



# Ascenty Data Centers e Telecomunicações S/A

Relatório de Asseguração Razoável  
dos Auditores Independentes -  
SOC 3, para os princípios de  
Segurança e Confidencialidade

SOC 3

Período de 1º de janeiro a 31 de dezembro de 2024



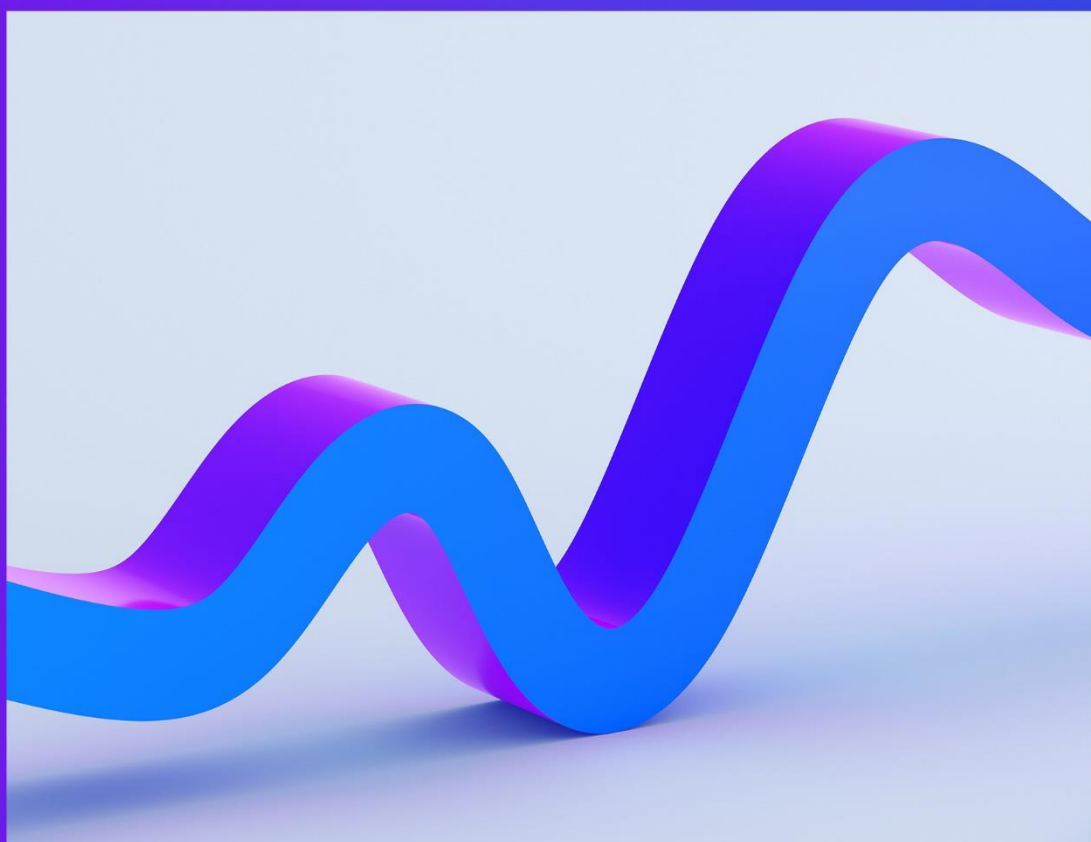


# Índice

Seção I .....	3
Seção II .....	8
Seção III .....	12

# Seção I

## Relatório de Asseguração dos Auditores Independentes





KPMG Assurance Services Ltda.  
Rua Verbo Divino, 1400, Conjunto Térreo ao 801 - Parte,  
Chácara Santo Antônio, CEP 04719-911, São Paulo - SP  
Caixa Postal 79518 - CEP 04707-970 - São Paulo - SP - Brasil  
Telefone +55 (11) 3940-1500  
kpmg.com.br

Aos  
Diretores e Acionistas da  
Ascenty Data Centers e Telecomunicações S/A  
Vinhedo - SP

### Escopo

Fomos contratados para emitir um relatório sobre a descrição elaborada pela organização prestadora de serviços Ascenty Data Centers e Telecomunicações S/A (“Ascenty” ou “Empresa”) sobre os controles de acesso físico, manutenção e operação de Data Centers (*Facilities*) relacionados aos critérios de serviço de Segurança e Confidencialidade operacionalizados pela Ascenty entre 1º de janeiro e 31 de dezembro de 2024 (“Descrição”), com base nos critérios descritos e na adequação do desenho e efetividade operacional dos controles especificados na descrição, para fornecer asseguarção razoável de que os controles da Ascenty, com base nos critérios de serviço de confiança (“Critérios de Serviço”) estabelecidos na Seção 100 do TSP, *2017 Trust Services Criteria for Security (AICPA, Trust Services Criteria)* estavam desenhados e operando com efetividade.

Essa descrição considera que certos controles relacionados aos Critérios de Serviço somente poderão ser alcançados se os controles complementares das organizações usuárias, previstos no desenho de controles da organização prestadora de serviços, estejam devidamente desenhados e operando de forma efetiva, juntamente com os controles relacionados da Ascenty. Não avaliamos a adequação do desenho nem a efetividade operacional dos controles complementares das organizações usuárias.

### Responsabilidades da organização prestadora de serviços

A Ascenty é responsável por seus controles relacionados aos Critérios de Serviço e por desenhar e implementar controles que sustentam os Data Centers da Ascenty, para fornecer asseguarção razoável de que os Critérios de Serviço da Ascenty foram alcançados. A organização prestadora de serviço Ascenty nos forneceu a “Descrição fornecida pela Organização Prestadora de Serviços”, Seção III, contendo a descrição dos controles para atender aos critérios e confirmando que eles foram desenhados, descritos e que estão funcionando efetivamente.



A Ascenty é responsável por elaborar a Descrição e a Afirmação correspondente (Seção II e III), incluindo (i) a integridade, exatidão e método de apresentação da descrição e da declaração; (ii) a prestação dos serviços incluídos na descrição; (iii) a especificação dos controles para cumprir os Princípios de Serviço de Confiança (TSP); e (iv) a identificação dos riscos que ameaçam o cumprimento dos compromissos de serviço e requisitos do sistema da organização prestadora de serviços.

### **Nossa independência e controle de qualidade**

Cumprimos a independência e outros requisitos éticos do Código de Ética para Contadores Profissionais da emitidos pelo *International Ethics Standards Board for Accountants*, que se baseia em princípios fundamentais de integridade, objetividade, competência profissional e devido zelo, confidencialidade e comportamento profissional.

A firma aplica a Norma Internacional de Controle de Qualidade e, dessa forma, mantém um sistema abrangente de controle de qualidade, incluindo políticas e procedimentos documentados relativos ao cumprimento de requisitos éticos, normas profissionais e requisitos legais e regulamentares aplicáveis.

### **Responsabilidades do auditor de serviço**

Nossa responsabilidade é a de expressar um parecer sobre o desenho e a efetividade operacional dos controles relacionados aos critérios especificados nesta descrição, elaborados pela organização prestadora de serviços Ascenty, com base nos nossos procedimentos. Realizamos os nossos trabalhos de acordo com a Norma Brasileira NBC TO Nº 3000 – Trabalho de Asseguração Diferente de Auditoria e Revisão, emitida pelo Conselho Federal de Contabilidade, e sua equivalente internacional *ISAE Nº 3000 - Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, emitida pelo *International Auditing and Assurance Standards Board (IAASB)*. Essas Normas requerem que planejem e realizemos nossos procedimentos para obter asseguração razoável sobre se, em todos os aspectos relevantes, a descrição é apresentada de acordo com os critérios de descrição e se os controles nelas declarados foram adequadamente desenhados e estão funcionando de maneira efetiva.

