campo (19 de dezembro de 2023 12:51 GMT-3)

---

Gabriel Del Campo  
VP Data Center  
Cirion Technologies

## **Attachment A – Description of Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System**

### **About Cirion Technologies**

Cirion Technologies provides local, national and global communications services to enterprise, government and carrier customers. Cirion Technologies' comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; data center and cloud-based solutions. Cirion Technologies serves customers in more than 450 markets in 45 countries over a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities. For more information, please visit [www.ciriontechnologies.com](http://www.ciriontechnologies.com).

The following services are offered as part of the Data Center business line: managed services, hosting, housing, office space, storage utilities, security solutions, backbone Data Center, monitoring and mail & messaging. To support its transactions in the different Latin American countries, Cirion Technologies has Data Center facilities at the following locations:

#### **ARGENTINA**

Buenos Aires (BUE1)  
Mendoza (MEN1)  
Córdoba (COR1)  
Rosario (ROS1)

#### **ECUADOR**

Guayaquil (GUA1)  
Quito (QUI1)  
Quito (QUI2)

#### **BRAZIL**

São Paulo (SAO1) (\*)  
Curitiba (CUR1)  
Rio de Janeiro (RIO1)

#### **PERU**

Lima (LIM1) (\*)

#### **CHILE**

Santiago (SAN1) (\*)

#### **VENEZUELA**

Caracas (CAR1)

#### **COLOMBIA**

Bogotá (BOG2) (\*)  
Bogotá (BOG1)  
Cali (CAL1) (\*)

#### **MEXICO**

Ciudad de México (MEX1)

#### **PANAMÁ**

Ciudad de Panamá (PAN1)

(\*) Data Centers covered by this report.

## Components of the System:

The following Cirion Technologies services are covered in this report:

- Housing/Colocation

The Housing/Colocation services enable a company to place its mission critical equipment in a high-availability computing center with distinctive infrastructure characteristics, featuring a private area for the development of its business, with reliable high-performance connectivity to the inter-carrier networks and the Internet. Environmental conditions are ensured by applying controls, and which are monitored to provide a suitable environment.

- Hosting

The main objective of the Cirion Technologies Hosting services is to offer customers dedicated hardware and a secure environment for the installation of their applications, avoiding the need for these customers to perform maintenance and operating tasks. Environmental conditions are ensured by applying controls, and which are monitored to provide a suitable environment.

The current Hosting service is based on leading-edge servers, fully installed with base software, and configured in the most flexible way to cater to the needs of customers.

Cirion Technologies also has an excellent track record of distribution of these services and a solid commitment to best practices in management, monitoring and services.

- DEC 3

DEC 3 (Dynamic Enterprise Computing v3) is a service developed to provide safe and flexible cloud processing capacity to corporate users. By means of Computer Components, Consumer Elements that will determine the use of such components with added functionalities and supplementary Services that complete the solution, Customers may create a computing environment adequate for each of their essential applications. This way, customers can dispose and manage network, security and computation systems in a centralized and interrelated way, with complete independence of the physical components, the basic software and the architectures that support them. This concept helps the addition of new environments that cover the efficiency, technical and economic requirements from demanding applications.

DEC 3 is a Community Cloud Service, basically implemented with VMware tool. This tool provides a portal interface to clients to let them manage their environment with autonomy and in a simple and intuitive way, by using Vrealize Automation. Customers are able to manage their environment by creating virtual machines and limited to the resources hired to Cirion Technologies. Those limits are configured by Cirion Technologies operators for each client. Cirion Technologies performs capacity analysis from the computer resources of the cluster by using VCenter tool, from VMware,

Nevertheless, customers can delegate Cirion Technologies specialists the management of approved operational systems, databases and applications by hiring additional managed services.

## **Applicable Trust Services Criteria**

The following Trust Services Criteria set forth in TSP section 100, “Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria, issued 2017) are covered by this report:

- **Security**

The security criterion refers to the protection of systems that use electronic information to process, transmit or transfer and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

- **Availability**

This criterion refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. The availability criterion does not address system functionality (the specific functions a system performs) or system usability (the ability of users to apply system functions to the performance of specific tasks or problems) but does address whether the system includes controls to support accessibility for operation, monitoring, and maintenance.

