SOC1 Report - *Service Organization Control 1* - About the Description, Design and Operational Effectiveness of Controls Related to the Information Technology Environment during the Period from January 1, 2022 to December 31, 2022.

ASCENTY DATA CENTERS E TELECOMUNICAÇÕES S/A.
ISAE3402 - Type II

Building a better working world

INDEX

Ascenty
A Digital Realty and Brookfield Infrastructure JV

I. Management statement about the service

We prepared the Description of the processes and controls of physical access and infrastructure, covering the transactions that occurred in the period from January 1, 2022 to December 31, 2022, for service user entities (Clients), and for independent auditors who have sufficient understanding to consider the Description.

Ascenty confirms what it is given to know and know, that:

a) The Description adequately presents the processes and physical access control and infrastructure made available to customers from January 1, 2022 to December 31, 2022 for the processing of their transactions. The criteria used to make this statement considered that the Description of controls provided by Ascenty ("Description"):

> (1) presents the way in which the services available to customers were designed and implemented, including the Physical Access Management processes to the Data Center, Change Management and *Facilities Management*.
>
> (2) does not omit or distort information relevant to the scope and its associated controls that support it, while recognizing that the Description is prepared to meet the common needs of a wide range of clients and the clients' independent auditors and that , therefore, cannot include all aspects that each individual client and its auditor may consider important in the clients' specific environment.

b) The Description includes relevant details of system improvements during the period from January 1, 2022 to December 31, 2022.

c) The controls related to the control objectives presented in the Description of Control Objectives, Controls, Tests and Test Results operated effectively throughout the period from January 1, 2022 to December 31, 2022 to achieve said control objectives . The criteria we used to make this statement were that:

(1) the risks that threaten the achievement of the control objectives presented in the Description have been identified;

(2) The controls identified in the description were designed and tested for the period from January 1, 2022 to December 31, 2022; It is,

(3) The company's Compliance area is constantly monitoring and implementing improvements in controls.

Fabio Trimarco

Fabio Trimarco
Compliance and Quality Director
Ascenty Data Centers e Telecomunicações S/A

Marcos Siqueira

Marcos Siqueira
VP of Operations
Ascenty Data Centers e Telecomunicações S/A

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

II. Opinion of the Independent Auditors

Independent auditors' assurance report on the description, design and operational effectiveness of Ascenty Data Centers e Telecomunicações S/A controls.

To Ascenty Data Centers e Telecomunicações S/A.

II.1 Scope

As requested by Your Lords and described in our employment contract, we were hired to issue a report on the Description of Physical Access Controls, Changes and *Facilities* of Ascenty Data Centers e Telecomunicações S/A (Ascenty) observing the operational effectiveness of its controls, aiming to achieve the relative objectives presented in the Description for the period from January 1, 2022 to December 31, 2022 for the following Data Centers:

- Data Center of Campinas;
- Jundiaí Data Center (1);
- Jundiaí Data Center (2);
- Hortolândia Data Center (1);
- Hortolândia Data Center (2);
- Data Center of Hortolândia (3);
- Data Center of Hortolândia (4);
- Data Center of Sumaré (1);
- Data Center of Sumaré (2);
- Fortaleza Data Center;
- Data Center of São Paulo (1);
- Data Center of São Paulo (2);
- Data Center of São Paulo (3);
- Data Center of Rio de Janeiro (1);
- Data Center of Rio de Janeiro (2);
- Paulínia Data Center;
- Vinhedo Data Center (1);
- Vinhedo Data Center (2); and
- Data Center of Chile (1).

The Description only includes the objectives of control and controls related to Ascenty and excludes the objectives of control and controls related to third-party service providers, and objectives of controls and complementary controls performed by user entities (Customers). The extent of our review did not cover the controls of these third-party service provider organizations, as well as controls performed by customers.

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

The information contained in Section V – 'Other Information provided by Ascenty' - is presented by Ascenty itself with the aim of providing additional information and is not part of the Description prepared by Ascenty. This information has not been subject to the procedures applied in our assessment of the Description.

II.2 Ascenty's Responsibilities

Ascenty provided the attached statement in section I “Declaration by Ascenty Data Centers e Telecomunicações” on the adequacy of the presentation of the Description and the adequacy of the design and operational effectiveness of the controls, for the achievement of the control objectives related and presented in the Description. Ascenty is also responsible for the completeness, precision, and method of preparation of the Description and Declaration, as well as for the declaration of the control objectives presented in the Description.

Ascenty is also responsible for providing the services contemplated in the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria presented in the Declaration and designing, implementing and documenting controls to achieve the relative objectives of control presented in the Description.

II.3 Our independence and Quality Control

We comply with the independence and other ethical requirements of the *International Code of Ethics for Professional Accountants Council* (including International Independence Standards), which is based on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

We apply the International Quality Control Standard I and accordingly maintain a comprehensive quality control system, including documented policies and procedures relating to compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

II.4 Responsibilities of the Independent Auditor

Our responsibility is to express an opinion on the adequacy of the presentation of the Description and the adequacy of the design and operating effectiveness of controls to achieve said control objectives specified in the Description, based on our procedures. Our examination was conducted in accordance with ISAE 3402, Reporting on Assurance of Controls in Service Organizations, issued by the *International Auditing and Assurance Standards Board (IAASB)*. This standard requires that we observe the ethical requirements, plan, and perform our examination to obtain reasonable assurance that the description is adequately presented in all material respects, that the controls were properly designed and

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

operated effectively to achieve the related control objectives presented. in the Description, from January 1, 2022 to December 31, 2022.

An examination of a service organization's System Description and the adequacy of the design and operating effectiveness of a service organization's controls to achieve the control objectives set out in the Description involves performing procedures to obtain evidence about the adequacy of the presentation of the Description, adequacy of the design and operational effectiveness of said controls to achieve the control objectives. Our procedures included assessing the risks of the Description not being adequately presented and the controls not being adequately designed or operating effectively to achieve the stated control objectives.

Our procedures also include testing the operating effectiveness of such controls, which we believe are necessary to provide reasonable assurance that the control objectives set out in the Description have been achieved. Such an examination also includes evaluating the overall presentation of the Description, the adequacy of the control objectives stated therein, and the adequacy of the criteria specified by the service organization and described in the Statement. We believe that the evidence we have obtained is sufficient and adequate to provide a reasonable basis for our opinion.

II.5 Inherent Limitations

The Description is designed to meet the common needs of a wide range of user entities and their auditors, and therefore cannot include all aspects that each individual client may find important in its specific environment. By their nature, a service organization's controls may not prevent or detect and correct all errors or omissions. In addition, the future projection of any assessment of the adequacy of the presentation of the Description, or conclusions about the adequacy of the design or operating effectiveness of controls to achieve related control objectives, is subject to the risk that the service organization's controls become inadequate or fail.

II .6 Opinion

Our opinion was based on the matters described in this report and did not cover the evaluation and adequacy of the design or operational effectiveness of the complementary controls of the user organizations.

