

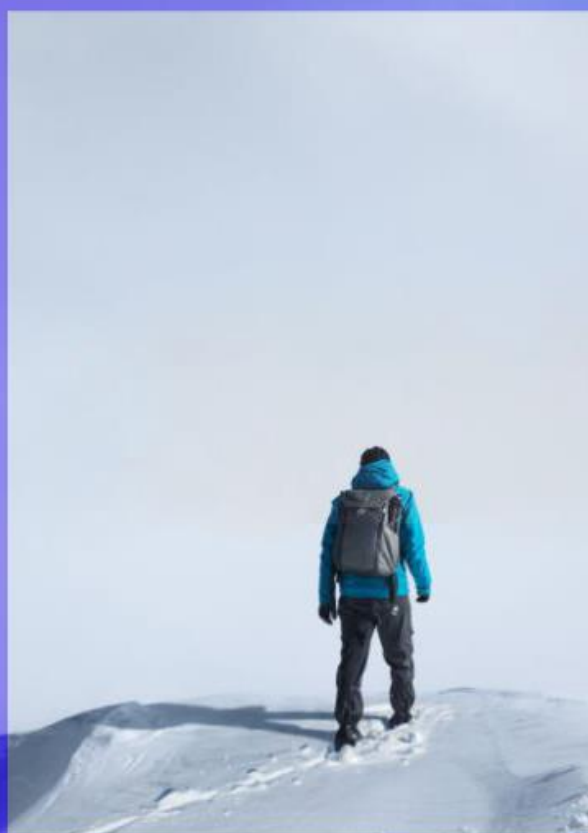


Ascenty Data Centers e Telecomunicações S/A

Relatório de Asseguração Razoável
dos Auditores Independentes -
SOC 2 - Tipo 2, para os princípios de
Segurança e Confidencialidade

SOC 2 - Tipo 2

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



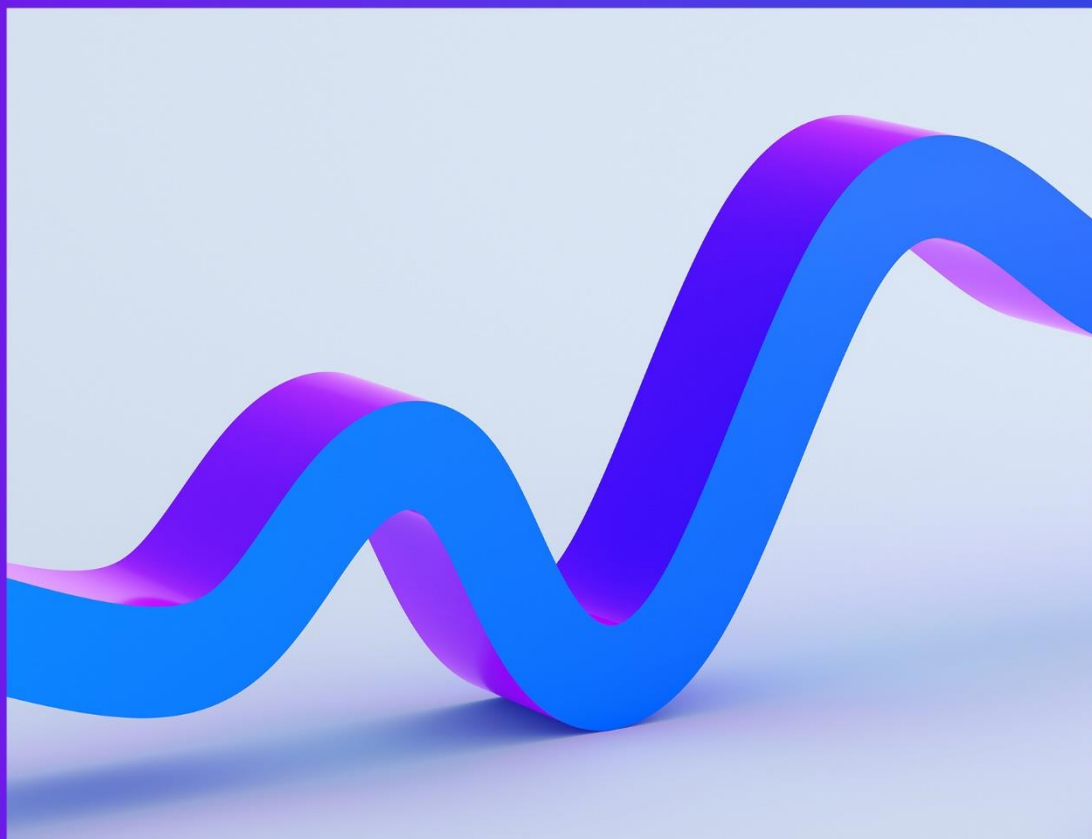
Índice

Seção I	3
Seção II	9
Seção III	13
Seção IV	38
Seção V	64

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 2A80-C293-C965-6220.

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 asseguração 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.

As informações contidas na Seção V, “Outras informações fornecidas pela Organização Prestadora de Serviços”, fornecidas pela administração da Ascenty para prover informações adicionais sobre a organização prestadora de serviços, não fizeram parte da nossa avaliação dos controles de acesso físico, manutenção e operação de Data Centers (*Facilities*) durante o período de 1º de janeiro a 31 de dezembro de 2024. Desse modo, essas informações não foram sujeitas aos mesmos procedimentos aplicados pela Ascenty, tampouco realizamos avaliação sobre a adequação do desenho e a efetividade operacional dos controles relacionados com os objetivos de controles especificados nessa descrição, portanto não emitimos opinião sobre essas informações.



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 asseguração 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:

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

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 2A80-C293-C965-6220.

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 2A80-C293-C965-6220.



- 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

Nossa opinião foi fundamentada nos assuntos descritos neste relatório. Os critérios utilizados na formação de nossa opinião são aqueles descritos na Seção IV. 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.

Descrição dos Testes de Controle

Os controles específicos testados e a natureza, época e resultados desses testes estão listados na seção IV.