## **Relevant Aspects of Internal Controls**

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity’s board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- **Risk Management** – The entity’s identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Information and Communication** – Surrounding these activities are information and communication systems. These enable the entity’s people to capture and exchange information needed to conduct and control its operations.
- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- **Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary

to address risks to achievement of the entity's control objectives are effectively carried out.

This section briefly describes the components of Cirion Technologies' internal controls over the trust services principles and criteria of security and availability that may be relevant to customers.

### **Control environment**

Cirion Technologies' organizational structure and, specifically, the Data Center's area organizational structure provides a framework for the planning, management and control of operations in which personnel and business functions are segregated into departments based on documented job descriptions. With this approach, the organization defines responsibilities as well as reporting and communication lines, and the employees focus on the tasks unique to their positions within the company. Sales (Sales), Operations (Network Operations) and Product (Product & Marketing) functions are organized under different VPs, who report to the company's President Regional.

The Data Center, Cloud & Security area (which belongs to the Product & Marketing area) is in charge of maintaining central infrastructure and carrying out the processes supporting the operation. In addition, there is a customer service area that participates in the first customer-service assurance level.

Global Security area is responsible for establish global policies of security for Cirion Technologies and the Data Center, Cloud and Security is responsible for procedures for maintain the security of every Data Center through monitoring activities and control activities on their internal system, with the objective to avoid external attacks or internal deficiencies.

Customer accounts are managed by an account executive belonging to the Sales vertical, who receives the assistance of sales support from the Data Center Product Line. There is also a Project Manager in the Data Center Product Line, who is in charge of implementing the service agreed upon with the customer.

Being part of GCL Group, Cirion Technologies is subject to the Foreign Corrupt Practices Act (the FCPA), which prohibits companies and their intermediaries from making improper payments to foreign officials for the purpose of obtaining or keeping business and/ or other benefits. The Company has policies and procedures designed to ensure that the company, its employees and agents comply with the FCPA.

The company has an employee recruitment policy in place that provides for the general conditions of the recruitment process. The recruitment process for each candidate is documented in the Success Factors tool, where it also possible to evaluate the performance of each employee and their goals.

The Company is committed to upholding the highest standards of ethics in relationships with customers, employees, shareholders and the business community. This commitment to ethical business practices is confirmed and contained in a Code of Conduct and Business Conduct policy, which includes counsel on ethical conduct and emphasizes its significance in all business activities.

The Code of Conduct must be read and accepted by all the employees joining the company.

The company's Code of Conduct has a specific section dealing with preventive measures to protect employees against conflicts of interest with the customers. A conflict of interest

is defined as any particular investment, interest, activity, association or service of Cirion Technologies employees or of any of their direct family members, which biases or seems to bias their judgment upon making decisions for the best benefit of Cirion Technologies or its customers.

The policies and procedures effective at the Company are applied both to Cirion Technologies' employees and contractors.

Cirion Technologies has a training calendar for all employees with mandatory courses about security, privacy among others to have updated the ethical knowledge of the company.

Vendor agreements include confidentiality commitments with Non-Disclosure Agreement clauses and the acceptance of the code of conduct.

The Board of Directors has Committees that have a number of independent Board members and where each Board and Committee member is qualified to serve in such capacity.

## **Risk assessment**

### **Internal Audit**

The Company's Internal Audit department, led by the Senior VP of Internal Audit and SOX Compliance, reports functionally to the Audit Committee of the Board of Directors and administratively to the Chief Financial Officer.

Internal Audit supports the Audit Committee and management through objective risk-based assurance and advisory services designed to add value and improve the operations of the Company. Internal Audit brings a systematic, disciplined approach to evaluating and recommending improvements to the risk management, control and governance processes, relating to, but not limited to operational, financial, compliance and information systems/technology.

Internal Audit has responsibility to:

- a) Develop a flexible annual audit plan using an appropriate risk-based methodology and submit the plan for review and approval by the Audit Committee.
- b) Regularly communicate to the Audit Committee information of the results of Internal Audit activities and progress on the annual plan.
- c) Issue audit reports to management summarizing significant audit observations and recommendations.
- d) Evaluate the action taken by management to address recommendations made by Internal Audit.
- e) Review the systems of internal control and risk management that management has implemented. This includes reviews of current and planned financial, management and operational systems, as well as steps taken to mitigate risks and impediments to the achievement of corporate objectives.