Uma asseguração razoável da descrição do sistema de uma organização prestadora de serviços e da adequação do desenho e da efetividade operacional dos controles envolve o seguinte:

- Obter um entendimento do sistema e dos compromissos de serviço e requisitos de sistemas da organização prestadora de serviços;
- Avaliar os riscos de que a descrição não seja apresentada de acordo com os critérios de descrição e que os controles não tenham sido desenhados adequadamente ou não funcionem de uma maneira eficaz;
- Executar procedimentos para obter evidências sobre se a descrição é apresentada de acordo com os critérios de descrição;



- Executar procedimentos para obter evidências sobre se os controles declarados na descrição foram desenhados adequadamente para fornecer asseguração razoável de que a organização prestadora de serviços alcançaria seus compromissos de serviço e requisitos de sistemas com base nos critérios de serviços de confiança aplicáveis caso esses controles funcionassem de maneira eficaz;
- Testar a efetividade operacional dos controles indicados na descrição para fornecer asseguração razoável de que a organização prestadora de serviços atingiu seus compromissos de serviço e requisitos de sistemas com base nos critérios de serviços de confiança aplicáveis;
- Avaliar a apresentação geral da descrição.

Nosso trabalho de asseguração razoável também incluiu a realização desses outros procedimentos conforme consideramos necessários nas circunstâncias.

### **Limitações inerentes**

A descrição é preparada para atender às necessidades comuns de uma ampla gama de usuários deste relatório e não pode, portanto, incluir todos os aspectos de controles que cada usuário dos relatórios individuais pode considerar importante para atender às suas necessidades de informações.

Existem limitações inerentes a efetividade de qualquer sistema de controle interno, incluindo a possibilidade de erro humano e a anulação de controles.

Em função da sua natureza, os controles podem nem sempre funcionar de maneira eficaz para fornecer asseguração razoável de que os compromissos de serviço da organização prestadora de serviços e os requisitos do sistema são alcançados com base nos critérios de serviços de confiança aplicáveis. Da mesma forma, a projeção em relação ao futuro de quaisquer conclusões sobre a adequação do projeto e da eficácia operacional está sujeita ao risco de que os controles podem se tornar inadequados em função das mudanças nas condições, ou que o nível de conformidade com as políticas ou procedimentos pode se deteriorar.

### **Opinião**

Em nossa opinião, em todos os aspectos relevantes:

- (a) A descrição apresenta adequadamente os controles da Ascenty relacionados aos Critérios de Serviço de Segurança e Confidencialidade, conforme desenhados e implementados durante o período de 1º de janeiro a 31 de dezembro de 2024;
- (b) O desenho dos controles relacionados com os Critérios de Serviço de Segurança e Confidencialidade, especificados na descrição, foi adequado durante o período de 1º de janeiro a 31 de dezembro de 2024;



- (c) Os controles testados, necessários para fornecer segurança razoável de que os Critérios de Serviço de Segurança e Confidencialidade especificados na descrição foram alcançados, operaram efetivamente durante o período de 1º de janeiro a 31 de dezembro de 2024.

São Paulo, 27 de janeiro de 2025

KPMG Assurance Services Ltda.  
CRC 2SP023228/O-4

Danilo Sandroni Carra  
Contador CRC 1SP353622/O-4

KPMG Assurance Services Ltda., uma sociedade simples brasileira, de responsabilidade limitada e firma-membro da organização global KPMG de firmas-membro independentes licenciadas da KPMG International Limited, uma empresa inglesa privada, de responsabilidade limitada

KPMG Assurance Services Ltda., a Brazilian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Este documento foi assinado eletronicamente por Danilo Sandroni Carra.

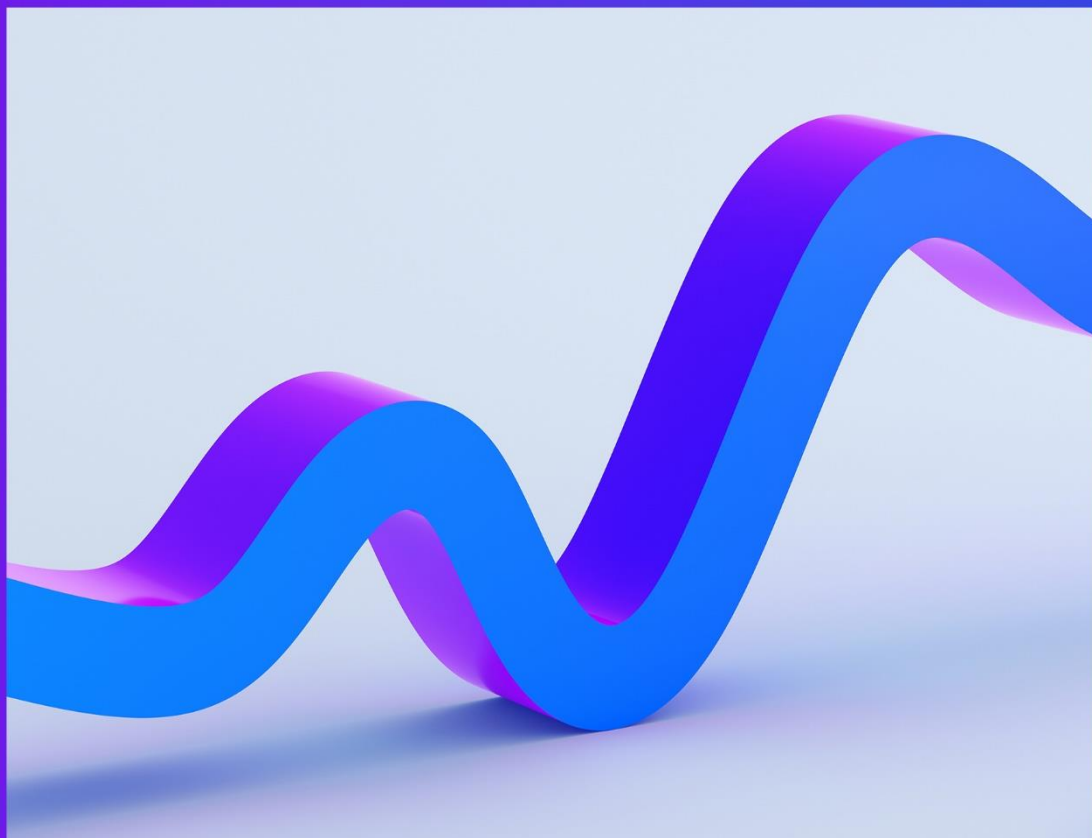
Para verificar as assinaturas vá ao site <https://apiconfirmations.kpmg.com.br> e utilize o código 3DD5-B3FE-FD90-76B7.

Este documento foi assinado eletronicamente por Danilo Sandroni Carra.  
Para verificar as assinaturas vá ao site <https://apiconfirmations.kpmg.com.br> e utilize o código 3DD5-B3FE-FD90-76B7.



# Seção II

Afirmação da Organização  
Prestadora de Serviços





### **Afirmação da Organização Prestadora de Serviços Ascenty**

A descrição foi elaborada pela Ascenty às organizações usuárias que utilizaram os controles relacionados aos princípios de Segurança e Confidencialidade entre 1º de janeiro a 31 de dezembro de 2024 ("descrição"), com base nos critérios descritos no DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), ("description criteria"). A descrição tem como objetivo fornecer aos usuários do relatório informações sobre os controles relacionados aos processos de prestação de serviços que podem ser úteis ao avaliar os riscos decorrentes, a adequação do desenho dos controles na descrição e a efetividade operacional desses controles, para fornecer segurança razoável de que os serviços da Ascenty seriam alcançados com base nos critérios, se operados de forma efetiva, relevantes para Segurança e Confidencialidade ("critérios de serviços aplicáveis") estabelecidos na seção 100 do Trust Service Principles (TSP).

Essa descrição considera que determinados controles nela especificados somente poderão ser alcançados se os controles complementares das organizações usuárias, previstos no desenho dos controles da organização prestadora de serviços, estejam devidamente desenhados e operando de forma efetiva, juntamente com os controles relacionados na descrição da Ascenty para atingimento do Trust Service Principles (TSP). Não avaliamos a adequação do desenho, nem a efetividade operacional dos controles complementares das organizações usuárias.