The criteria used in forming our opinion are described in Management's Statement, in section I of this report “Management's Statement of Service Provided”.

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

In our opinion:

A. The description of controls adequately presents Ascenty's Physical Access, Change Management and *Facilities Controls*, which were designed and implemented in the period from January 1, 2022 to December 31, 2022.

B. The controls related to the control objectives presented in the Description were adequately designed to provide reasonable assurance that the control objectives were achieved considering the operation effectively in the period from January 1, 2022 to December 31, 2022.

C. The controls tested were sufficient to provide reasonable assurance that the control objectives set out in the Description were achieved and the controls operated effectively from January 1, 2022 to December 31, 2022.

II.7 Description of controls design tests

The specific controls tested and the nature, timing, and results of said tests are presented in Section IV - Description of Objectives of Controls, Controls, Tests and Test Results.

II.8 Restricted use

This report, including the description of the controls design and operation tests and their results for the period from January 1, 2022 to December 31, 2022 , in the Description of Control Objectives, Controls, Tests and Test Results are intended exclusively for the information and use of Ascenty Data Centers e Telecomunicações S/A , for the service user entities (Clients) and the independent auditors of said user entities, who have sufficient understanding to consider it, along with other information, including on controls implemented by the user entities themselves, when assessing the risks of material misstatements in the financial statements of the user entities. This report must not be used by any third parties other than the aforementioned specified parties.

ERNST & YOUNG
Auditores Independentes S.S.
CNPJ 61.366.936/0002-06

Francesco Giglio Bottino

Francesco Bottino
CRC - RJ 65261/O
Partner

Ascenty
A Digital Realty and Brookfield Infrastructure JV

III. Description of Systems, Processes and Controls Provided by Ascenty for the Period from January 1, 2022 to December 31, 2022

III.1. About Ascenty

Ascenty offers its customers a combination of optical fiber networks and proprietary Data Center services.

Connectivity services to service operators via fiber optic networks began in the second half of 2011, in the ABC region of São Paulo. In February 2012, Ascenty was acquired, based in São Paulo, focused on colocation and connectivity services. From there the name Ascenty was adopted.

The Data Centers are distributed as follows:

1. In the city of Campinas/SP, opened in October 2012;
2. In the city of Jundiaí/SP (JDI1), opened in August 2014;
3. In the region of Maracanaú/CE, opened in June 2015;
4. In the city of Hortolândia/SP (HTL1), opened in December 2015;
5. In the city of Osasco/SP (SP1), opened in March 2017;
6. In the city of Osasco/SP (SP2), opened in May 2017;
7. In the city of Sumaré/SP (SUM1), opened in July 2017;
8. In the city of Rio de Janeiro/RJ (RIO1), opened in November 2017;
9. In the city of Paulínia/SP (PLN), opened in May 2019;
10. In the city of Jundiaí/SP (JDI 2), opened in August 2019;
11. In the city of Hortolândia/SP (HTL 2), opened in August 2019;
12. In the city of Hortolândia/SP (HTL 3), opened in August 2019;
13. In the city of Sumaré/SP (SUM2), opened in September 2019;
14. In the city of Vinhedo/SP (VND1), opened in November 2019;
15. In the city of Osasco/SP (SP3), opened in July 2020;
16. In the city of Vinhedo/SP (VND2), opened in October 2020;
17. In the Metropolitan Region of Santiago/Chile (CHL1), opened in November 2020;
18. In the city of Hortolândia/SP (4), opened in December 2021; and,
19. In the city of Rio de Janeiro/RJ (RIO2), opened in February 2022.

Commitment and requirements with customers

Ascenty's strategy is aimed at operating Data Centers with its own fiber optic networks to promote high-capacity colocation and connectivity services, focusing on serving national and international clients, always respecting the legislation in force in the country.

III.2. Report Scope

The scope of this report includes physical access processes and infrastructure, which Ascenty has determined to be significant for its clients from a financial statement perspective. Are they:

- Physical Access Management – Ascenty's controls must provide reasonable assurance that only authorized persons have access to the Data Center's restricted environments.

- Change Management – Controls to provide reasonable assurance that changes to the environment are approved, documented and homologated before being transported to the system/equipment production environment.

- *Facilities* Management - Ascenty's controls must provide reasonable assurance that only authorized people have access to the Data Center's restricted environments.

Note : For the controls related to the Change Management process, our analyzes were limited to the Elipse and BMS (*Building Management System*) systems.

We present below a brief description of the physical access and infrastructure processes and the respective controls.

Management of Physical Access to the Data Center.

All of the company's Data Centers are located in strategic locations that have a 24x7 doorman and access by employees, service providers and customers is controlled via access badges and biometrics. Visitor access is allowed only after registration with the presentation of original documents and, in the case of cargo vehicles, a search carried out by the security team.

Access to all critical rooms in the Data Center is controlled by double authentication systems (badge and biometrics).

Access Grant Control

Employees: The Human Resources department opens a call requesting access to the ITSM tool and forwards the call to the access and monitoring department, which analyzes the employee's position and department, registers in the access system and grants a profile of pre-approved accesses according to the position/department constant with the data center specific access matrix.

The process for granting access to employees is detailed in the Data Center access policy " *POL-SE-0001 - Physical Security Policy* ", in the procedures " *PRO-SE-0001 - Operational Process for Physical Access to the Data Center* " and " *PRC-SE-0001 - Procedure for Physical Access to the DC* ", in the latter case, we list the main steps below:

1. PRC-RH-0001 - Recruitment and selection procedure.

2. PRC-RH-0002 - Hiring procedure:
    2.1. Request for access to IT systems
    2.2. New employee access request (Release of physical access)

3. PRC-SE-0001 - Physical Access Procedure to the DC:
    3.1. Registration in the access system according to the Access Matrix
    3.2. badge designation
    3.3. biometrics registration
    3.4. access test

Customers: In the design phase, the pre-authorized access form is filled out, where the person responsible for the customer, categorized at level N5, must inform which employees can access the Data Center, categorizing access according to the levels described below:

- N1 - Authorization to open a ticket (Service Desk) for requesting services
- N2 - Authorization to open tickets (Service Desk) and access the customer room (access the equipment only via the console).
- N3 - Authorization to open tickets (Service Desk), access the customer room, enter the data center for installation, maintenance and removal of equipment.
- N4 - Authorization to open tickets (Service Desk), access the customer room, enter the data center for installation, maintenance and removal of equipment, in addition to creating temporary access tickets to the Data Center and/or Data Hall.
- N5 - Authorization to open tickets (Service Desk), access the customer room, enter the data center for installation, maintenance and removal of equipment, modify the list of pre-authorized people to enter the Data Center and create a ticket for temporary access to the Data Center and/or Data Hall.

Whenever the customer's technicians need to access the Data Center System, the access request must be made by opening a ticket in the ITSM tool, which will be sent to the access and monitoring department. The access and monitoring department will verify the call and will assign accesses according to the pre-approved profiles for the client.