Uso restrito

Este relatório, incluindo a descrição dos testes de controles e resultados dos mesmos na Seção IV, destina-se exclusivamente para informação e uso da Ascenty, entidades usuárias dos serviços relacionados durante parte ou todo o período de 1º de janeiro a 31 de dezembro de 2024, parceiros de negócios da Ascenty sujeitos a riscos decorrentes de interações com os serviços da Ascenty e profissionais que prestam serviços a essas entidades de usuários e parceiros de negócios, que têm conhecimento e entendimento suficientes sobre:

- A natureza do serviço prestado pela organização prestadora de serviços;
- Como o sistema da organização prestadora de serviços interage com entidades de usuários, parceiros de negócios, organizações de subserviços e outras partes;
- Controle interno e suas limitações;
- Controles complementares da entidade usuária e controles complementares da organização de subserviços e como esses controles interagem com os controles na organização prestadora de serviços para atingir os compromissos de serviço e requisitos de sistemas da organização prestadora de serviços;
- Responsabilidades da entidade usuária e como elas podem afetar a capacidade da entidade usuária de usar efetivamente os serviços da organização prestadora de serviços;
- Os critérios de serviços de confiança aplicáveis; e



- Os riscos que podem ameaçar o cumprimento dos compromissos de serviço e requisitos de sistemas da organização prestadora de serviços e como os controles abordam esses riscos.

O presente relatório não tem como objetivo e nem deverá ser utilizado por qualquer um que não as partes especificadas.

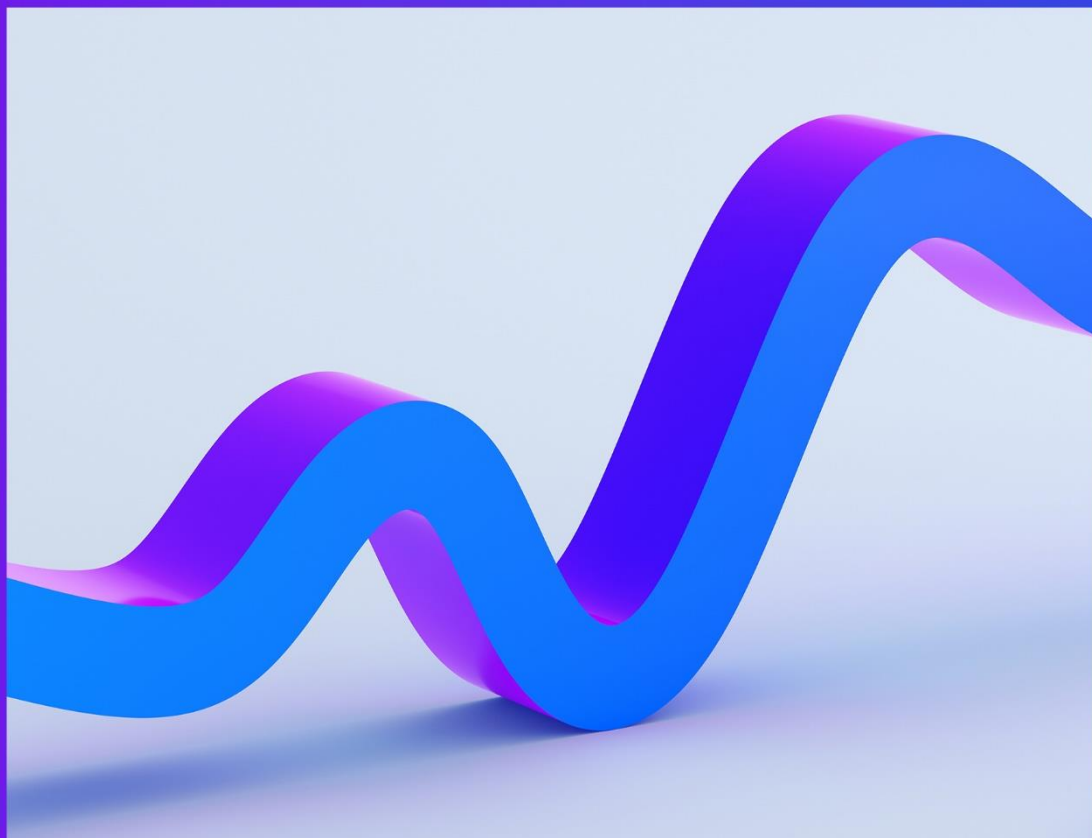
São Paulo, 27 de janeiro de 2025

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

Danilo Sandroni Carra
Contador CRC 1SP353622/O-4

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:



9842EF54AA924BD

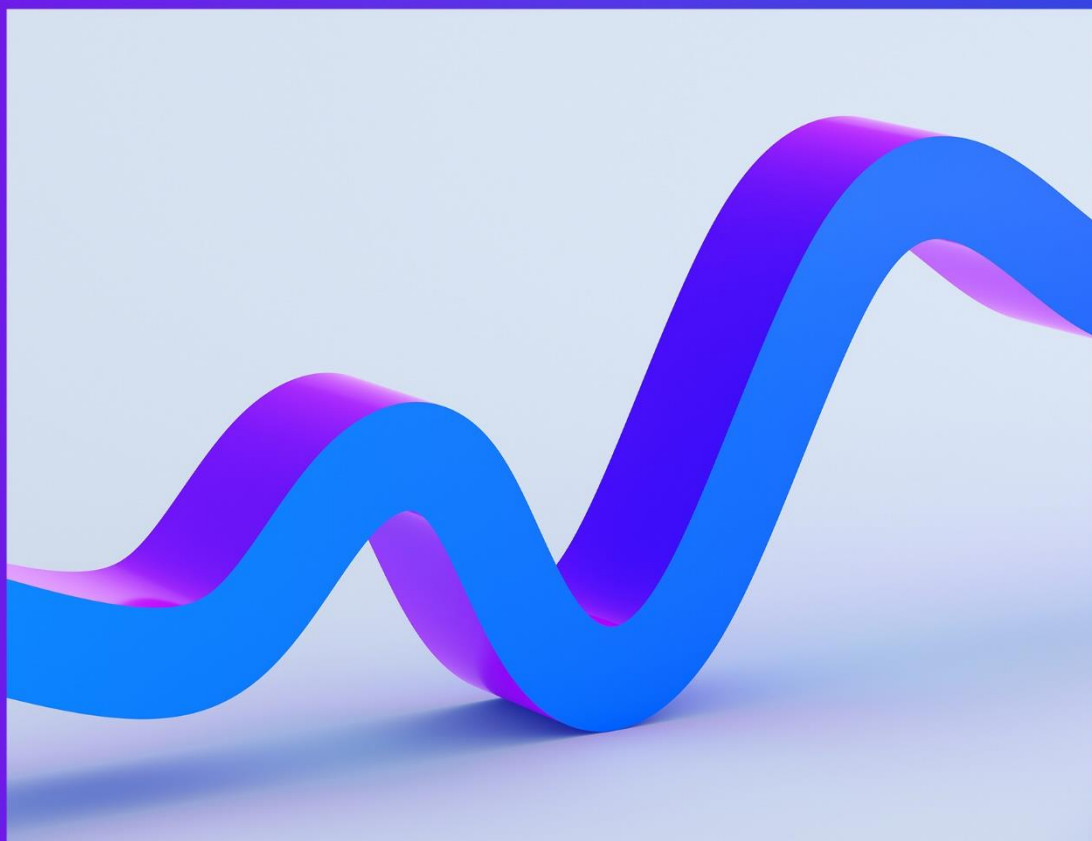
Marcos Siqueira

VP de Operações

Ascenty Data Centers e Telecomunicações S/A

Seção III

Descrição elaborada pela
Organização Prestadora de
Serviços Ascenty



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 Datas 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	
<i>Trust Services Criteria (TSC)</i>	Descrição do controle especificado pela Ascenty
CC1.1 <i>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</i>	CC1.1.A 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.
	CC1.1.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.
	CC1.1.C 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.
	CC1.1.D Anualmente, são realizadas avaliações individuais, dos colaboradores, realizada pela gerência dos colaboradores em conjunto a área de Recursos Humanos.
CC1.2 <i>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</i>	CC1.2.A 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.
CC1.3 <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 CC1.4.A.

CC1.4 <i>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</i>	CC1.4.A 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.
	CC1.4.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.
CC1.5 <i>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</i>	Vide controle CC1.4.A .

Communication and Information	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
CC2.1 <i>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</i>	CC2.1.A 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.
CC2.2 <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 CC1.4.A .
	CC2.2.A 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.
CC2.3 <i>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</i>	CC2.3.A Sob demanda, a equipe de marketing utiliza de processos para comunicar informações relevantes e oportunas a entidades externas.
	CC2.3.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
CC3.1 <i>COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</i>	CC3.1.A 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 CC2.2.A .
CC3.2 <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 CC3.1.A .
CC3.3 <i>COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</i>	Vide controle CC3.1.A .
CC3.4 <i>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</i>	Vide controle CC3.1.A .

Monitoring Activities	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
CC4.1 <i>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.</i>	Vide controle CC2.1.A.
CC4.2 <i>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.</i>	Vide controle CC2.1.A.

Control Activities	
<i>Trust Services Criteria (TSC)</i>	Descrição do controle especificado pela Ascenty
CC5.1 <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 CC2.2.A.
	Vide controle CC2.2.A.
CC5.2 <i>COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</i>	CC5.2.A 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 CC1.4.A.
	Vide controle CC3.1.A.
	Vide controle CC8.1.A.
CC5.3 <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 CC1.4.A.

Logical and Physical Access Controls	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
CC6.1 <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>	CC6.1.A 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.
	CC6.1.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.
	CC6.1.C 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.
	CC6.1.D 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
CC6.2 <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>	ASC.1.2 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.
	ASC.1.3 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.
	ASC.1.4 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.

	ASC.1.7 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
	ASC.1.5 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 CC5.2.C.
	Vide controle CC6.1.B.
CC6.3 <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 ASC.1.2.
	Vide controle ASC.1.3.
	Vide controle ASC.1.7.
CC6.4 <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 ASC.1.2.
	Vide controle ASC.1.4.
	Vide controle ASC.1.3.
	Vide controle ASC.1.5.
	Vide controle ASC.1.7.

<p>CC6.5</p> <p><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></p>	<p>Vide controle CC1.4.A.</p>
<p>CC6.6</p> <p><i>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i></p>	<p>CC6.6.A</p> <p>Usa Tecnologias de Criptografia para proteger a transmissão de dados e outras</p>
	<p>CC6.6.C</p> <p>Implementa firewalls para todos os data centers em escopo</p>
	<p>Vide controle CC1.4.A.</p>
	<p>Vide controle CC6.1.D.</p>
<p>CC6.7</p> <p><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></p>	<p>Vide controle CC6.1.D.</p>
<p>CC6.8</p> <p><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></p>	<p>CC6.8.A</p> <p>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.</p>
	<p>CC6.8.B</p> <p>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.</p>

System Operations	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
CC7.1 <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>	CC7.1.A 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 CC6.8.A.
	Vide controle CC6.8.B.
CC7.2 <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>	ASC.4.3 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 CC7.1.A.
CC7.3 <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>	CC7.3.A 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.
CC7.4 <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 CC7.3.A.

CC7.5 <i>The entity identifies, develops, and implements activities to recover from identified security incidents.</i>	Vide controle CC7.3.A .
	Vide controle CC9.1.A .

Change Management	
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty
CC8.1 <i>The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</i>	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

CC9.1

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

CC9.1.A

Anualmente, as 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.

CC9.1.B

Anualmente, realiza testes e exercícios regulares de simulação para verificar a eficácia do PCN.

CC9.1.C

A Ascenty possui mecanismos de mitigação de riscos e contratos de seguros estabelecidos para reduzir impacto financeiro caso ocorram adversidades na operação.

CC9.1.D

Através do sistema BMS ("Building Management System"), possuem mecanismos para mitigar riscos de interrupção na operação.

ASC.2.2

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.

ASC.3.2

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.

ASC.3.3

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.

ASC.4.1

O Data Center possui mecanismos de refrigeração dimensionada de forma a controlar efetivamente a temperatura, umidade e qualidade do ar do ambiente.

ASC.4.2

O Data Center possui mecanismos de detecção de incêndio (sensores de fumaça) com acionamento precoce de incêndio.