A Ascenty confirma que:

- a) a descrição na Seção III apresenta adequadamente os controles relacionados aos princípios de Segurança e Confidencialidade durante o período entre 1º de janeiro a 31 de dezembro de 2024 com base nos critérios estabelecidos;
- b) o desenho e a efetividade operacional dos controles relacionados com os critérios especificados na descrição foi adequado período entre 1º de janeiro a 31 de dezembro de 2024, e, consideraram que, as organizações usuária tenham aplicado seus controles complementares, previstos no desenho de controles da Ascenty, entre 1º de janeiro a 31 de dezembro de 2024.

Os critérios utilizados para elaboração dessa afirmação foram que a descrição:

- apresenta como os controles de acesso físico, manutenção e operação de Data Centers (Facilities) relacionados aos processos de prestação de serviços foram desenhados, implementados, e operados efetivamente incluindo:
  - os tipos de serviços prestados;
  - os procedimentos por meio dos quais os serviços são prestados;
  - os critérios e os controles desenhados para alcançar esses objetivos;
  - os controles que, no desenho dos controles relacionados aos processos de prestação de serviços, seriam implementados pelas organizações usuárias e que, se necessário para alcançar os objetivos de controle especificados na descrição, são identificados na descrição juntamente com os objetivos de controle específicos que não podem ser alcançados individualmente;
  - outros aspectos do ambiente de controle, do processo de avaliação de riscos, do sistema de informações (incluindo os respectivos processos de negócio) e da comunicação, das atividades de controle e dos controles de monitoramento que foram relevantes para os serviços prestados;
- inclui detalhes relevantes de mudanças nos controles relacionados aos princípios de Segurança e Confidencialidade da organização prestadora de serviços Ascenty entre 1º de janeiro a 31 de dezembro de 2024;
- não omite ou distorce informações relevantes para o escopo dos controles relacionados aos princípios de Segurança e Confidencialidade que estão sendo descritos, apesar de saber que a descrição foi elaborada para atender as necessidades das organizações usuárias e, portanto, pode não incluir todos os aspectos que possam considerar importante em seu próprio ambiente específico.

Os controles relacionados com os critérios especificados na descrição foram adequadamente desenhados e operaram efetivamente entre 1º de janeiro a 31 de dezembro de 2024. Os critérios usados na elaboração dessa afirmação foram que:

- os riscos que ameaçaram o escopo dos critérios especificados na descrição foram identificados;

- os controles identificados forneceriam, se estivessem operando conforme descrito, segurança razoável de que esses riscos não impediriam que os objetivos de controle especificados fossem alcançados; e
- os controles foram aplicados de maneira uniforme conforme desenhados, incluindo que foram aplicados controles manuais por pessoas com competência e autoridade adequadas.

DocuSigned by:



461CD50EE4D1424

Fabio Trimarco

Diretor de Compliance e Qualidade

Ascenty Data Centers e Telecomunicações S/A

Assinado por:



9842EF54AA824BD

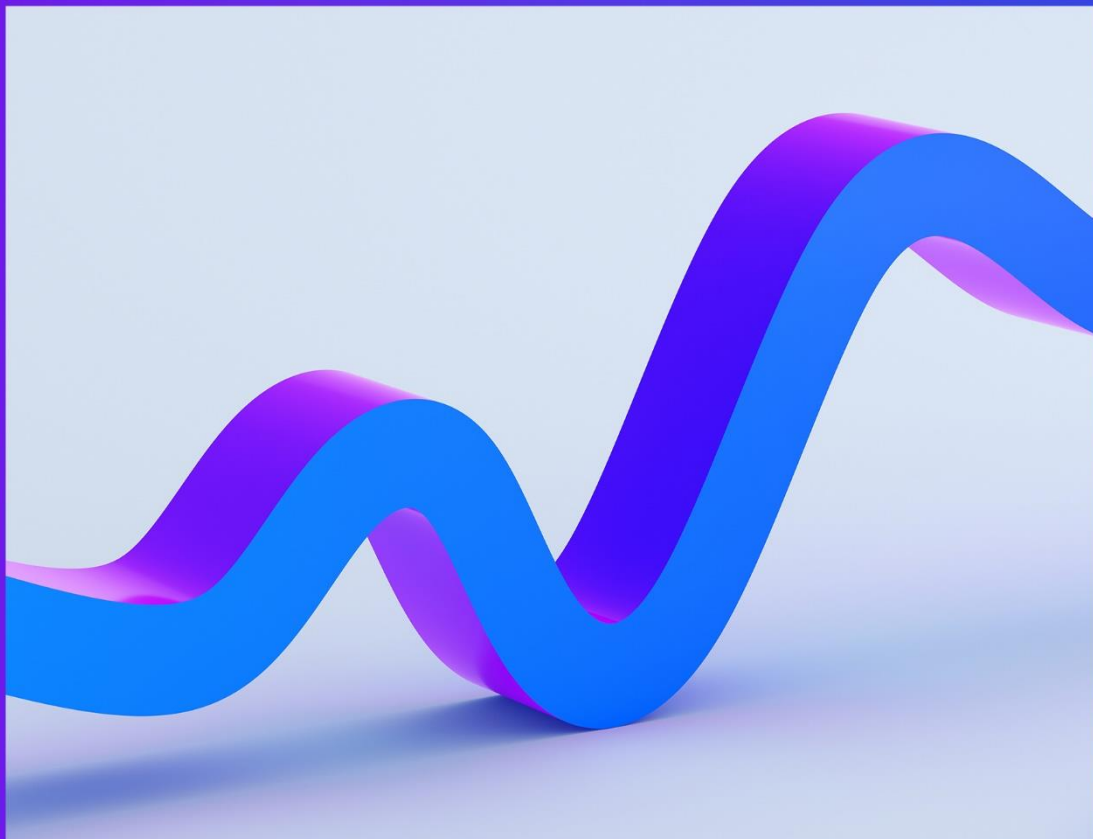
Marcos Siqueira

VP de Operações

Ascenty Data Centers e Telecomunicações S/A

# Seção III

Descrição elaborada pela  
Organização Prestadora de  
Serviços Ascenty



Este documento foi assinado eletronicamente por Danilo Sandroni Carra.  
Para verificar as assinaturas vá ao site <https://apiconfirmations.kpmg.com.br> e utilize o código 3DD5-B3FE-FD90-76B7.



A Digital Realty and Brookfield Infrastructure JV

## Sobre a Ascenty

A Ascenty oferece a seus clientes uma combinação de redes de fibras ópticas e serviços de Data Centers próprios. Os serviços de conectividade para atendimento a operadoras via redes de fibra óptica tiveram início no segundo semestre de 2011, na região do ABC paulista. Em fevereiro de 2012 foi adquirida a empresa Ascenty, baseada em São Paulo, com foco em serviços de Colocation e Conectividade. A partir daí o nome Ascenty foi adotado.