The process for granting access to customers is detailed in the Data Center access policy " *POL-SE-0001 - Physical Security Policy* ", in the procedures " *PRO-SE-0001 - Operational Process for Physical Access to the Data Center* " and " *PRC-SE-0001 - Physical Access Procedure to the DC* ", in the latter case we discriminate below:

1. POL-SE-0001 - Physical Security Policy.

2. PRO-SE-0001 - Operational Process for Physical Access to the Data Center.

3. PRC-SE-0001 - Physical Access Procedure to the DC:
    - 3.1. Request with customer pre-authorization form
    - 3.2. Registration in the access system according to the Access Matrix
    - 3 .3. Badge designation (according to access levels)
    - 3.4. biometrics registration
    - 3.5. access test

Service providers: Requesting access to service providers must be done via the ITSM tool. The calls must contain the period of permanence of the service provider in the Data Center, which places the provider needs to have access and indicate the employee responsible for the service provider. The Access and Monitoring department verifies the request and assigns the pre-approved profiles to the provider.

The process for granting access to service providers is detailed in the Data Center access policy " *POL-SE-0001 - Physical Security Policy", in the procedures "PRO-SE-0001 - Operational Process for Physical Access to the Data Center" and "PRC-SE-0001 - Physical Access Procedure to the DC* ", in the latter case we detail below:

1. POL-SE-0001 - Physical Security Policy.

2. PRO-SE-0001 - Operational Process for Physical Access to the Data Center.

3. PRC-SE-0001 - Physical Access Procedure to the DC:
    - 3 .1. Data center access request
    - 3.2. Validate identification
    - 3.3. Completion of the term of access
    - 3.4. Verification of photo/image devices
    - 3.5. Registration in the access system (visitor)

Visitors: Visitor access to the Data Center must be carried out through an open call from the ITSM Tool and forwarded to the access and monitoring department, which is responsible for analyzing the request and releasing a badge with a pre-approved visitor profile to access the Ascenty dependencies. The visitor must always be accompanied by the employee or customer requesting access.

The process for granting access to service providers is detailed in the Data Center access policy *"POL-SE-0001 - Physical Security Policy", in the procedures "PRO-SE-0001 - Operational Process for Physical Access to the Data Center" and "PRC-SE-0001 - Physical Access Procedure to the DC"* , in the latter case we detail below:

1. POL-SE-0001 - Physical Security Policy.
2. PRO-SE-0001 - Operational Process for Physical Access to the Data Center.
3. PRC-SE-0001 - Physical Access Procedure to the DC:
    - 3.1. Data center access request
    - 3.2. Validate identification
    - 3.3. Completion of the term of access
    - 3.4. Verification of photo/image devices
    - 3.5. Registration in the access system (visitor)

Revocation of Access to the Data Center

Employee: For the employee access revocation process, the Human Resources department opens a ticket in the ITSM tool requesting the removal of access. The call is forwarded to Internal Support, which blocks the employee's logical access (systems, e-mail, telephone) and the access and monitoring department disables physical badge and biometric access. Employees are collected and monitored until they leave by a person in charge.

The access revocation process is detailed in the procedures "*PRO-SE-0001 - Operational Process for Physical Access to the Data Center", "PRC-RH-0003 - Disconnection Procedure ",* in the latter case we detail below:

1. PRC-RH-0003 - Employee Termination:
    - 1.1. Request to block access to IT systems
    - 1.2. Shutdown request (Physical access block)

two. PRO-SE-0001 - Operational Process for Physical Access to the Data Center:
    - 2.1. Access system lock
    - 2.2. badge collection

Renewal of access for employees, customers and providers (Review):

Access for customers and service providers can be revoked during the access review

process, which is carried out every six months or when requested by the person in charge (N5).

The access revocation process is detailed in the policy *"POL-SE-0001 - Physical Security Policy", in the procedure "PRC-SE-0002 - Access Review Procedure"*, in the latter case we discriminate in a macro way below:

1. POL-SE-0001 - Physical Security Policy.

2. PRC-SE-0002 - Access Review Procedure:
    - 2.1. Access review request
    - 2.2. Request access review (Customer/Provider)
    - 2.3. Access system validation and adjustment
    - 2.4. Updating lists published in the system

Visitors: Visitor access is revoked at the end of the period requested in the access request.

Periodic review of access to the Data Center

The periodic review of access to the Data Center is carried out in stages: employees, customers and service providers. Every quarter, all service provider accesses are listed, and the access and monitoring department performs access validation, validating whether they are accesses that should be maintained or not, as described in Service provider access renewal.

Data Center organization and signaling management

The management of the organization and signaling of the Data center is the responsibility of the Access and monitoring department, both for execution and for monitoring activities. All Data Center Systems are signposted with signs, informing the place you are visiting and the prohibitions for each System.

Physical Access Management Controls

Ascenty's controls must provide reasonable assurance that only authorized persons have access to the Data Center's restricted environments.

Controls	Associated Risk
GAF.1.1 – Access to all critical environments in the Data Center is controlled by a single access device with double identification (badge and biometrics).	Improper or unauthorized access to Data Center environments, compromising the safeguarding of allocated information and services.
GAF.1.2 – Access to all Data Center environments is granted by creating a ticket in the Service Now tool for all employees, service providers and customers. Access authorizations are recorded in the ticket itself, as well as the access period.	
GAF.1.3 – For every employee leaving the company, a ticket is created in the Service Now tool informing the termination and requesting the permanent blocking of access to the Data Center facilities.	
GAF.1.4 – Visitor access to the Data Center premises is only authorized upon creation and approval of a ticket in the Service Now tool and this ticket must be accompanied during the entire visit period.	
GAF.1.5 – Every six months, an employee access review process to the Data Center is carried out. This review is formalized in the Service Now tool, where all employees with active access are listed, and the person responsible for the Access and Monitoring area reviews and requests any necessary access adjustments.	
GAF.1.6 – Every three months, third-party access to the Data Center is reviewed. This review is formalized in the Service Now tool, where all third parties with active access are listed, and the person responsible for the Access and Monitoring area reviews and requests any necessary access adjustments.	

Facilities Management and Change Management.

Installation, Configuration and Maintenance of equipment

For the installation, removal, or maintenance of Data Center equipment / systems, it is necessary to open a ticket in the ITSM Tool and forward it to the responsible department, for installation / removal / maintenance. Changes made to Data Center equipment and systems used by Ascenty are classified as follows:

- Planned - Changes that need to be approved by the change committee and that are applied in the regular window (defined by Ascenty);
- Emergency - Changes that need to be approved by the change committee and that are applied in a special window (emergency) requested by the customer, even if the System is not stopped.
- Routine - Non-impact (pre-approved) changes that have already been approved

by the change committee at least three times.
- Critical - Changes that occur when customer service is down and need to be fixed, must have an associated incident.

It is important to highlight that Ascenty does not develop applications or *software* internally, as these are market packages.