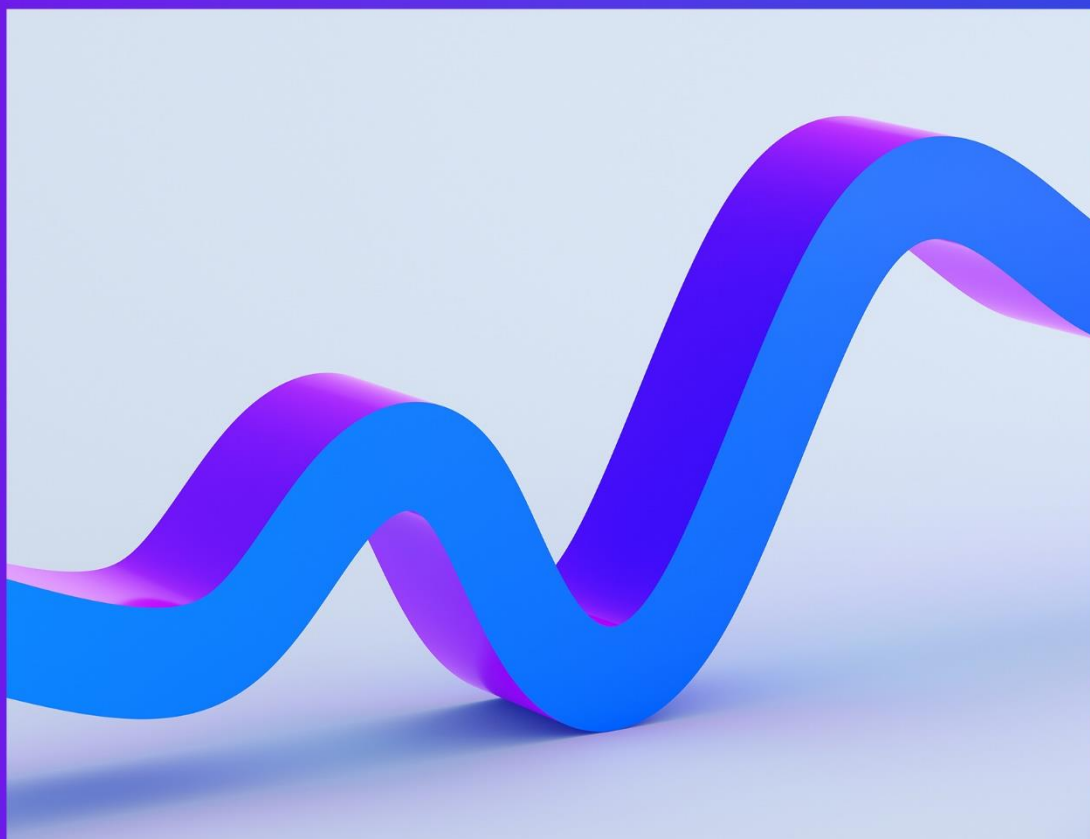
	ASC.4.4 O Data Center possui infraestrutura de cabeamento de energia e dados dispostos de forma segregada e qualquer tipo de modificação ou manutenção a ser realizado é necessário a abertura de um ticket na ferramenta Service Now.
	ASC.5.1 A companhia possui formalizado um plano de evacuação em caso de desastres e equipe de brigadistas treinados para evacuação imediata do prédio
CC9.2 <i>The entity assesses and manages risks associated with vendors and business partners.</i>	CC9.2.A 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 CC2.3.B.
	Vide controle CC3.1.A.

Additional criterias for Confidentiality

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

Seção IV

Critérios de Serviço, Controles
Relacionados, Teste de
Projeto e de Eficácia
Operacional



Considerações dos Entity Level Controls

No planejamento da natureza, período e extensão dos procedimentos de teste dos controles especificados pela Organização Prestadora de Serviços em sua Descrição na Seção III, a KPMG considerou os aspectos do ambiente de controle da Organização Prestadora de Serviços, dentre eles as atividades de controle, avaliação de riscos, informação e comunicação, além do monitoramento das atividades, considerando esses componentes de controles internos necessários nas circunstâncias de prestação de serviços às organizações usuárias.

Procedimentos para avaliação da Integridade e Precisão (Completeness and Accuracy – C&A) das Informações Produzidas pela Entidade (Information Provided by the Entity – IPE)

Durante a realização dos testes de controle que requeriam o uso de Informações Produzidas pela Entidade (IPE), foram realizados procedimentos para avaliar a Integridade e Precisão (C&A) das informações, incluindo avaliação de outros controles ou relatórios, para determinar se a informação poderia ser considerada nos procedimentos de nosso exame. Isso inclui IPEs produzidos pela Organização Prestadora de Serviços e/ou fornecido às organizações usuárias (se relevante), IPEs usados pela administração da Organização Prestadora de Serviços na execução dos controles, e IPEs utilizados na execução de nossos procedimentos de teste.

Com base na natureza dos IPEs, uma combinação dos seguintes procedimentos foram realizadas para avaliar a Integridade e Precisão (C&A) dos dados ou relatórios utilizados: (1) Inspeção da documentação de origem relativa ao IPE; (2) Inspeção da consulta, script ou dos parâmetros utilizados para geração do IPE; e/ou (3) Confronto dos dados entre o IPE e a fonte ou origem da informação.



Control Environment			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.A 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.	Indagação aos responsáveis pelo processo de manutenção do Código de Ética e Conduta, a fim de inspecionar o desenho do controle. Inspeção do Código de Ética e Conduta, a fim de observar se este estabelece as diretrizes para condutas de fornecedores, clientes e colaboradores, além de conter procedimentos de denúncias para infrações, e também se este é revisado anualmente pelo conselho de diretores.	Não identificamos exceções.
	CC1.1.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.	Indagação aos responsáveis pelo processo de treinamento, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de treinamento estão devidamente documentadas e formalizadas. Seleção de colaboradores ativos, a fim de observar se participaram dos treinamentos anuais obrigatórios.	Não identificamos exceções.
	CC1.1.C 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.	Indagação aos responsáveis pela gestão do Comitê de Ética, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de meses para os quais foi solicitada documentação suporte, a fim de observar se os comitês mensais foram realizados e registrados.	Não identificamos exceções.

	<p>CC1.1.D</p> <p>Anualmente, são realizadas avaliações individuais, dos colaboradores, realizada pela gerência dos colaboradores em conjunto a área de Recursos Humanos.</p>	<p>Indagação aos responsáveis pelo processo de avaliação individual dos colaboradores, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de colaboradores ativos, a fim de observar se participaram do processo de avaliação de desempenho individual anual.</p>	Não identificamos exceções.
<p>CC1.2</p> <p>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</p>	<p>CC1.2.A</p> <p>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.</p>	<p>Indagação aos responsáveis pela manutenção do organograma, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção do organograma, a fim de observar se os membros da alta administração possuem independência em relação à gerência.</p>	Não identificamos exceções.
<p>CC1.3</p> <p>COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</p>	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.

CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.A 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.	Indagação aos responsáveis pelo processo de gerenciamento das normativas internas, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção das seguintes normativas internas, a fim de observar se estavam devidamente formalizadas, revisadas e disponíveis: “POL-AS-0001 – Política de classificação informações”, “POL-AS-0002 – Política de segurança da informação”, POL-AS-0017 – Política de privacidade de Dados”, POL-OP-0002 – Política de backup”, “PRC-OP-0013 – Procedimento de descarte de informações”, “PRC-RH-0002 – Procedimento de contratação” e “PRC-RH-0004 – Treinamento e Desenvolvimento”.	Não identificamos exceções.
	CC1.4.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.	Indagação aos responsáveis pelo processo de contratação, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de colaboradores admitidos, a fim de observar se a contratação foi aprovada por alçada competente.	Não identificamos exceções.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.

Communication and Information			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.A 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.	Indagação aos responsáveis pelo processo de acompanhamento das auditorias ISO, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção do relatório de conclusão das auditorias ISO, a fim de observar se os principais assuntos foram registrados e comunicados às partes interessadas.	Não identificamos exceções.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
	CC2.2.A 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.	Indagação aos responsáveis pela gestão das reuniões entre os times operacionais e os executivos da diretoria, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de meses para os quais foi solicitada documentação suporte, a fim de observar se os encontros mensais foram realizados e registrados.	Não identificamos exceções.



CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.A Sob demanda, a equipe de marketing utiliza de processos para comunicar informações relevantes e oportunas a entidades externas.	Indagação aos responsáveis pela processo de comunicação com entidades externas, a fim de inspecionar o desenho do controle adotado pela companhia.	Observamos que não houve ocorrência da execução do controle durante o período entre 1º de janeiro a 31 de dezembro de 2024, de forma que não foi possível opinar sobre sua efetividade operacional.
	CC2.3.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.	Indagação aos responsáveis pelo processo de gestão de contratos, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos contratos definidos como relevantes pela Ascenty, a fim de observar se estes possuem compromissos de confidencialidade e nível de serviço (SLA) devidamente formalizados.	Não identificamos exceções.



Risk Assessment			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.A 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.	Indagação aos responsáveis pelo processo de gerenciamento de riscos, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção da documentação suporte referente ao relatório anual de avaliação de riscos, a fim de observar se o processo foi devidamente documentado e formalizado.	Não identificamos exceções.
	Vide controle CC2.2.A.	Vide controle CC2.2.A.	Vide controle CC2.2.A.
CC3.2 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.	Vide controle CC3.1.A.	Vide controle CC3.1.A.	Vide controle CC3.1.A.



CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Vide controle CC3.1.A.	Vide controle CC3.1.A.	Vide controle CC3.1.A.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Vide controle CC3.1.A.	Vide controle CC3.1.A.	Vide controle CC3.1.A.

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 2A80-C293-C965-6220.



Monitoring Activities			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
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.	Vide controle CC2.1.A.	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.	Vide controle CC2.1.A.	Vide controle CC2.1.A.

Control Activities			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC5.1 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.	Vide controle CC2.2.A.	Vide controle CC2.2.A.	Vide controle CC2.2.A.
	Vide controle CC2.2.A.	Vide controle CC2.2.A.	Vide controle CC2.2.A.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.2.A 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.	Indagação aos responsáveis pelo processo de monitoramento da disponibilidade dos serviços de TI, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de meses, a fim de observar se os relatórios de monitoramento de disponibilidade de TI foram confeccionados e disponibilizados.	Não identificamos exceções.
	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
	Vide controle CC3.1.A.	Vide controle CC3.1.A.	Vide controle CC3.1.A.
	Vide controle CC8.1.A.	Vide controle CC8.1.A.	Vide controle CC8.1.A.



CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
--	-------------------------------	-------------------------------	-------------------------------

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 2A80-C293-C965-6220.

Logical and Physical Access Controls			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC6.1 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.	CC6.1.A 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.	Indagação aos responsáveis pelo processo de configuração dos parâmetros de senha do <i>Active Directory</i> , a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos parâmetros de senha do <i>Active Directory</i> , a fim de observar estes possuem parâmetros mínimos de segurança configurados (histórico de senhas que não podem ser utilizadas, duração máxima de uma senha, tamanho mínimo de uma senha e complexidade de senha habilitada).	Não identificamos exceções.
	CC6.1.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.	Indagação aos responsáveis pelo processo de gestão de acessos físicos, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de colaboradores admitidos no período escopo, a fim de observar se os acessos foram concedidos de acordo com matriz de cargo vs departamento pré-existente.	Não identificamos exceções.
	CC6.1.C 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.	Indagação aos responsáveis pelo processo de segregação de redes, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção das configurações de rede, a fim de observar se a rede de visitante está devidamente segregada.	Não identificamos exceções.

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 2A80-C293-C965-6220.

	<p>CC6.1.D</p> <p>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</p>	<p>Indagação aos responsáveis pelo processo de gestão de ativos, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de Data Center para os quais foi solicitada documentação suporte referente à atualização anual do inventário, a fim de observar se estas foram devidamente atualizadas e registradas.</p>	Não identificamos exceções.
<p>CC6.2</p> <p>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.</p>	<p>ASC.1.2</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de acesso aos Data Centers estão devidamente documentadas e formalizadas.</p> <p>Seleções de concessões de acesso a prestadores de serviço e a clientes aos Data Centers, a fim de observar os chamados foram devidamente registrados na ferramenta de ITSM.</p>	Não identificamos exceções.
	<p>ASC.1.3</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleções de revogações de acesso aos Data Centers do Brasil, Chile e do México, a fim de observar os chamados foram tempestiva e devidamente registrados na ferramenta de ITSM.</p>	Não identificamos exceções.