Os Data Centers estão distribuídos do seguinte modo:

1. Na cidade de Campinas/SP (CPS1), inaugurado em outubro de 2012;
2. Na cidade de Jundiaí/SP (JDI1), inaugurado em agosto de 2014;
3. Na região de Maracanaú/CE (FTZ1), inaugurado em junho de 2015;
4. Na cidade de Hortolândia/SP (HTL1), inaugurado em dezembro de 2015;
5. Na cidade de Osasco/SP (SP1), inaugurado em março de 2017;
6. Na cidade de Osasco/SP (SP2), inaugurado em maio de 2017;
7. Na cidade de Sumaré/SP (SUM1), inaugurado em julho de 2017;
8. Na cidade do Rio de Janeiro/RJ (RJ1), inaugurado em novembro de 2017;
9. Na cidade de Paulínia/SP (PLN1), inaugurado em maio de 2019;
10. Na cidade de Jundiaí/SP (JDI2), inaugurado em agosto de 2019;
11. Na cidade de Hortolândia/SP (HTL2), inaugurado em agosto de 2019;
12. Na cidade de Hortolândia/SP (HTL3), inaugurado em agosto de 2019;
13. Na cidade de Sumaré/SP (SUM2), inaugurado em setembro de 2019;
14. Na cidade de Vinhedo/SP (VIN1), inaugurado em novembro de 2019;
15. Na cidade de Osasco/SP (SP3), inaugurado em julho de 2020;
16. Na cidade de Vinhedo/SP (VIN2), inaugurado em outubro de 2020;
17. Na região Metropolitana de Santiago/Chile (SCL1), inaugurado em novembro de 2020;
18. Na cidade de Hortolândia/SP (HTL4), inaugurado em dezembro de 2021; e,
19. Na cidade do Rio de Janeiro/RJ (RJ2), inaugurado em fevereiro de 2022;
20. Na região Metropolitana de Santiago/Chile (SCL2), inaugurado em julho de 2022;
21. Na cidade de Querétaro/México (QRO1), inaugurado em junho de 2022;
22. Na cidade de Querétaro/México (QRO2), inaugurado em junho de 2022;
23. Na cidade de Hortolândia/SP (HTL5), inaugurado em setembro de 2022; e
24. Na cidade de Osasco/SP (SP4), inaugurado em junho de 2023.

## Compromisso e requisitos junto aos clientes

A estratégia da Ascenty está direcionada para operar Data Centers com redes de fibra óptica próprias para promover serviços de Colocation e Conectividade de alta capacidade, estando focada no atendimento a clientes nacionais e internacionais, sempre respeitando a legislação vigente no País.

## Escopo do Relatório

O escopo deste relatório contempla os processos de acesso físico e infraestrutura, os quais a Ascenty determinou como significantes para seus clientes na perspectiva das demonstrações financeiras. São eles:

- Gerenciamento de Acesso Físico – Os controles da Ascenty devem prover segurança razoável de que apenas pessoas autorizadas possuem acesso aos ambientes restritos do Data Center.
- Gerenciamento de Mudanças – Controles para prover segurança razoável de que as mudanças no ambiente são aprovadas, documentadas e homologadas antes de serem transportadas para o ambiente de produção do sistema /equipamentos.
- Gerenciamento de Facilities - Os controles da Ascenty devem prover segurança razoável de que apenas pessoas autorizadas possuem acesso aos ambientes restritos do Data Center.

Nota: Para os controles relacionados ao processo de Gerenciamento de Mudanças, nossas análises limitaram-se aos sistemas Elipse e BMS (Building Management System).

Apresentamos abaixo uma breve descrição dos processos de TI e os respectivos controles.

### Gerenciamento de Acesso Físico ao Data Center.

Todos os Data Centers da companhia estão localizados em locais estratégicos que possuem portaria 24x7 e que os acessos de funcionários, prestadores de serviço e clientes são controlados via crachá de acesso e biometria. Os acessos de visitantes, são liberados somente após realização de cadastro com apresentação de documentos originais e, em caso de veículos de carga, revista realizada pela equipe de segurança.

Os acessos a todas as salas críticas do Data Center são controlados por sistemas de dupla autenticação (crachá e biometria).

### Controle de Concessão de Acesso

Funcionários: O departamento de Recursos Humanos abre chamado para solicitação de acessos na ferramenta de ITSM e encaminha o chamado para o departamento de acesso e monitoramento, que analisa o cargo e o departamento do funcionário, efetua o cadastro no sistema de acesso e concede perfil de acessos pré-aprovados de acordo com o cargo/departamento constante com a matriz de acesso específica do data center.

O processo de concessão de acessos para funcionários está detalhado na política de acessos ao Data Center “POL-SE-0001 - Política de Segurança Física”, no procedimento “PRC-SE-0001 - Procedimento Acesso Físico ao DC”, neste último caso discriminamos os principais passos abaixo:

1. PRC-RH-0001 - Procedimento de recrutamento e seleção.
2. PRC-RH-0002 - Procedimento de contratação:
  - 2.1 Requisição de acesso aos sistemas do TI
  - 2.2 Requisição de acesso do novo funcionário (Liberação de acesso físico)
3. PRC-SE-0001 - Procedimento Acesso Físico ao DC:
  - 3.1 Cadastro no sistema de acesso de acordo com a Matriz de acesso
  - 3.2 Designação de crachá
  - 3.3 Cadastro de biometria
  - 3.4 Teste de acesso

**Clientes:** Durante a fase de projeto, é preenchido o formulário de acessos pré-autorizados, no qual o responsável pelo cliente define os colaboradores autorizados a acessar o Data Center. Todos os acessos devem ser previamente autorizados e registrados via ferramenta ITSM/Portal CSM/Painel Cliente. Cabe ao cliente a responsabilidade de solicitar as liberações para seus visitantes e prestadores de serviço, sendo responsabilidade da Ascenty realizar as verificações e proceder com a autorização de acesso.

Sempre que os técnicos do cliente precisarem acessar o Sistema do Data Center, a solicitação de acessos deve ser feita através de abertura de chamado na ferramenta de ITSM, que será enviado ao departamento de acesso e monitoramento. O departamento de acesso e monitoramento irá verificar o chamado e irá atribuir os acessos de acordo com os perfis pré-aprovados para o cliente.

O processo de concessão de acessos para cliente está detalhado na política de acessos ao Data Center “POL-SE-0001 - Política de Segurança Física”, no procedimento “PRC-SE-0001 - Procedimento Acesso Físico ao DC”, neste último caso discriminamos abaixo:

1. POL-SE-0001 - Política de Segurança Física.
2. PRC-SE-0001 - Procedimento Acesso Físico ao DC:
  - 2.1 Requisição com formulário de pré-autorização do cliente
  - 2.2 Cadastro no sistema de acesso de acordo com a Matriz de acesso
  - 2.3 Designação de crachá (conforme níveis de acesso)
  - 2.4 Cadastro de biometria
  - 2.5 Teste de acesso

**Prestadores de serviços:** A solicitação de acessos para prestadores de serviços deve ser realizada via ferramenta de ITSM. Os chamados devem conter o período de permanência do prestador de serviços no Data Center, quais os locais que o prestador precisa ter acesso e indicar o funcionário responsável pelo prestador de serviços. O departamento



de Acesso e monitoramento verifica a solicitação e atribui os perfis pré-aprovados para o prestador.

O processo de concessão de acessos para prestadores de serviços está detalhado na política de acessos ao Data Center “POL-SE-0001 - Política de Segurança Física”, no procedimento “PRC-SE-0001 - Procedimento Acesso Físico ao DC”, neste último caso discriminamos abaixo:

1. POL-SE-0001 - Política de Segurança Física.
2. PRC-SE-0001 - Procedimento Acesso Físico ao DC:
  - 2.1 Requisição de acesso ao data center
  - 2.2 Validar identificação
  - 2.3 Preenchimento do termo de acesso
  - 2.4 Verificação de dispositivos de foto/imagem
  - 2.5 Cadastro no sistema de acesso (visitante)

Visitantes: O acesso para visitantes ao Data Center deve ser realizado através de chamado aberto da Ferramenta de ITSM e encaminhado ao departamento de acesso e monitoramento, que é responsável por analisar a solicitação e liberar um crachá com perfil pré-aprovado de visitante para acesso as dependências da Ascenty. O visitante deve estar sempre acompanhado pelo funcionário ou cliente solicitante do acesso.

O processo de concessão de acessos para prestadores de serviços está detalhado na política de acessos ao Data Center “POL-SE-0001 - Política de Segurança Física”, no procedimento “PRC-SE-0001 - Procedimento Acesso Físico ao DC”, neste último caso discriminamos abaixo:

1. POL-SE-0001 - Política de Segurança Física.
2. PRC-SE-0001 - Procedimento Acesso Físico ao DC:
  - 2.1 Requisição de acesso ao data center
  - 2.2 Validar identificação
  - 2.3 Preenchimento do termo de acesso
  - 2.4 Verificação de dispositivos de foto/imagem
  - 2.5 Cadastro no sistema de acesso (visitante)

## Revogação de Acessos ao Data Center

Funcionário: Para o processo de revogação de acessos de funcionários o departamento de Recursos Humanos abre um chamado na ferramenta de ITSM solicitando a remoção dos acessos. O chamado é encaminhado para Suporte interno que bloqueia os acessos lógicos do funcionário (sistemas, e-mail, telefone) e o departamento de acessos e monitoramento desativa os acessos físicos de crachá e biometria. É realizado o recolhimento e acompanhamento do funcionário até a saída por um responsável.