The infrastructure department has documents to manage the distribution of equipment in the Data Center and other facilities in the building. Information can be obtained by company leadership online through the system. At the end of the year, the infrastructure department carries out an inventory of the Data Center equipment and documents it via the ITSM tool.

The infrastructure department is also responsible for preparing the maintenance schedule for the Data Center equipment. All maintenance is formalized through an open call in the ITSM tool.

The Data Center equipment installation, configuration and maintenance process is detailed in the procedure "*PRC-FL-0004 - Good Maintenance Practices - DC"*. This we discriminate in a macro way below:

1. PRC-FL-0004 - Good Maintenance Practices - DC:
    1.1. Consult maintenance schedule
    1.2. Verify change order approval
    1.3. Monitor the execution of maintenance

Energy demand management

The availability of energy for Ascenty's data centers is guaranteed through a contract established between the company and local energy suppliers.

The energy received by the supplier is distributed in 03 different BUSes at Ascenty, which are supported by generators and UPS devices. These are responsible for feeding the Data Center (racks) and each room serves as redundancy for each other.

The use of energy in the Data Center is monitored through the BMS tool. The tool also monitors the PUE (*Power Usage Effectiveness*) index. Information regarding power management is used to compose the report. Information can be obtained by company leadership online through the system.

Controls for optimizing operations such as alerts and monitoring

The infrastructure department uses the BMS tool to monitor temperature levels, air humidity, fire detection and prevention equipment. In case of alerts, the BMS tool automatically generates tickets in the ITSM tool for the infrastructure group, which verifies the incidents.

The Data Center also has security cameras that are monitored twenty-four hours a day and the images are stored for 90 days, as determined by ISO27001 and PCI-DSS. Additionally, the entire data cabling infrastructure is carried out in a structured manner.

Management of operations optimization controls, such as alerts and infrastructure monitoring for the critical system, is managed by the ITSM tool through the incident process being handled by the responsible team *"PRO-OP-0001 - Incident and Request Management".*

Security controls and disaster response

The Data Center has a formal process for evacuating the area and meeting points in case of disasters. The access and monitoring department monitors all changes to the building's structure and issues management reports to the company's leadership.

The process of managing security controls and fighting disasters is formalized in the procedures below:

PRC-ST-0016 (CH) Emergency and evacuation plan – Santiago;
PRC-ST-0016(BR) - Emergency Assistance Plan – Campinas;
PRC-ST-0017(BR) - Emergency Response Plan - Vinhedo DC;
PRC-ST-0018(BR) - Emergency Assistance Plan - Jundiaí 1;
PRC-ST-0019(BR) - Emergency Assistance Plan - Jundiaí 2;
PRC-ST-0020(BR) - Emergency Assistance Plan – Osasco;
PRC-ST-0021(BR) - Emergency Assistance Plan – Paulínia;
PRC-ST-0022(BR) - Emergency Assistance Plan – Fortaleza;
PRC-ST-0023(BR) - Emergency Assistance Plan – Sumaré;
PRC-ST-0024(BR) - Emergency Assistance Plan - Rio de Janeiro; and,
PRC-ST-0025(BR) - Emergency Response Plan – Hortolândia.

Supplier contract management

The Infrastructure department, together with the legal department, is responsible for managing contracts with Data Center suppliers. The contracts are maintained by the legal department and it is up to the Infrastructure department to control the execution of the services. The company carries out the control through the company's intranet (Sharepoint).

Depending on the type of service, the contract may contain SLA definitions (Service Level Agreement) for monitoring the activities performed. It is up to the Infrastructure department to monitor the ANSs and call the service provider in case of failures and/or delays in the contracted services.

The contracts comply with the contract policy *"POL-AS-0016 - Policy for contracts"* and the management of suppliers is verified by the process *"PRO-FN-0008 – Approval and Management of suppliers".*

Facility Management *Controls*

Ascenty's controls must provide reasonable assurance that only authorized persons have access to the Data Center's restricted environments.

Control Objective	Controls	Associated Risk
#1: The controls must provide reasonable assurance that the activities of a property management (Facilities) must be outsourced or contracted by suppliers.	GFA.1.1 – The Data Center environments have clear, objective and easily accessible rule/warning signals for everyone accessing the environment.	Unavailability of services due to an interruption due to lack of signaling and lack of organization and cleanliness of the Data Center.
#2: Controls must provide reasonable assurance that the different types of equipment in the data center have specific installation requirements and are properly managed in terms of installation, maintenance and retirement from the data center.	GFA.2.1 – For all installation of equipment for customers and facilities, a ticket is created in the Service Now tool with a description of what will be done, the period required and the person responsible for the activity.	Unavailability of services due to an interruption resulting from the incorrect installation of Data Center equipment.
	GFA.2.2 – Annually, a maintenance calendar is created for all equipment in the company's Data Center and maintenance is carried out and formalized in the Service Now tool on pre-established dates.	
	GFA.2.3 – For every uninstallation or removal of equipment from the Data Center, a ticket is created in the Service Now tool with a description of what will be done, the period required and the person responsible for the activity.	

	GFA.2.4 – An inventory process of all Data Center equipment is carried out annually. This process is carried out automatically and on-time by the Power BI tool.	
#3: Controls must provide reasonable assurance that power management requirements exist, equipment in the data center.	GFA.3.1 – The Data Center Technical control team issues a monthly energy consumption report to all the company's Directors in order to ensure that energy resources are being properly used and managed.	Unavailability of services due to an interruption due to lack of energy in the Data Center
	GFA.3.2 – Existence of a formal contract with an energy supplier that meets all the requirements needed by the company, such as preventive maintenance on the electrical networks and uninterrupted supply of electrical energy for the Data Center.	
	GFA.3.3 – The company has energy redundancy equipment in case of momentary interruption of the main service, such as: no- *breaks*, generators, and diesel supply system.	
#4: Controls must provide reasonable assurance that the Data Center is maintained at correct levels to optimize IT operations.	GFA.4.1 – The Data Center has sized cooling mechanisms in order to effectively control the temperature, humidity and air quality in the environment.	Unavailability of services due to an interruption resulting from the absence of minimum environmental controls.
	GFA.4.2 – The Data Center has fire detection mechanisms (smoke sensors) with early fire activation.	
	GFA.4.3 – The Data Center has mechanisms for monitoring security cameras 24x7, with automatic motion detection, in high definition, recording and storage of images.	