## Risk Management

Data Center, Cloud & Security area, which supports local and regional directions, performs an annual audit plan for Data Center (Local and Regional audits). This plan must be reviewed by the correspondent Direction. Every audit plan has the evaluations and recommendations of improvements on processes, systems and infrastructure. This audit plan establishes the internal and external audits to be realized for each Data Center. Audits can be required from clients or from Cirion Technologies.

In addition to internal assessments, Cirion Technologies pursues various industry-recognized programs, including SOC 1 reports as well as this SOC 2 report, and ISO 27001 certification. The services and locations provided are ISO 27001 certified.

Every issue identified on the audits is documented on Cirion Technologies SharePoint to do a follow up and is reviewed in direction meetings to define a resolution plan. This is documented in the Cirion Technologies SharePoint and in the risk matrix, if necessary.

As part of the Risk Management and risk mitigation processes, Cirion Technologies has contracted insurance policies in place for operational risks such as earthquakes, flooding, storms and machine breakage.

## **Information & Communication**

Cirion Technologies has a regulatory framework for its information system area, which consists of policies, procedures, configuration standards and technical documentation. Policies include the definition of basic standards for information protection, information security, user administration, security incidents administration and passwords, among others.

Based on the general standards defined, procedures were performed stating the steps for the implementation thereof. In addition, there are technical standards and procedures stating the values expected for operating systems, as well as the description of procedures stating the tasks to be performed to modify passwords or review logs, among others.

There are also formalized procedures to require and implement changes to programs supporting the company's transactions and the chart of account supporting book entries. Such procedures include defining the authorizations required in each case and the duties of each process participant.

The tools supporting Cirion Technologies operations require a username and a password. They validate if the user is authorized to perform an operation by verifying whether such user has a profile assigned for such purpose.

Cirion Technologies has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; annual training programs tailored based on employee roles and responsibilities that may include Code of Conduct, Cirion Technologies Information Security Awareness, Business Continuity Management, Privacy Overview; regular management meetings for updates on business performance and other matters; and electronic means such as video conferencing, electronic mail messages, and the posting of information via the Cirion Technologies intranet on topics such as entity organization structure, process, organizational roles and responsibilities,

reporting of information security incidents and guidelines describing change management.

Services engagements are defined on Master Services Agreements to communicate Cirion Technologies responsibilities to clients.

Cirion Technologies performs an annual operational plan to determinate objectives for different areas as Sales, Delivery or Operative, among others. The plan is communicated to the areas involved to prepare or take actions to achieve the goals defined.

### **Monitoring**

Monitoring activities are carried out through different methods. Management reviews the results of regulatory examinations, reports by Cirion Technologies' external auditor and client communications.

Internal monitoring is carried out by an administration committee and, specifically for the business line, by the data center management. Supervisory staff in general, monitors the performance, quality and controls as a normal part of its activities. Monitoring activities include reviewing the operating performance, quality control reviews and different reports that measure the results of processes involved in the data center operation.

The Data Center management, specifically the Executive VP, monthly analyzes financial and non-financial KPIs variations to study and examine business and operational performance and trends evolution. The analysis is performed for each branch.

### **Control Activities**

Cirion Technologies has implemented procedures and controls to achieve service commitments and service requirements in accordance with its defined policies.

- ***Security Organization***
- ***Logical Access – User Access Management***
- ***Cybersecurity***
- ***Physical Access***
- ***System Monitoring and Incident Management***
- ***Change Management***
- ***Environmental Controls***
- ***Backups***
- ***Availability***

### **Complementary User Entity Controls (CUECS)**

Housing/Colocation, Hosting and DEC3 Services security is a shared responsibility between the service provider and its customer. Cirion Technologies Housing/Colocation,

Hosting and DEC3 Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Cirion Technologies Housing, Hosting and DEC3 Infrastructure’s controls are suitably designed and operating effectively, along with related controls at Cirion Technologies Housing, Hosting and DEC3 Infrastructure.