O processo de revogação de acessos está detalhado nos procedimentos “POL-SE-0001 - Política de Segurança Física”, “PRC-RH-0003 - Procedimento de desligamento”, neste último caso discriminamos abaixo:

1. PRC-RH-0003 - Desligamento de funcionário:
  - 1.1 Requisição de bloqueio acesso aos sistemas do TI
  - 1.2 Requisição de desligamento (Bloqueio de acesso físico)
2. -“POL-SE-0001 - Política de Segurança Física”:
  - 2.1 Bloqueio no sistema de acesso
  - 2.2 Recolhimento do crachá

## **Renovação de acesso de funcionários, clientes e prestadores (Revisão):**

Os acessos de clientes e prestadores de serviços podem ser revogados durante o processo de revisão de acessos que é realizado trimestralmente ou quando solicitado pelo responsável.

O processo de revogação de acessos está detalhado na política “POL-SE-0001 - Política de Segurança Física”, no procedimento “PRC-SE-0002 - Procedimento Revisão de Acesso”, neste último caso discriminamos de forma macro abaixo:

1. POL-SE-0001 - Política de Segurança Física.
2. PRC-SE-0002 - Procedimento Revisão de Acesso:
  - 2.1 Requisição de revisão de acesso
  - 2.2 Solicitar a revisão de acesso (Cliente/Prestador)
  - 2.3 Validação e ajuste do sistema de acesso
  - 2.4 Atualização das listas publicadas no sistema

Visitantes: Os acessos de visitante são revogados no término do período solicitado na requisição de acesso.

## **Revisão periódica dos acessos ao Data Center**

A revisão periódica de acessos ao Data Center é realizada em etapas: funcionários, clientes e prestadores de serviços. Trimestralmente, são listados todos os acessos dos prestadores de serviços e o departamento de acesso e monitoramento realiza a validação dos acessos, validando se são acessos que devem ser mantidos ou não, conforme descrito na Renovação de acesso de prestadores de serviço. Semestral é realizado um processo de revisão de acessos de funcionários ao Data Center, onde são listados todos os funcionários com acesso ativo, e o responsável pela área de Acesso e Monitoramento revisa e solicita qualquer ajuste de acesso necessário.

## **Gerenciamento de organização e sinalização do Data Center**

O gerenciamento da organização e sinalização do Data center é de responsabilidade do departamento de Acesso e monitoramento, tanto para execução quanto para monitoramento das atividades. Todos os Sistemas do Data Centers estão sinalizados com placas, informando o local que se está visitando e as proibições para cada Sistema.

## Gerenciamento de Facilities e Gerenciamento de Mudanças.

Instalação, Configuração e Manutenção dos equipamentos Para a instalação, retirada ou manutenção de equipamentos / sistema do Data Center, é necessário abrir um chamado na Ferramenta de ITSM e encaminhar ao departamento de responsável, para a instalação / remoção / manutenção. As mudanças realizadas nos equipamentos dos Data Centers e nos sistemas utilizados pela Ascenty são classificadas da seguinte maneira:

- Planejadas - Mudanças que precisam ser aprovadas pelo comitê de mudanças e
- que são aplicadas na janela regular (definida pela Ascenty);
- Emergenciais - Mudanças que precisam ser aprovadas pelo comitê de mudanças
- e que são aplicadas em uma janela especial (emergencial) solicitada pelo cliente,
- mesmo que o Sistema não esteja parado.
- Rotina - Mudanças sem impacto (pré-aprovadas) que já foram aprovadas pelo comitê de mudanças pelo menos três vezes.
- Crítica - Mudanças que ocorrem quando o serviço do cliente está parado e
- precisa ser corrigido, necessário ter um incidente associado.

É importante ressaltar que não há desenvolvimento de aplicações ou softwares realizados internamente pela Ascenty, sendo pacotes de mercado.

O departamento de Infraestrutura possui documentos para gerenciar a distribuição dos equipamentos no Data Center e das demais instalações do prédio. As informações podem ser obtidas pela liderança da companhia on-line pelo sistema. Ao final do ano o departamento de Infraestrutura realiza um inventário dos equipamentos do Data Center e documenta via ferramenta de ITSM.

O departamento de Infraestrutura também é responsável por elaborar o cronograma de manutenção dos equipamentos do Data Center. Todas as manutenções são formalizadas por chamado aberto na ferramenta de ITSM.

O processo de instalação, configuração e manutenção de equipamentos do Data Center está detalhado no procedimento “IF-0002 - Manual de Infraestrutura”. Este discriminamos de forma macro abaixo:

1. PRC-FL-0004 - Boas Práticas de Manutenção – DC:
  - 1.1 Consultar calendário de manutenções
  - 1.2 Verificar a aprovação da requisição de mudança

## 1.3 Acompanhar a execução da manutenção

### Gerenciamento de demandas de energia

A disponibilidade de energia para os Data centers da companhia Ascenty é garantida mediante contrato estabelecido entre a companhia e os fornecedores de energia locais.

A energia recebida pelo fornecedor é distribuída em 03 BUS distintos na Ascenty, sendo que estas são suportadas por geradores e dispositivos de Nobreaks. Estas são responsáveis por alimentar o Data Center (racks) e cada sala serve de redundância uma da outra.

A utilização de energia no Data Center é monitorada através da ferramenta BMS. A ferramenta também monitora o índice PUE (Power Usage Effectiveness). As informações referentes ao gerenciamento de energia são usadas para compor o relatório. As informações podem ser obtidas pela liderança da companhia on-line pelo sistema.

### Controles de otimização das operações como alertas e monitoramento

O departamento de Infraestrutura utiliza a ferramenta BMS para monitorar os níveis de temperatura, umidade do ar, equipamentos de detecção e prevenção a incêndios. Em caso de alertas, a ferramenta BMS gera chamados automaticamente na ferramenta de ITSM para o grupo de Infraestrutura, que verifica os incidentes.

O Data Center também possui câmeras de segurança que são monitoradas vinte e quatro horas por dia e as imagens são armazenadas por 90 dias, como determina a ISO27001 e PCI-DSS. Adicionalmente, toda a infraestrutura de cabeamento de dados é realizada de forma estruturada.

Os gerenciamentos dos controles de otimização das operações como alertas e monitoramento de infraestrutura para o Sistema crítico, é gerenciado pela ferramenta

de ITSM através do processo de incidente sendo tratado pelo time responsável "PRO-OP-0001 - Gerenciamento de Incidente e Requisições".

### Controles de segurança e combate a desastres

O Data Center conta com processo formal para evacuação de área e pontos de encontro em caso de desastres. O departamento de acesso e monitoramento faz o acompanhamento de todas as modificações na estrutura do prédio e emite relatórios gerenciais à liderança da empresa.