	GFA.4.4 – The Data Center has energy and data cabling infrastructure arranged in a segregated manner and any type of modification or maintenance to be carried out requires opening a ticket in the Service Now tool.	
#5 - Controls must provide reasonable assurance that safety standards are established.	GFA.5.1 – The company has formalized an evacuation plan in case of disasters and a team of trained brigade members for immediate evacuation of the building.	Possibility of risks to life in cases of natural disasters.
#6 Controls must provide reasonable security for receiving and delivering devices.	GFA.6.1 – The Data Center has a physical space adequately signaled for receiving materials. Access control to these facilities is controlled by opening a ticket in the Service Now tool.	Unavailability of services due to an interruption due to the absence of controls for receiving materials.
#7 - Controls must provide reasonable assurance that there is management over contracts with entities.	GFA.7.1 – All contracts with third party companies / Data Center service providers are properly managed so that the SLAs, maturities and agreed services are monitored, verifying that they are in accordance with the contract.	Unavailability of services due to an interruption in the supply or provision of services by suppliers.
#8: Controls must support data security practices and sensitive information.	GFA 8.1 – The Information Security Policy is reviewed and disclosed formally and annually to all Ascenty professionals.	Possibility of access by unauthorized persons and disclosure of confidential information
	GFA 8.2 – Tests for intrusion attempts to the Data Center and CCTV access control systems are periodically carried out by Ascenty's information security team.	
	GFA 8.3 – Ascenty professionals are periodically trained and guided on practices and obligations to adhere to the anti-corruption law.	

Ascenty
A Digital Realty and Brookfield Infrastructure JV

Change Management Controls

Controls to provide reasonable assurance that changes to the environment are approved, documented, and homologated prior to being transported to the system/equipment production environment.

Control Objective	Controls	Associated Risk
#1: Ascenty controls reasonable assurance that changes to the environment are approved, documented and homologated before being transported to the system/equipment production environment.	CC8.1.1 - Systemic and/or equipment changes are transported to the production environment through the appropriate approvals recorded in the ITSM tool.	Systemic unavailability due to undue changes migrated to the production environment.
	CC8.1.2 – Access to the scope systems' production servers is restricted to Ascenty professionals.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

IV. Description of the Objectives of Controls, Controls, Tests and Test Results

This section presents the following information provided by Ascenty:

- The control objectives specified by the company's management.
- The controls established and specified by Ascenty in order to meet the specified control objectives.

In addition, this section contains the following information provided by the independent auditor:

- Description of the procedures carried out by the auditor of the organization providing outsourced services with the intention of determining whether Ascenty's controls were designed and operated effectively to meet the control objectives in the period from January 1, 2022, to December 31, 2022. The auditor of the service provider organization ascertained the nature, timing and extent of the procedures carried out.
- The results of procedures performed by the auditor of the service organization.

PROCEDURES FOR ASSESSING THE INTEGRITY AND ACCURACY OF INFORMATION PRODUCED BY THE COMPANY (IPE)

For tests of controls that require the use of Company Produced Information (IPE), procedures have been performed to assess the reliability of the information, including the completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the review procedures. This includes Ascenty and IPE Produced Information used in carrying out our exam procedures.

Based on the nature of the EPIs, a combination of the following procedures was performed in relation to the integrity and accuracy of the data or reports used: (1) verify the documentation that gave rise to the EPIs, (2) verify the query, *script* or the parameters used to generate the EPIs, (3) compare the data between the EPIs and the source, and/or (4) check the EPIs to identify differences in sequences or periods.

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

4.1 Description of the objectives of controls, related controls and procedures performed

Process: Management of physical access to the Data Center.

Control Objective #1:
Ascenty's controls must provide reasonable assurance that only authorized persons have access to the Data Center's restricted environments.

Ascenty Control	Operation test carried out by EY
GAF.1.1 – Access to all critical environments in the Data Center is controlled by a single access device with double identification (badge and biometrics).	On a visit to the premises of the Data Centers of the scope, we observed whether the following items were operating properly, through: 1 - Existence of guardhouse with security professionals at the entrances of the condominiums; 2 - Existence of a concierge and access control for vehicles and people to Ascenty's facilities in all units audited, since visitors and service providers must have their name on the list, present their personal document, and then receive a badge provisional, previously cleared by the Facilities department; 3 - Access to the Data Center, technical rooms, docks, maintenance rooms, energy rooms, NOC and air conditioning and administrative areas are controlled using badges and biometrics.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GAF.1.2 – Access to all Data Center environments is granted by creating a *ticket,* in the Service Now tool, for all employees, service providers and customers. Access authorizations are recorded in the *ticket itself*, as well as the access period.	For each of the Data Centers in the scope, we carried out a sample selection of the accesses granted to the respective Data Centers during the scope period, and we verified that the supporting documentation included the following aspects: 1. If the *ticket was created* in the Service Now tool to grant access to the Data Center for the selected provider. 2. If the *ticket* created in the Service Now tool was created in a timely manner and that access to the Data Center only occurred after closing the *ticket.*
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GAF.1.3 – For every employee leaving the company, a *ticket is created in the Service Now* tool informing the termination and requesting the permanent blocking of access to the Data Center facilities.	For each of the Data Centers in the scope, we carried out a sample selection of employees who left during the scope period, and verified that the supporting documentation included the following aspects: 1. *Service Now* tool to revoke access to the Data Center for the terminated employee. 2. Check that the ticket created in the *Service Now tool* was created in a timely manner and that the access revocation occurred on the closing date of the ticket.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GAF.1.4 – Visitor access to the Data Center premises is only authorized upon creation and approval of a *ticket in the Service Now* tool and this ticket must be accompanied during the entire visit period.	Based on the accesses created by visitors to the premises of the Data Centers of the scope, during the audited period, we selected a sample and identified whether there were due approvals in the *Service Now tool* for granting access by the responsible employee, as well as recording the follow-up to these visitors during the visit to all Data Centers in the scope.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GAF.1.5 – Every six months, a review process is carried out regarding employee access to the Data Center. This review is formalized in the *Service Now* tool, where all employees with active access are listed and the person responsible for the Access and Monitoring area reviews and requests any necessary access adjustments.	Based on the semiannual execution of the employee access review control to the Data Centers of the scope, we verified that the active users with access to the Data Centers had their access duly evaluated by the person in charge of the Access and Monitoring area, based on the tickets of the records of the access to environments formalized in the *Service Now tool*.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GAF.1.6 – On a quarterly basis, a third-party access review process to the Data Center is carried out. This review is formalized in the *Service Now* tool, where all third parties with active access are listed, and the person responsible for the Access and Monitoring area reviews and requests any necessary access adjustments.	Based on the quarterly execution of the third-party access review control to the Data Centers of the scope, we verified whether the active third parties with access to the Data Centers had their access duly evaluated by the person in charge of the Access and Monitoring area, based on the *tickets* in the records of the access to environments formalized in the *Service Now tool*.
Test result	
No exceptions were identified.	

Process: *Facilities* Management.

Control Objective #1: Controls should provide reasonable assurance that facilities management activities *should* be outsourced or contracted to vendors.

Ascenty Control	Operation test carried out by EY
GFA.1.1 – Data *Center environments* have rules/warnings that are clear, objective and easily accessible to all environments.	On a visit to the premises of the Data Centers in the scope, we checked whether the supporting documentation covered the following aspects: 1. Signaling of the dock areas, including local rules and regulations (no smoking, carrying liquids and taking pictures); 2. Internal signage to indicate location of premises; 3. Signaling of emergency exits and demarcated areas for fire extinguishers; 4. Power equipment, *racks* and air conditioning have signage; 5. Risk Map of the Data Center area; and, 6. Meeting point for emergencies.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Control Objective #2: The controls must provide reasonable assurance that the different types of equipment in the data center have specific installation requirements and are properly managed in terms of installation, maintenance and withdrawal from the data center.