	<p>ASC.1.4</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de concessões de acesso a visitantes aos Data Centers, a fim de observar os chamados foram devidamente registrados na ferramenta de ITSM.</p>	Não identificamos exceções.
	<p>ASC.1.7</p> <p>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</p>	<p>Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de acesso aos Data Centers estão devidamente documentadas e formalizadas.</p> <p>Seleções de colaboradores admitidos, a fim de observar se os chamados foram devidamente registrados na ferramenta de ITSM.</p>	Não identificamos exceções.
	<p>ASC.1.5</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de semestres vs Data Centers, para os quais foi solicitada documentação suporte, a fim de observar se as revisões de acesso foram realizadas e, se necessário, as ações corretivas foram tomadas.</p>	Não identificamos exceções.
	Vide controle CC5.2.C.	Vide controle CC5.2.C.	Vide controle CC5.2.C.
	Vide controle CC6.1.B.	Vide controle CC6.1.B.	Vide controle CC6.1.B.

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 2A80-C293-C965-6220.



CC6.3 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.	Vide controle ASC.1.2.	Vide controle ASC.1.2.	Vide controle ASC.1.2.
	Vide controle ASC.1.3.	Vide controle ASC.1.3.	Vide controle ASC.1.3.
	Vide controle ASC.1.7.	Vide controle ASC.1.7.	Vide controle ASC.1.7.
CC6.4 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.	Vide controle ASC.1.2.	Vide controle ASC.1.2.	Vide controle ASC.1.2.
	Vide controle ASC.1.4.	Vide controle ASC.1.4.	Vide controle ASC.1.4.
	Vide controle ASC.1.3.	Vide controle ASC.1.3.	Vide controle ASC.1.3.
	Vide controle ASC.1.5.	Vide controle ASC.1.5.	Vide controle ASC.1.5.
	Vide controle ASC.1.7.	Vide controle ASC.1.7.	Vide controle ASC.1.7.

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 2A80-C293-C965-6220.

CC6.5 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.	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.A Usa Tecnologias de Criptografia para proteger a transmissão de dados e outras	Indagação aos responsáveis pelo processo de gestão de criptografia, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção da configuração do console, a fim de observar se os parâmetros de criptografia estão habilitados para os dispositivos do parque tecnológico da Ascenty.	Não identificamos exceções.
	CC6.6.C Implementa firewalls para os data centers em escopo	Indagação aos responsáveis pelo processo de gestão de <i>firewalls</i> , a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos chamados de manutenção dos <i>firewalls</i> de cada um dos Data Centers em escopo, a fim de observar se estavam implementados e se o chamado foi registrado.	Não identificamos exceções.
	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
	Vide controle CC6.1.D.	Vide controle CC6.1.D.	Vide controle CC6.1.D.

<p>CC6.7</p> <p>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.</p>	<p>Vide controle CC6.1.D.</p>	<p>Vide controle CC6.1.D.</p>	<p>Vide controle CC6.1.D.</p>
<p>CC6.8</p> <p>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</p>	<p>CC6.8.A</p> <p>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 abrir um chamado no Service Now. Mensalmente, é aberto um ticket para verificação de instalação Software.</p>	<p>Indagação aos responsáveis pelo processo de restrição de privilégios e de revisão mensal de <i>softwares</i>, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção da relação de usuários com permissão para instalação de aplicativos e <i>softwares</i>, a fim de observar se este privilégio está restrito ao pessoal adequado.</p> <p>Seleção de meses para os quais foi solicitada documentação suporte acerca da revisão de <i>softwares</i> e, em caso de possíveis desvios, os devidos planos de ação.</p>	<p>Não identificamos exceções.</p>
	<p>CC6.8.B</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gerenciamento de <i>malwares</i>, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de alertas gerados pela ferramenta de monitoramento de <i>malware</i> para os quais foi solicitada documentação suporte a fim de observar se foram devidamente endereçados.</p>	<p>Não identificamos exceções.</p>

System Operations			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC7.1 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.	CC7.1.A 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.	Indagação aos responsáveis pelo processo de gerenciamento de vulnerabilidades, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção da ferramenta Rapid7 a fim de observar os planos de remediação e seu acompanhamento/progresso. Seleção de meses a fim de inspecionar a documentação suporte referente ao <i>scan</i> mensal de vulnerabilidades.	Observamos que o controle passou a operar a partir de junho de 2024, de forma que não foi possível opinar sobre seu desenho e efetividade operacional anterior a esta data. Para o período compreendido entre junho a dezembro de 2024, não identificamos exceções.
	Vide controle CC6.8.A.	Vide controle CC6.8.A.	Vide controle CC6.8.A.
	Vide controle CC6.8.B.	Vide controle CC6.8.B.	Vide controle CC6.8.B.
CC7.2 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.	ASC.4.3 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.	Indagação aos responsáveis pelo processo de monitoramento por meio de CFTV, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos Data Centers, a fim de observar se estes possuem sistema de CFTV ativo.	Não identificamos exceções.
	Vide controle CC7.1.A.	Vide controle CC7.1.A.	Vide controle CC7.1.A.

<p>CC7.3</p> <p>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.</p>	<p>CC7.3.A</p> <p>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.</p>	<p>Indagação aos responsáveis pelo processo de gerenciamento de requisições, incidentes e problemas, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de gerenciamento de requisições, incidentes e problemas estão devidamente documentadas e formalizadas.</p> <p>Seleções de requisições, incidentes e problemas, a fim de observar se foram devidamente registradas e aprovadas de acordo com a política vigente.</p>	<p>Não identificamos exceções.</p>
<p>CC7.4</p> <p>The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p>	<p>Vide controle CC7.3.A.</p>	<p>Vide controle CC7.3.A.</p>	<p>Vide controle CC7.3.A.</p>
<p>CC7.5</p> <p>The entity identifies, develops, and implements activities to recover from identified security incidents.</p>	<p>Vide controle CC7.3.A.</p>	<p>Vide controle CC7.3.A.</p>	<p>Vide controle CC7.3.A.</p>
	<p>Vide controle CC9.1.A.</p>	<p>Vide controle CC9.1.A.</p>	<p>Vide controle CC9.1.A.</p>



Change Management			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
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.	Indagação aos responsáveis pelo processo de gerenciamento de mudanças, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de gerenciamento de mudanças estão devidamente documentadas e formalizadas. Seleções de mudanças planejadas, emergenciais e críticas, a fim de observar se foram devidamente registradas e aprovadas de acordo com a política vigente.	Não identificamos exceções.