O processo de gerenciamento dos controles de segurança e de combate a desastres está formalizado nos procedimentos abaixo:

- PRC-ST-0015(MX) - Plan de emergencia y evacuación – Querétaro 1;
- PRC-ST-0016 (CH) Plan de emergencia y evacuación – Santiago 1;
- PRC-ST-0016(BR) - Plano de Atendimento a Emergência – Campinas;
- PRC-ST-0016(MX) - Plan de emergencia y evacuación – Querétaro 2;
- PRC-ST-0017(BR) - Plano de Atendimento a Emergência - Vinhedo;
- PRC-ST-0018(BR) - Plano de Atendimento a Emergência - Jundiaí 1;
- PRC-ST-0019(BR) - Plano de Atendimento a Emergência - Jundiaí 2;
- PRC-ST-0019(CL) - Plan de emergencia y evacuación – Santiago 2;
- PRC-ST-0020(BR) - Plano de Atendimento a Emergência – Osasco;
- PRC-ST-0021(BR) - Plano de Atendimento a Emergência – Paulínia;
- PRC-ST-0022(BR) - Plano de Atendimento a Emergência – Fortaleza;
- PRC-ST-0023(BR) - Plano de Atendimento a Emergência – Sumaré;
- PRC-ST-0024(BR) - Plano de Atendimento a Emergência - Rio de Janeiro;
- PRC-ST-0025(BR) - Plano de Atendimento a Emergência – Hortolândia; e
- PRC-ST-0067(BR) - Plano de Atendimento a Emergência - Osasco SP4.

## Gerenciamento sobre contratos de fornecedores

O departamento de Infraestrutura, em conjunto com o departamento jurídico, é responsável pelo gerenciamento dos contratos com os fornecedores do Data Center. Os contratos são mantidos pelo departamento jurídico e cabe ao departamento de Infraestrutura efetuar o controle sobre a execução dos serviços. A empresa realiza o controle através da intranet da companhia (Sharepoint).

Dependendo do tipo de serviço, pode constar no contrato definições de ANS (Acordo de Nível de Serviço) para monitoramento das atividades desempenhadas. Cabe ao departamento de Infraestrutura monitorar os ANSs e acionar a empresa prestadora de serviço em casos de falhas e/ou atrasos nos serviços contratados.

Os contratos obedecem a política de contratos “POL-AS-0016 - Política para contratos” sendo o gerenciamento de fornecedores verificado pelo processo “PRO-FN-0008 – Homologação e Monitoramento de fornecedores”.

## Ambiente de Controle

A Ascenty disponibiliza e mantém atualizadas as documentações em sua Intranet para que as suas políticas de valores e código de conduta estejam sempre à disposição de todos os seus colaboradores, deixando claro a responsabilidade e papel de cada profissional com a instituição, seja funcionário, terceiros ou parceiros.

Os objetivos e métricas planejadas são definidas levando em consideração as decisões estratégicas e definições da Gerência e conta com incentivos quando necessário para reter e atrair talentos capacitados para exercer as atividades demandadas a fim de que

os objetivos sejam alcançados através de reuniões gravadas e disponibilizadas no SharePoint.

## Comunicação e Informação

Por meio de seus canais de comunicação interna, notifica possíveis alterações e informações relevantes que possam impactar os objetivos previamente definidos pela instituição para que os responsáveis técnicos pela execução dos controles consigam planejar de forma tempestiva possíveis mudanças quando aplicáveis, a fim de que os objetivos da instituição não sejam impactados.

A Ascenty possui canais de comunicação (e-mail, telefone, intranet e site da companhia) onde é possível reportar qualquer tipo de informação, dúvidas, sugestões, incluindo desvios de condutas, onde o Comitê de Ética é responsável por tratar as denúncias recebidas. Qualquer desvio de conduta denunciado é tratado de maneira sigilosa e punições ao denunciado são aplicadas, caso necessário.

## Avaliação de Risco

A Ascenty, por meio de suas Gerências, realiza anualmente uma auditoria pelo departamento de Compliance para identificar todos os tipos de controles existentes na companhia, sejam eles operacionais, financeiros, compliance ou controles do nível da entidade. O referido programa tem por objetivo avaliar os seguintes aspectos:

- Manutenção do ambiente do controle;
- Avaliar a maturidade do processo;
- Melhoria contínua no ambiente;
- Capturar eventuais mudanças e impactos nos processos dos controles e, se necessário, desenvolver um plano de ação;
- Identificar vulnerabilidades e falhas nos controles; e,
- Assegurar o cumprimento das políticas e procedimentos, além das leis, normas e regulamentos aplicável.

Todos os planos de ações provenientes das falhas identificadas no plano de auditoria interna são formalizados na ferramenta Service Now e atrelado aos responsáveis pelo processo que apresentou a falha.

Adicionalmente, a companhia realiza anualmente treinamentos obrigatórios para seus colaboradores, onde são fornecidas oportunidades para que os funcionários aprimorem suas habilidades técnicas e comportamentais, assim como, financiamentos de cursos e certificações. São realizadas atualizações nas políticas de segurança da rede interna, bem como adequação das melhores práticas de segurança e todos os colaboradores tem o dever de realizar anualmente o treinamento de Segurança.

## Atividades de Monitoração

A Ascenty, por meio de sua administração, realiza a inspeção na documentação, além da inspeção física nos data centers em escopo, com o objetivo de verificar a efetividade dos controles abaixo:

- Sinalização dos data centers;
- Processo de instalação ou desinstalação de equipamentos;
- Calendário de manutenções;
- Inventário físico;
- Consumo de energia e contratos com os fornecedores de energia;
- Equipamentos de redundância de energia;
- Mecanismos de refrigeração dimensionados;
- Mecanismos de detecção de incêndio;
- Mecanismos de monitoração por câmeras de segurança;
- Infraestrutura de cabeamento de energia e dados;
- Plano de evacuação;
- Espaço físico para recebimento de materiais; e
- Gestão de contratos com terceiros.

O departamento de Compliance em conjunto com a diretoria executiva e demais áreas impactadas, realizam anualmente um processo de avaliação de risco da companhia. Nesse processo é realizada uma reflexão sobre os tipos de riscos existentes, bem como os limites de tolerância aceitáveis frente ao alcance dos objetivos. A companhia também possui processos estabelecidos para obtenção de certificações, o que implica em objetivos mais específicos. Esse tipo de análise é cascadeada em um plano de ação, que por sua vez inclui a implementação de novos controles e/ou redesenho dos controles já existentes. É importante ressaltar que todos os planos de ações são formalizados através da ferramenta Service Now e delegados aos responsáveis.

## Atividades de Controle

A Ascenty, por meio de suas políticas internas, mantém a segregação adequada na execução de seus controles operacionais em seu ambiente tecnológico. As atividades de controles, tanto manuais quanto automáticas, refletem os interesses operacionais, financeiros e estratégicos da instituição e são divulgados internamente para que os responsáveis estejam cientes de suas responsabilidades.

A administração da Ascenty define atividades de controles internos com base no seu mapa de riscos. Os riscos identificados possuem uma resposta, o que inclui a indicação de controles compensatórios ou indicação de planos de ação para endereçamento. Essa análise é conduzida pelo time de Compliance, diretoria executiva e demais áreas impactadas. O processo de revisão dos riscos versus controles visa avaliar os seguintes aspectos:



1. Que os riscos tiveram uma resposta adequada por meio de atividades de controles;
  2. Assegurar que as atividades de controles levem em consideração as particularidades da companhia, características do processo, inclusive nos diferentes níveis da companhia do ponto de vista de cargos e departamentos;
  3. Assegurar que os processos críticos estão cobertos por atividades de controles;
  4. Estabelecer uma linha de defesa por diferentes tipos de controles, que podem incluir controles automáticos, dependentes de TI ou manuais, e preventivos ou detectivos; e
5. Por fim, é levado em consideração a reflexão sobre a segregação de funções, atividades de controles frente aos riscos identificados leva em consideração tanto os processos de negócio, como controles relacionados à tecnologia da informação.