Ascenty Control	Operation test carried out by EY
GFA.2.1 – For all installation of equipment for customers and *facilities*, a *ticket is created in the Service Now* tool with a description of what will be done, the period required and the person responsible for the activity.	Based on the list containing all installations of customer equipment and *Facilities* in the Data Centers of the scope, during the audited period, we selected a random sample and checked whether a *ticket was created* in the Service Now tool with the description of what will be done, the necessary period and responsible for the activity.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA.2.2 – Annually, a maintenance schedule is created for all equipment in the company's Data Centers and maintenance is carried out and formalized in the *Service Now tool on* pre-established dates.	Based on the list containing the preventive maintenance carried out in the Data Centers of the scope, during the audited period, we randomly selected a sample and verified whether they were carried out according to the pre-established schedule and formalized in the *Service Now* tool.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GFA.2.3 – For every uninstallation or removal of equipment from the Data Center, a ticket is created in the *Service Now tool* with a description of what will be done, the period required and the person responsible for the activity.	Based on the list of uninstallation or removal of equipment from the Data Centers (clients and *facilities*) in the scope, during the audited period, we randomly selected a sample and checked if there was a *ticket opening in the Service Now* tool with the description of what was done, the period required and the person responsible for the activity.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA.2.4 – Annually, an inventory process is carried out for all equipment in the Data Center. This process is carried out automatically and *on-time by the Power BI* tool.	We verified whether the inventory of equipment in the Data Centers within the scope was carried out annually and whether it was carried out in an automated and *on-time manner using the Power BI* tool.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Control Objective #3: Controls must provide reasonable assurance that power management requirements exist, equipment in the data center.

Ascenty Control	Operation test carried out by EY
GFA.3.1 – Monthly, the Data Center Technical control team issues an energy consumption report to all the company's Directors in order to ensure that energy resources are being properly used and managed.	Based on the monthly execution of the energy consumption control of the Data Centers in the scope, we randomly selected two months, during the audited period, and verified whether the Data Center technical control team issued the energy consumption report for all the Directors of the Company.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA.3.2 – Existence of a formal contract with an energy supplier that meets all the requirements needed by the company, such as preventive maintenance on the electrical networks and uninterrupted supply of electrical energy for the Data Center.	We verify that each of the Data Centers has a contract signed with the concessionaires, which details the methods of supplying this energy, according to the needs of each Data Center, in addition to inspecting whether the contracts are within the contractual validity and whether the services offered by the company are according to Ascenty's needs. Additionally, we verified, through a technical visit to the Data Centers within the scope, whether the Ascenty units have their own facilities to support the energy supply provided by the local concessionaires.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GFA.3.3 – The company has energy redundancy equipment in case of momentary interruption of the main service, such as: no-*breaks*, generators and diesel supply system.	In a visit to the Data Centers of the scope, we verified whether each of these Data Centers has redundant power equipment (no- *break*), generators and diesel supply system.
Test result	
No exceptions were identified.	

Control Objective #4: Controls must provide reasonable assurance that the Data Center is maintained at correct levels to optimize IT operations.

Ascenty Control	Operation test carried out by EY
GFA.4.1 – The Data Center has sized cooling mechanisms in order to effectively control the temperature, humidity and air quality in the environment.	In a visit to the Data Centers within the scope, we checked whether each of these Data Centers has dimensioned refrigeration and humidity control equipment, as well as contingency equipment for all audited units.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA.4.2 – The Data Center has fire detection mechanisms (smoke sensors) with early fire activation.	In a visit to the Data Centers of the scope, we verified whether each of these Data Centers has equipment for fire detection, as well as procedures for monitoring this equipment.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GFA.4.3 – The Data Center has mechanisms for monitoring security cameras 24x7, with automatic motion detection, in high definition, recording and storage of images.	On a visit to the Data Centers within the scope, we verified whether each of these Data Centers has CCTV in the main facilities of the buildings and whether the images captured by this equipment are monitored 24x7 by security professionals.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA.4.4 – The Data Center has energy and data cabling infrastructure arranged in a segregated manner and any type of modification or maintenance to be carried out requires opening a *ticket in the Service Now* tool.	In a visit to the Data Centers of the scope, we verified whether each of these Data Centers has power and data cabling arranged in a segregated manner. Note: There was no modification or maintenance of power and data cabling during the audited period.
Test result	
No exceptions were identified.	

Control Objective #5: Controls must provide reasonable assurance that safety standards are established.

Ascenty Control	Operation test carried out by EY
GFA.5.1 – The company has formalized an evacuation plan in case of disasters and a team of trained brigade members for immediate evacuation of the building.	We verified that all Data Centers in the scope have a formalized evacuation plan in case of disasters and a team of trained brigade members for immediate evacuation of the building.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Control Objective #6: Controls must provide reasonable security for receiving and delivering devices.

Ascenty Control	Operation test carried out by EY
GFA.6.1 – The Data Center has a physical space adequately signaled for receiving materials. Access control to these facilities is controlled by opening a *ticket in the Service Now* tool.	In a visit to the Data Centers of the scope, we checked whether each of these Data Centers has a properly signaled physical space for receiving materials (docks). Additionally, we verify that access to these facilities is properly controlled by opening a *ticket in the Service Now* tool.
Test result	
No exceptions were identified.	

Control Objective #7: Controls must provide reasonable assurance that there is management over contracts with entities.

Ascenty Control	Operation test carried out by EY
GFA.7.1 – All contracts with third-party companies / Data Center service providers are properly managed so that the SLAs, maturities and agreed services are monitored, verifying whether they are in accordance with the contract.	Based on the list of contracts with third-party companies / service providers of the Data Centers in the scope, in force during the audited period, we verify, through inspection, if all contracts are properly managed so that the SLAs, maturities and agreed services are monitored and if they are in accordance with the contract.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Control Objective #8: Controls must support data security practices and sensitive information.

Ascenty Control	Operation test carried out by EY
GFA 8.1 – The Information Security Policy is reviewed and disclosed formally and annually to all Ascenty professionals.	We verify that the Information Security Policy is disclosed and shared with all Ascenty employees and that it is duly reviewed and updated. Additionally, based on the list of active employees at Ascenty, we carried out a random sample of 25 employees and obtained documentation that proves that they have completed Information Security training.
Test result	
No exceptions were identified.	

Ascenty Control	Operation test carried out by EY
GFA 8.2 – Tests for intrusion attempts to the Data Center and CCTV access control systems are periodically performed by Ascenty's information security team.	Based on the tests regarding intrusion attempts to access control systems to the Data Centers and CCTV, we observed whether the following items were included: 1. *scan* of systemic vulnerabilities, which cover both the CCTV systems and the access management system; It is, 2. Simulation of physical intrusion in order to validate the response of the Asset Security team, carried out annually.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
GFA 8.3 – Ascenty professionals are periodically trained and guided on practices and obligations to adhere to the anti-corruption law.	Based on the list of active employees at Ascenty, we selected a random sample of 25 employees and checked whether the supporting documentation proving the completion and approval of the annual anti-corruption training is due.
Test result	
No exceptions were identified.	