Risk Mitigation			
Trust Services Criteria (TSC)	Descrição do controle especificado pela Ascenty	Procedimentos adotados pela KPMG em relação ao desenho e efetividade do controle	Resultado do teste
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.A 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.	Indagação aos responsáveis pelo plano de continuidade de negócios, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de gerenciamento de mudanças estão devidamente documentadas e formalizadas. Inspeção da documentação suporte referente à última revisão anual do Plano de Continuidade de Negócios (PCN), a fim de observar se foi devidamente atualizado e formalizado.	Não identificamos exceções.
	CC9.1.B Anualmente, realiza testes e exercícios regulares de simulação para verificar a eficácia do PCN.	Indagação aos responsáveis pelo plano de continuidade de negócios, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção de normativos internos, a fim de observar se as diretrizes para execução do controle de gerenciamento de mudanças estão devidamente documentadas e formalizadas. Inspeção da documentação suporte referente à última revisão anual do Plano de Continuidade de Negócios (PCN), a fim de observar se os testes foram realizados e os resultados formalizados.	Não identificamos exceções.

	CC9.1.C A Ascenty possui mecanismos de mitigação de riscos e contratos de seguros estabelecidos para reduzir impacto financeiro caso ocorram adversidades na operação.	Indagação aos responsáveis pela apólice de seguros, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção do certificado de cobertura da apólice de seguro, a fim de observar se o contrato está válido para os Data Centers em escopo.	Não identificamos exceções.
	CC9.1.D Através do sistema BMS (“Building Management System”), possuem mecanismos para mitigar riscos de interrupção na operação.	Indagação aos responsáveis pelo monitoramento de eventos que podem interromper a operação, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de alertas gerados pela ferramenta BMS, a fim de observar se foram devidamente registrados e endereçados.	Não identificamos exceções.
	ASC.2.2 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.	Indagação aos responsáveis pela manutenção dos equipamentos de Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de manutenções planejadas e emergenciais, a fim de observar se foram realizadas conforme cronograma parametrizado no ServiceNow.	Não identificamos exceções.
	ASC.3.2 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.	Indagação aos responsáveis pelo gerenciamento de contratos, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de Data Centers, a fim de observar se os contratos com fornecedores de energia, dispunham dos requisitos necessários pela companhia, tais como a manutenção preventiva e o fornecimento de energia.	Não identificamos exceções.

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 2A80-C293-C965-6220.

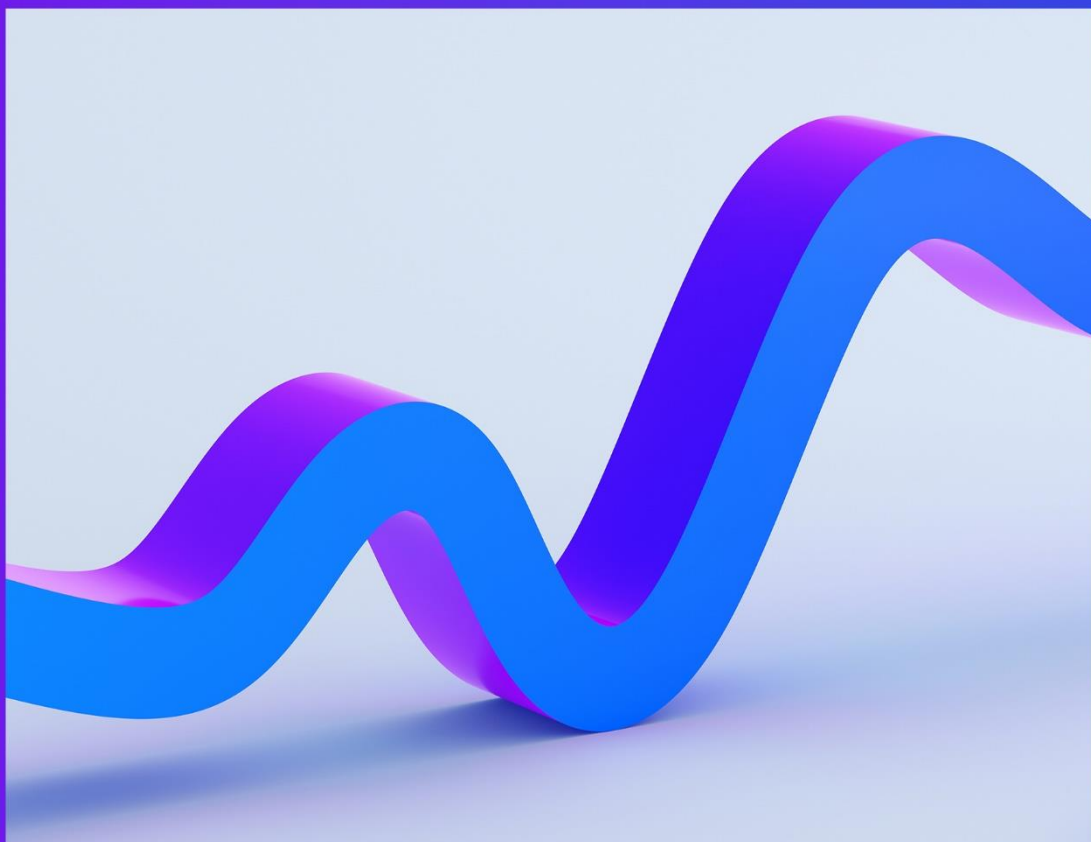
	<p>ASC.3.3</p> <p>A companhia possui equipamentos de redundância de energia em caso de interrupção momentânea do serviço principal, tais como: no-breaks, geradores e sistema de fornecimento de diesel.</p>	<p>Indagação aos responsáveis pelo gerenciamento dos equipamentos de fornecimento de energia em redundância, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção dos consoles de monitoramento dos equipamentos de energia, a fim de observar se estão funcionando em redundância.</p>	<p>Não identificamos exceções.</p>
	<p>ASC.4.1</p> <p>O Data Center possui mecanismos de refrigeração dimensionada de forma a controlar efetivamente a temperatura, umidade e qualidade do ar do ambiente.</p>	<p>Indagação aos responsáveis pelo gerenciamento dos equipamentos de refrigeração, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção dos Data Centers, a fim de observar se estes possuem equipamentos de ar condicionado e de monitoramento de qualidade, umidade e de temperatura.</p>	<p>Não identificamos exceções.</p>
	<p>ASC.4.2</p> <p>O Data Center possui mecanismos de detecção de incêndio (sensores de fumaça) com acionamento precoce de incêndio.</p>	<p>Indagação aos responsáveis pelo gerenciamento dos equipamentos de detecção de incêndio, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção dos Data Centers, a fim de observar se estes possuem equipamentos de detecção de incêndio.</p>	<p>Não identificamos exceções.</p>
	<p>ASC.4.4</p> <p>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.</p>	<p>Indagação aos responsáveis pelo cabeamento dos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção dos Data Centers, a fim de observar o cabeamento foi feito respeitando a segregação entre cabos de dados e de energia.</p>	<p>Não identificamos exceções.</p>