## Operações Sistêmicas

A Ascenty monitora seus sistemas em camadas de aplicação e infraestrutura realizados por pessoal apropriado. Eventos de segurança no ambiente de produção são registrados e monitorados para serem tratados e considerados nas avaliações e implantações de políticas internas

## Descrição dos controles

Control Environment	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC1.1</b>  <i>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</i>	<b>CC1.1.A</b>  Implementa e mantém um Código de Ética e Conduta divulgado, revisado anualmente pelo conselho de diretores, que estabelece diretrizes para condutas de fornecedores, clientes e colaboradores, com procedimentos de denúncia para infrações.
	<b>CC1.1.B</b>  Anualmente, a área de treinamento proporciona treinamentos obrigatórios aos colaboradores, visando o aprimoramento de suas habilidades técnicas, abrangendo temas como Código de Ética e conduta, Segurança da Informação, Privacidade de Dados e Serviços de TI.
	<b>CC1.1.C</b>  Mensalmente, o Comitê de Ética conduz reuniões para supervisionar e fomentar a integridade e os valores éticos na organização e comunica deficiências nos controles internos em tempo hábil aos responsáveis por tomar ações corretivas.
	<b>CC1.1.D</b>  Anualmente, são realizadas avaliações individuais, dos colaboradores, realizada pela gerência dos colaboradores em conjunto a área de Recursos Humanos.
<b>CC1.2</b>  <i>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</i>	<b>CC1.2.A</b>  A Ascenty mantém um organograma interno que enumera os membros da alta administração, os quais atuam de forma independente em relação à gerência e demonstram imparcialidade nas avaliações e tomada de decisões.
<b>CC1.3</b>  <i>COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</i>	Vide controle <b>CC1.4.A</b> .

<b>CC1.4</b> <i>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</i>	<b>CC1.4.A</b> A Ascenty possui um conjunto de políticas, acessíveis através da intranet, com o propósito de orientar os colaboradores no cumprimento das diretrizes da empresa, e apoiar o funcionamento dos controles internos. Tais como Treinamento e Desenvolvimento, Contratação, Descarte, Backup, Classificação de informações, Segurança da Informação e Privacidade de Dados.
	<b>CC1.4.B</b> Sob demanda, a Ascenty consulta a descrição de competências técnicas relacionada com cargo e/ou área de novos colaboradores, a fim de contratar colaboradores que possuem o nível técnico de acordo com os objetivos da empresa.
<b>CC1.5</b> <i>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</i>	Vide controle <b>CC1.4.A</b> .

Communication and Information	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC2.1</b>  <i>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</i>	<b>CC2.1.A</b>  Anualmente, a organização conduz auditorias independentes para avaliar a aderência às políticas éticas, a eficácia do controle interno e a utilização de informações relevantes e de alta qualidade para respaldar a operação dos controles internos. Adicionalmente, identifica e comunica de forma oportuna quaisquer deficiências nos controles internos.
<b>CC2.2</b>  <i>COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</i>	Vide controle <b>CC1.4.A</b> .
	<b>CC2.2.A</b>  Mensalmente, para que os profissionais obtenham as informações necessárias para apoiar funcionamento do controle interno, objetivos e responsabilidades é realizada uma reunião com os responsáveis e diretoria executiva.
<b>CC2.3</b>  <i>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</i>	<b>CC2.3.A</b>  Sob demanda, a equipe de marketing utiliza de processos para comunicar informações relevantes e oportunas a entidades externas.
	<b>CC2.3.B</b>  A Ascenty utiliza um modelo de contrato padrão que define o escopo do trabalho, assim como especificações, papéis, responsabilidades e nível de serviço prestado, e existem cláusulas contratuais referentes ao cumprimento do Código de Ética e Conduta, obtém compromissos de confidencialidade.

Risk Assessment	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC3.1</b>  <i>COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</i>	<b>CC3.1.A</b>  Anualmente, a organização realiza uma avaliação de riscos e de controles internos, sendo esse um mecanismo para capturar eventuais exceções ao Código de Conduta da companhia, bem como para avaliar os riscos associados ao fornecedores e parceiros de negócios e desenvolver estratégias para mitigar riscos éticos identificados, possíveis interrupções no negócio e para manter controle sobre a tecnologia.
	Vide controle <b>CC2.2.A</b> .
<b>CC3.2</b>  <i>COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</i>	Vide controle <b>CC3.1.A</b> .
<b>CC3.3</b>  <i>COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</i>	Vide controle <b>CC3.1.A</b> .
<b>CC3.4</b>  <i>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</i>	Vide controle <b>CC3.1.A</b> .

## Monitoring Activities

### Trust Services Criteria (TSC)

### Descrição do controle especificado pela Ascenty

#### CC4.1

*COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*

Vide controle **CC2.1.A.**

#### CC4.2

*COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.*

Vide controle **CC2.1.A.**

<b>Control Activities</b>	
<b>Trust Services Criteria (TSC)</b>	<b>Descrição do controle especificado pela Ascenty</b>
<b>CC5.1</b>  <i>COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</i>	Vide controle <b>CC2.2.A.</b>
	Vide controle <b>CC2.2.A.</b>
<b>CC5.2</b>  <i>COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</i>	<b>CC5.2.A</b>  Mensalmente, o departamento de TI realizada o monitoramento da disponibilidade dos principais serviços de TI , que checa parâmetros de conectividade de rede e recursos operacionais do serviço, através de relatórios Power BI.
	Vide controle <b>CC1.4.A.</b>
	Vide controle <b>CC3.1.A.</b>
	Vide controle <b>CC8.1.A.</b>
<b>CC5.3</b>  <i>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</i>	Vide controle <b>CC1.4.A.</b>



Logical and Physical Access Controls	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC6.1</b>  <i>The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</i>	<b>CC6.1.A</b>  A autenticação em aplicativos e serviços corporativo Ascenty é realizado através do ID de identificação única (usuário e senha). Esse processo é automatizado para cumprir os critérios da Política de Senha Segura definida pela Ascenty.
	<b>CC6.1.B</b>  Através da matriz de cargo x departamento, são definidos os níveis adequados de permissões e acessos para usuários e grupos, para que cada indivíduo tenha acesso somente ao que é necessário para realizar suas funções.
	<b>CC6.1.C</b>  Através da topologia de rede da Ascenty, existe a adequada segregação entre as partes não relacionadas do Sistema, bem como se existem redes separadas entre colaboradores Ascenty e visitantes, a fim de prover um mecanismo de defesa adicional contra invasões à sua rede.
	<b>CC6.1.D</b>  Anualmente, realiza um inventário de seus ativos de informações, mantendo um registro dos ativos de informações e proteção adequada. Este processo é registrado através de um ticket na ferramenta de ITSM
<b>CC6.2</b>  <i>Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</i>	<b>ASC.1.2</b>  Os acessos aos ambientes do Data Center são concedidos mediante criação de ticket na ferramenta Service Now para os prestadores de serviço e clientes. As autorizações dos acessos são registradas no próprio ticket, assim como o período de acesso.
	<b>ASC.1.3</b>  Para o funcionário desligado da companhia um ticket é criado na ferramenta Service Now informando o desligamento e solicitando o bloqueio permanente dos acessos as dependências do Data Center.
	<b>ASC.1.4</b>  Os acessos de visitantes nas dependências do Data Center somente são autorizados mediante criação e aprovação de ticket na ferramenta Service Now e este deve ser acompanhado durante toda o período de visita.