Process: Change Management.

Control Objective #1: Ascenty's controls must provide reasonable assurance that changes to the environment are approved, documented, and homologated before being transported to the system/equipment production environment.

Ascenty Control	Operation test carried out by EY
CC8.1.1 - Systemic and/or equipment changes are transported to the production environment through the appropriate approvals recorded in the ITSM tool.	Based on the list of systemic / equipment changes that occurred during the scope of the work, we selected a random sample and checked whether: 1. The changes were recorded in the ITSM tool. 2. There is a Change Committee activated in all customization requests, and its approval is mandatory prior to development (maintainer) and application in a production environment, in addition to being documented via meeting minutes. 3. Ascenty does not develop applications and software internally.
Test result	
No exceptions were identified.	

Building a better working world

Praia de Botafogo, n º 370, 8º andar,
Botafogo, Rio de Janeiro - RJ, Brasil
Tel:+ 55 (21) 3263-7000
www.ey.com.br

Ascenty Control	Operation test carried out by EY
CC8.1.2 - Access to the scope systems' production servers is restricted to Ascenty professionals.	We obtained the professionals who have access to the production servers of the scope systems and verified that access was restricted to the appropriate professionals, in addition to validating that there are no professionals from the supplier companies with access to the servers in question.
Test result	
No exceptions were identified.	

V. Other information provided by Ascenty

Ascenty's expansion goal in its strategic plan is the replication of internal controls related to physical access and Infrastructure management processes for the new Data Centers.

Components that support the provided service:

It follows the organizational structure of Ascenty Data Centers e Telecomunicações S/A.

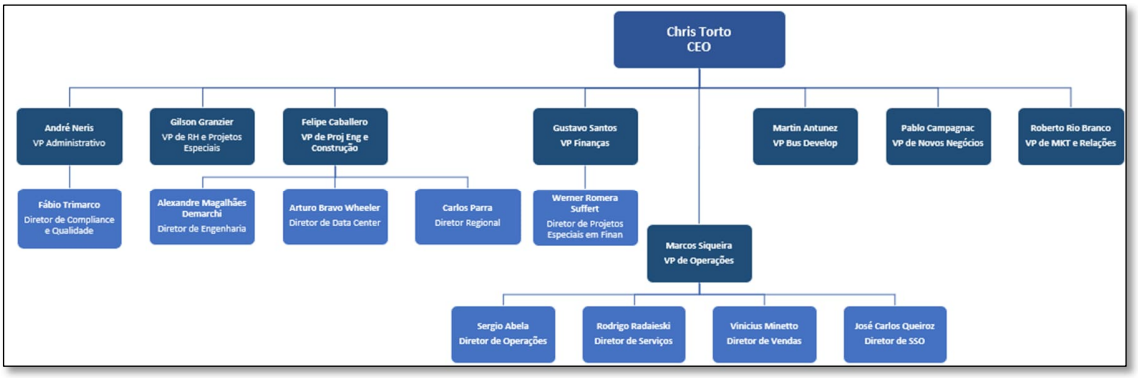

Figure 1: Ascenty's Organizational Structure

President Chris Torto (CEO): US citizen with permanent residence in Brazil since 1989. Co-founder and CEO of Vivax, the second largest cable TV operator in Brazil. In 2006, he led the IPO of Vivax, which was later acquired by NET Serviços in 2007. He was also head of Voyager Inc., from which he led the IPO in 1999 (the company was acquired by a telecommunications group in the north American in 2000). Chris holds a Business Administration degree from the University of Maine and an MBA from Harvard University.

Main functions: Ensuring that the company has the right strategy and the necessary resources to execute it. Identify the most promising markets, improve the organization and processes, focusing on long-term issues.

Vice President (VP) and Directors:

André Neris (Administrative VP) – Has extensive experience in Controllership, Business Administration and Finance, with a career that started at the Big Four Firm, working in Multinational Companies and experience in Brazilian Public Companies. Experience covers the areas of Controllership, Accounting, Auditing, Financial and Strategic Planning, Tax, Budgeting, Treasury, Cash Flow, Internal Controls, IT, HR, Legal, Administrative and Logistics. Analysis and conversion of financial and managerial statements in USGAAP, BRGAAP and IFRS. Planned processes and Internal Controls and SOX compliance.

Gustavo Henrique Santos de Sousa (VP of Finance) - held executive positions in large Brazilian companies, having held the positions of CEO and CFO/DRI at Cielo, CFO/DRI at Klabin, CEO and CFO/DRI at CPFL Renováveis, Controllership Director, Treasury, Investor Relations and Tax at Companhia Siderúrgica Nacional and Controlling Director at Banco do Brasil. He holds an MBA from Columbia Business School, a Masters in Economic Business Management from the University of Brasília, an MBA in Financial Administration from Fundação Getúlio Vargas and a degree in Business Administration from the Federal University of Rio Grande do Norte. At Ascenty, he works as CFO.

Pablo Campagnac (VP New Business) - Has extensive experience in sales and operations management. In the last fifteen years, he participated in the Vivax startup, where he took over the sales and operations directorates. Pablo is an economist and holds an MBA from Boston University.

Gilson Granzier (VP of HR and Special Projects) - Has extensive experience in the financial area. For the last thirteen years, he has been in charge of finance at Vivax and Buscapé as CFO. Gilson is a business administrator at the Regional University Center of Espírito Santo do Pinhal and has a postgraduate degree in finance from the Methodist University of Piracicaba.

Roberto Rio Branco (VP of Marketing and Relations) - He has extensive experience in marketing, sales, and operations. He served as chief operating officer at Vivax for four years and previously as COO at TVA Pay TV. He also led several managerial positions at Mesbla, Bank of Boston and City Bank. Roberto is a business administrator from Moraes College Jr.

Felipe Caballero (VP of Engineering and Construction Project) - Active in the areas of electrical engineering and data networks since 1997, focusing on datacenters and other large works. Participated in the development of several datacenter projects from concept to implementation. He was responsible for operating the infrastructure of large datacenters, managing all operational and maintenance routines for highly critical systems. Felipe Caballero studied at the ORT university in Uruguay, his country of nationality.

Marcos Siqueira (VP of Operations) - With extensive experience in Data Center e Telecomunicações, he has led Operations, Products, Pre-Sales and Post-Sales teams for Latin America in companies such as Global Crossing / Level 3. At Ascenty, he leads the areas of Data Center and Telecom Services. He holds a degree in technology and an Executive MBA from INSPER.