### **Impact of Covid-19 (Corona Virus)**

In response to the global Covid-19 pandemic and at the direction of local, state and federal / governmental authorities in the jurisdictions in which we operate, Cirion Technologies implemented a work from home policy as of March 2020 for all non-essential employees and vendors. The architecture of the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System has been designed in a manner which enables Cirion Technologies to continue business as usual operations irrespective of the physical location of employees.

Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System data center teams continue to perform and sustain standard operating procedures, as they relate to the controls tested in this audit. Due to the novel coronavirus, where required by local mandates, precautionary measures and limitations have been placed on the number of visitor staff and duration of visits at the data centers. In the event of a procedural impact or modification for the purposes of conforming to the constraints presented by Covid-19, Cirion Technologies Hosting, Housing and DEC3 Services System data center teams have initiated and executed any required approvals for such exceptions. Critical functions continue to operate.

## **Attachment B – Principal Service Commitments and System Requirements**

### **Overview**

Cirion Technologies designs its processes and procedures to meet its objectives for the Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System. Those objectives are based on the service commitments that Cirion Technologies makes to user entities, the laws and regulations that govern the provision of the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System, and the financial, operational and compliance requirements that Cirion Technologies has established for the services.

The Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Cirion Technologies operates.

Security and Availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the Cirion Technologies website. Security, and Availability commitments are standardized and include, but are not limited to, the following:

- Security principle inherent to the fundamental design of the Cirion Technologies System is designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- Security principle inherent to the fundamental design of the Cirion Technologies System is designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principle inherent in the fundamental design of the Cirion Technologies System is designed to replicate critical system components at various locations and maintain the level of service to meet agreed SLAs.

Cirion Technologies establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cirion Technologies' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System.

As an Infrastructure as a Service (IaaS) System, the Cirion Technologies System is designed based on a shared responsibility model where both Cirion Technologies and the customers are responsible for aspects of security and availability. Details of the responsibilities of customers can be found on the Cirion Technologies website and in the Customer Agreement.


# Multi User Report - ISAE 3402 - Cirion 2023 - SOC3


Relatório de auditoria final

2023-12-19


Criado em:	2023-12-19
Por:	Edney Kieger (edney.kieger.ext@ciriontechnologies.com)
Status:	Assinado
ID da transação:	CBJCHBCAABAARStyOauCCIlde8grexw-O-fNqXDHbzf0
Quantidade de documentos:	1
Contagem de páginas do documento:	14
Quantidade de arquivos de apoio:	0
Contagem de páginas dos arquivos de apoio:	0

## Histórico de "Multi User Report - ISAE 3402 - Cirion 2023 - SOC3"

-  Documento criado por Edney Kieger (edney.kieger.ext@ciriontechnologies.com)  
2023-12-19 - 14:59:13 GMT
-  Documento enviado por email para gabriel.delcampo@ciriontechnologies.com para assinatura  
2023-12-19 - 15:02:09 GMT
-  Documento enviado por email para pablo.dandois@ar.ey.com para assinatura  
2023-12-19 - 15:02:09 GMT
-  Email visualizado por gabriel.delcampo@ciriontechnologies.com  
2023-12-19 - 15:51:30 GMT
-  Contrato visualizado por gabriel.delcampo@ciriontechnologies.com  
2023-12-19 - 15:51:32 GMT
-  O signatário gabriel.delcampo@ciriontechnologies.com inseriu o nome Gabriel del Campo ao assinar  
2023-12-19 - 15:51:54 GMT
-  Documento assinado eletronicamente por Gabriel del Campo (gabriel.delcampo@ciriontechnologies.com)  
Data da assinatura: 2023-12-19 - 15:51:56 GMT - Fonte da hora: servidor
-  Email visualizado por pablo.dandois@ar.ey.com  
2023-12-19 - 18:12:33 GMT

 Contrato visualizado por pablo.dandois@ar.ey.com


2023-12-19 - 18:12:34 GMT

 O signatário pablo.dandois@ar.ey.com inseriu o nome Pablo Dandois ao assinar

2023-12-19 - 18:13:28 GMT

 Documento assinado eletronicamente por Pablo Dandois (pablo.dandois@ar.ey.com)

Data da assinatura: 2023-12-19 - 18:13:30 GMT - Fonte da hora: servidor

 Contrato finalizado.

2023-12-19 - 18:13:30 GMT