	<b>ASC.1.7</b>  Para funcionários a concessão ou alteração de direitos de acesso é realizada através de chamado na ferramenta de ITSM. Na concessão, o RH registra uma solicitação na ferramenta de ITSM
	<b>ASC.1.5</b>  Semestralmente é realizado um processo de revisão de acessos de funcionários ao Data Center. Esta revisão é formalizada na ferramenta Service Now, onde são listados todos os funcionários com acesso ativo, e o responsável pela área de Acesso e Monitoramento revisa e solicita qualquer ajuste de acesso necessário.
	Vide controle <b>CC5.2.C.</b>
	Vide controle <b>CC6.1.B.</b>
<b>CC6.3</b>  <i>The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</i>	Vide controle <b>ASC.1.2.</b>
	Vide controle <b>ASC.1.3.</b>
	Vide controle <b>ASC.1.7.</b>
<b>CC6.4</b>  <i>The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</i>	Vide controle <b>ASC.1.2.</b>
	Vide controle <b>ASC.1.4.</b>
	Vide controle <b>ASC.1.3.</b>
	Vide controle <b>ASC.1.5.</b>
	Vide controle <b>ASC.1.7.</b>
<b>CC6.5</b>  <i>The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.</i>	Vide controle <b>CC1.4.A.</b>

<b>CC6.6</b>  <i>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i>	<b>CC6.6.A</b>  Usa Tecnologias de Criptografia para proteger a transmissão de dados e outras
	<b>CC6.6.C</b>  Implementa firewalls para todos os data centers em escopo
	Vide controle <b>CC1.4.A.</b>
	Vide controle <b>CC6.1.D.</b>
<b>CC6.7</b>  <i>The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.</i>	Vide controle <b>CC6.1.D.</b>
<b>CC6.8</b>  <i>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</i>	<b>CC6.8.A</b>  O departamento de TI, restringe a instalação de Aplicativos e Software a apenas o time de Segurança de Informação, possui acesso de administrador, e se, caso seja necessário por uma questão do negócio, o usuário deve abriu um chamado no Service Now. Mensalmente, é aberto um ticket para verificação de instalação Software.
	<b>CC6.8.B</b>  O departamento de TI utiliza ferramenta para monitorar o ambiente, identificar vírus e malwares, inclusive para fazer a reparação. Adicionalmente, os itens não removidos de forma automática são colocados em quarentena e se são excluídos de forma manual.

System Operations	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC7.1</b>  <i>To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</i>	<b>CC7.1.A</b>  São realizadas varreduras de vulnerabilidades em tempo real por meio de uma ferramenta de Gestão de Vulnerabilidades, que identifica e registra os pontos fracos possam impactar nos ativos de informação. Planos de Remediação são criados e acompanhados diretamente na ferramenta. O departamento de TI monitora continuamente para prevenir a materialização de vulnerabilidades e fortalece os controles internos.
	Vide controle <b>CC6.8.A.</b>
	Vide controle <b>CC6.8.B.</b>
<b>CC7.2</b>  <i>The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</i>	<b>ASC.4.3</b>  O Data Center possui mecanismos de monitoração por câmeras de segurança 24x7, com detecção automática de movimento, em alta definição, gravação e armazenamento das imagens.
	Vide controle <b>CC7.1.A.</b>
<b>CC7.3</b>  <i>The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</i>	<b>CC7.3.A</b>  Sob demanda, os eventos de segurança são registrados e comunicados na ferramenta de ITSM, os incidentes de segurança identificados, a organização realiza uma análise de impacto para entender as consequências potenciais e reais desses eventos em relação ao alcance de seus objetivos, e executa um programa de resposta à incidentes conforme apropriado. A Ascenty possui uma área responsável pelo acompanhamento do fluxo de Gestão de Incidentes, Problemas e Eventos e Requisições de Serviços.
<b>CC7.4</b>  <i>The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</i>	Vide controle <b>CC7.3.A.</b>
<b>CC7.5</b>	Vide controle <b>CC7.3.A.</b>

*The entity identifies, develops, and implements activities to recover from identified security incidents.*

Vide controle **CC9.1.A**.

## **Change Management**

### **Trust Services Criteria (TSC)**

### **Descrição do controle especificado pela Ascenty**

#### **CC8.1**

*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*

#### **CC8.1.A**

Sob demanda, as mudanças no ambiente são aprovadas, documentadas e homologadas antes de serem transportadas para o ambiente de produção do sistema / equipamentos, mediante as devidas aprovações registradas na ferramenta de ITSM. Um registro das mudanças implementadas é mantido, incluindo detalhes sobre as alterações, autorização e datas correspondentes.

## Risk Mitigation

Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
<b>CC9.1</b>  <i>The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</i>	<b>CC9.1.A</b>  Anualmente, às áreas realizam a revisão do plano de continuidade de Negócios (PCN), que descreve as ações a serem tomadas em caso de interrupções, incluindo planos de recuperação, planos de comunicação e atribuição de responsabilidades claras.
	<b>CC9.1.B</b>  Anualmente, realiza testes e exercícios regulares de simulação para verificar a eficácia do PCN.
	<b>CC9.1.C</b>  A Ascenty possui mecanismos de mitigação de riscos e contratos de seguros estabelecidos para reduzir impacto financeiro caso ocorram adversidades na operação.
	<b>CC9.1.D</b>  Através do sistema BMS ("Building Management System"), possuem mecanismos para mitigar riscos de interrupção na operação.
	<b>ASC.2.2</b>  Anualmente é realizado a criação de um calendário de manutenção para todos os equipamentos do Data Center da companhia e as manutenções são realizadas e formalizadas na ferramenta Service Now nas datas pré estabelecidas.
	<b>ASC.3.2</b>  Existência de um contrato formal com um fornecedor de energia que atenda os requisitos necessários pela companhia, tais como manutenções preventivas nas redes elétricas e fornecimento de energia elétrica para o Data Center.
	<b>ASC.3.3</b>  A companhia possui equipamentos de redundância de energia em caso de interrupção momentânea do serviço principal, tais como: no-breaks, geradores e sistema de fornecimento de diesel.
	<b>ASC.4.1</b>  O Data Center possui mecanismos de refrigeração dimensionada de forma a controlar efetivamente a temperatura, umidade e qualidade do ar do ambiente.
	<b>ASC.4.2</b>  O Data Center possui mecanismos de detecção de incêndio (sensores de fumaça) com acionamento precoce de incêndio.

	<b>ASC.4.4</b>  O Data Center possui infraestrutura de cabeamento de energia e dados dispostos de forma segregada e qualquer tipo de modificação ou manutenção a ser realizado é necessário a abertura de um ticket na ferramenta Service Now.
	<b>ASC.5.1</b>  A companhia possui formalizado um plano de evacuação em caso de desastres e equipe de brigadistas treinados para evacuação imediata do prédio
<b>CC9.2</b>  <i>The entity assesses and manages risks associated with vendors and business partners.</i>	<b>CC9.2.A</b>  De acordo com a recorrência dos atendimentos, a equipe de infraestrutura realiza o monitoramento do controle de qualidade dos fornecedores que possuem contratos de serviços e que envolvam os processos críticos para a Infraestrutura de Data Centers, avaliando os aspectos à qualidade dos serviços prestados.
	Vide controle <b>CC2.3.B.</b>
	Vide controle <b>CC3.1.A.</b>

## Additional criterias for Confidentiality

Trust Service Criteria	Descrição do controle especificado pela Ascenty
<b>C1.1</b>  <i>The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.</i>	<b>C1.1.D</b>  A Ascenty disponibiliza backup para o seu ambiente corporativo, permite restaurar o sistema integralmente ou parte dele.
	Vide controle <b>CC1.4.A.</b>
	Vide controle <b>CC2.3.B.</b>
<b>C1.2</b>  <i>The entity disposes of confidential information to meet the entity's objectives related to confidentiality.</i>	Vide controle <b>CC1.4.A.</b>



## PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas KPMG. Para verificar as assinaturas clique no link: <https://apiconfirmations.kpmg.com.br/Verificar/3DD5-B3FE-FD90-76B7>.

Por motivo de segurança e sigilo das informações, não é permitido o download do documento pela tela de validação de assinatura.

**Código para verificação: 3DD5-B3FE-FD90-76B7**



### Hash do Documento

C246F0D28A14C67C331A4A1C25CB5FF8E63E929C22A9F967DA251727F81B026A

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 28/01/2025 é(são) :

☒ Danilo Sandroni Carra - 228.795.768-57 em 28/01/2025 18:41 UTC-03:00

**Tipo:** Assinatura Eletrônica

**Identificação:** Por email: dcarra@kpmg.com.br; Código de acesso: 1418398

### Evidências

**Client Timestamp** Tue Jan 28 2025 18:41:17 GMT-0300 (Brasilia Standard Time)

**Geolocation** Location not shared by user.

**Email** dcarra@kpmg.com.br

**IP** 10.201.227.202

**Assinatura:**



### Hash Evidências:

4E0D540D37626A4BD14589EA440708DDDF5AD70A14233FEA9932B456A3188A9F