Martin Antunez (VP Business Development) - Extensive experience in the technology/telecommunications industry and holds a degree in Electrical Engineering from the University of Illinois at Chicago. In addition, it has other certifications and industry recognition. Previously with Digital Realty, he participated in the design, build,

commissioning, operation, and sales process of over 200 MW of uninterruptible power supply (UPS) capacity in over 90 data center projects across the United States, Madrid and Mexico City. In these projects, he participated and accompanied the credential certifications such as: LEED Platinum & Gold, UPTIME TIER III and IV and ICREA IV. Additionally, as Vice President of Sales for HEIT Consulting, he led a team that designed and delivered VoIP and Security & Compliance solutions to the financial services industry. He was also a senior manager at several organizations at SBC Communications (prior to the AT&T merger), leading technical sales teams that provided complex WAN/LAN solutions to enterprise and Fortune 500 customers in Silicon Valley.

Alexandre Magalhães (Director of Engineering DC) – Highly qualified professional with experience in the areas of Electrical Engineering and Telecommunications Engineering with a degree in Electrical-Electronic/Electrical Engineering. Expertise in the implementation of major telecommunications projects and works, telecommunications infrastructure and electrical engineering. Expertise in the development of various telecommunications systems and electrical installations with emphasis on oil platforms, oil refineries, chemical and petrochemical industries, fertilizer plants, mining, steel, power generation, cellulose paper, pharmaceuticals, hospitals, airports, commercial facilities and or administrative and implementation of data centers. Registration and Certifications at CREA-SP as Electric Engineer/Electrical Technician, EM-Designer CAE Elétrica Prominp/Escola Politécnica POLI-USP, Indigo Vision Integrator Certification for analog and IP CCTV systems, professional training in structured cabling FCP Furukawa -Designer and Installer, professional training in structured cabling ACT- $_1$ AMP/Tyco Eletronics-Designer, Basic SCS Certificate BICSI Brasil.

Sergio Abela (Director of Operations) – He has extensive experience in Data Center infrastructure, managing infrastructure projects at Ascenty. He graduated as a civil engineer from the University of São Paulo.

José Carlos Marques Queiroz (Occupational Health and Safety Director) – He has extensive experience in occupational safety in an IT environment, with a degree from Unicamp University – (Campinas) in occupational safety engineering.

Rodrigo Radaieski (Services Director) – He has extensive experience on the Internet and Data Center market in these segments since its inception in Brazil. With a solid career as a manager in IT areas with a focus on providing services. Graduated in informatics from the Catholic University of Rio Grande do Sul.

Arturo Wheeler (Regional Data Center Director) – Has extensive experience leading highly effective teams in mission-critical IT roles in globalized environments for Mexico and Latin America. He developed his career mainly in the financial sector with work at Citibank, where he was responsible for several areas of operation and engineering of Telecommunications and Data Centers. The executive was also part of the Americas regional leadership teams for the bank, where he was responsible for establishing

operating models and transitions of local, regional and global teams through which operational efficiencies, service improvements and cost reductions were achieved.

Carlos Parra (Regional Director) – He has extensive experience in electrical engineering with more than 20 years of experience in the infrastructure and technology industry. He began his career at the Colombian Association of Engineers, a technical advisory body to the National Government. Worked with the Inter-American Development Bank IDB to strengthen the engineering production chain. He worked for several years at the Colombian Ministry of Information and Communications Technology in one of its technological inclusion programs. He participated in different technological innovation projects with the State, alternative banks (Fintech) and private companies.

Werner Romera Suffert (Director of Special Projects in Finance) - He has extensive experience in large Brazilian companies listed on B3 in the Novo Mercado, occupying executive positions, board of directors, audit committee and fiscal council. He was CEO and CFO/DRI of security BB, CFO/DRI of IRB Brasil RE, executive in several boards of Banco do Brasil. He was a member of the board of directors of security BB, IRB Brasil RE, Brasilprev and Brasildental. He also held a position on the Audit Committee of IRB Brasil RE and Fiscal Council at Brasildental. He was chairman of the financial committee of Brasilprev, Brasilcap and Brasilseg. He was also General Manager of BB Paris. He holds a master's in business administration from COPPEAD/UFRG, an MBA in International Business from FIPE/USP and a degree in Administration from the University of Brasília - UNB.

Vinicius Camiloti Minetto (Sales Director) - Has extensive experience in the Data Center and Telecommunications market, where he has been operating for over 15 years. He worked for major players in the domestic market and joined Ascenty in 2012, reinforcing the commercial team. Graduated and Graduated from FATEC and with an MBA in Commercial Management from Fundação Getúlio Vargas (FGV). At Ascenty, he is responsible for the Commercial, Solutions and Product Architecture team.

Main functions: Lead the preparation and implementation of strategic and operational plans, in all areas of the company, aiming to ensure its development, growth and continuity. Identify opportunities, assess feasibility and make recommendations on new investments or new business development, with a view to ensuring an adequate return for shareholders, safeguarding the security of the company's assets and ensuring that the actions taken do not cause significant impacts on the System environment. Maintain contacts with the management of client companies to identify opportunities for expanding or improving the products / services provided or solving any contractual or operational problems, aiming to maintain customer satisfaction and project a positive image of the company in the market. Lead the processes of changes in the organization's culture, aiming to gain the engagement of all its members and ensure the consolidation of an organizational culture oriented towards the continuous pursuit of quality and high standards of individual and collective performance.

Ascenty's Vice Presidents and Directors are fully committed to the code of conduct, encouraging an ethical and transparent System, demanding compliance with rules and laws.

Compliance and Quality

Fabio Trimarco (Compliance and Quality Director) - Has extensive experience in IT, passed through the areas of development, planning and operation, with the last 10 years focusing on corporate IT governance, Bachelor of Science in Computer Science and MBA in IT Governance from the University of Education of São Caetano do Sul and extension of the graduation in Corporate Compliance by PUC. Currently responsible for Ascenty's Compliance and Quality department, focusing on ethics, conduct and quality based on the implementation and management of standards and certifications such as ISOs 9001 quality management, 14001 environmental management, 20000-1 IT services management, 27001\ 27701 information security management\data privacy management, 37001\37301 anti-bribery management\compliance management, 45001 occupational health and safety management, 50001 energy management, PCI DSS, SOC, UPTIME TIER III and TÜV TR3 (TIA942) .

Main functions: The Compliance Function was established with authority and independence within the organization with free access to executives and shareholders for the performance of its function. It is the representative area that manages the management systems and other certifications implemented in the company, ensuring that:

- The objectives are aligned with reality;
- Performance and opportunities for improvement are reported to senior management;
- Develop and maintain standardized service delivery processes in line with best practice recommendations from ITIL, CobiT and PMI in line with offerings;
- Check the efficiency and effectiveness of the use of processes in the departments;
- Provide training and continuous improvement of processes for the entire company;
- Notify and guide the correct operation when the deviation from the written process is verified;
- Manage the continuous process improvement program;
- Manage internal audits to ensure adherence to certified processes;
- Identify and propose new service management tools, when applicable; It is,
- Keep processes aligned with certifications.