	<p>ASC.5.1</p> <p>A companhia possui formalizado um plano de evacuação em caso de desastres e equipe de brigadistas treinados para evacuação imediata do prédio</p>	<p>Indagação aos responsáveis pelo plano de evacuação, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspeção de normativos internos, a fim de observar se as diretrizes para execução de evacuação estão devidamente formalizados.</p>	Não identificamos exceções.
<p>CC9.2</p> <p>The entity assesses and manages risks associated with vendors and business partners.</p>	<p>CC9.2.A</p> <p>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.</p>	<p>Indagação aos responsáveis pelo gerenciamento de fornecedores, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de meses para os quais foi solicitada documentação suporte referente à avaliação dos fornecedores críticos, a fim de observar se a qualidade destes foi devidamente monitorada, bem como se as execuções foram realizadas sem falhas.</p>	Não identificamos exceções.
	Vide controle CC2.3.B.	Vide controle CC2.3.B.	Vide controle CC2.3.B.
	Vide controle CC3.1.A.	Vide controle CC3.1.A.	Vide controle CC3.1.A.

Additional criterias for Confidentiality			
Trust Service Criteria	Descrição do controle especificado pela Ascenty	Procedimentos aplicados pela KPMG sobre o desenho e a efetividade operacional do controle	Resultado dos testes
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C1.1.D A Ascenty disponibiliza backup para o seu ambiente corporativo, permite restaurar o sistema integralmente ou parte dele.	Indagação aos responsáveis pelo gerenciamento de <i>backup</i> , a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de rotinas automatizadas de backup, a fim de observar se foram devidamente parametrizadas, bem como se as execuções foram realizadas sem falhas. Seleção de meses, para os quais foi solicitada documentação suporte referente aos testes de <i>restore</i> , a fim de observar se foram devidamente executados e documentados.	Não identificamos exceções.
	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.
	Vide controle CC2.3.B.	Vide controle CC2.3.B.	Vide controle CC2.3.B.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Vide controle CC1.4.A.	Vide controle CC1.4.A.	Vide controle CC1.4.A.

Seção V

Outras informações fornecidas
pela Organização Prestadora
de Serviço



Outras informações fornecidas pela Ascenty

A Ascenty possui um plano de expansão no seu plano estratégico, onde todos os controles internos dos processos de gerenciamento de acesso físico e de Infraestrutura serão replicados para os novos Data Centers.

Componentes que suportam o serviço fornecido:

Segue a estrutura organizacional da Ascenty Data Centers e Telecomunicações S/A.

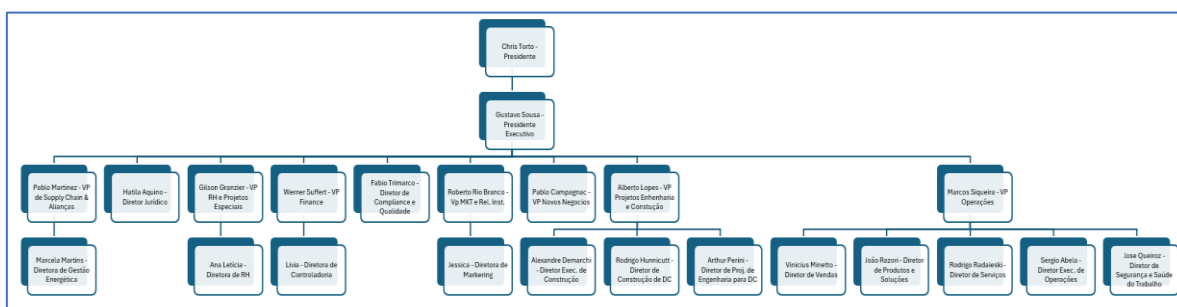


Figura 1: Estrutura Organizacional da Ascenty

Presidente Chris Torto (CEO): Cidadão norte-americano com residência permanente no Brasil desde 1989. Cofundador e CEO da Vivax, a segunda maior operadora de TV a cabo no Brasil. Em 2006, conduziu a abertura de capital da Vivax, que posteriormente foi adquirida pela NET Serviços em 2007. Também esteve à frente da Voyager Inc., de onde conduziu a abertura de capital em 1999 (a empresa foi adquirida por um grupo de telecomunicações norte-americano em 2000). Chris é administrador de empresas pela University of Maine e possui MBA pela Harvard University.

Principais funções: Garantir que a empresa tenha a estratégia certa e os recursos necessários para executá-la. Identificar os mercados mais promissores, aperfeiçoar a organização e os processos, focando nas questões de longo prazo.

Gustavo Henrique Santos de Sousa (Presidente Executivo) - ocupou posições executivas em grandes companhias brasileiras, tendo exercido as posições de CEO e CFO/DRI na Cielo, CFO/DRI na Klabin, CEO e CFO/DRI na CPFL Renováveis, Diretor de Controladoria, Tesouraria, Relações com Investidores e Tributário na Companhia Siderúrgica Nacional e Diretor de Controladoria no Banco do Brasil. Possui MBA pela Columbia Business School, Mestrado em Gestão Econômica de Negócios pela Universidade de Brasília, MBA em Administração Financeira pela Fundação Getúlio Vargas e Graduação em Administração de Empresas na Universidade Federal do Rio Grande do Norte. Na Ascenty atua como Presidente Executivo.

Vice-Presidente (VP) e Diretores:

Gilson Granzier (VP de RH e Projetos Especiais) – Possui ampla experiência na área financeira. Nos últimos treze anos esteve à frente das finanças das empresas Vivax e Buscapé como CFO. Gilson é administrador de empresas pelo Centro Regional Universitário do Espírito Santo do Pinhal e pós-graduado em finanças pela Universidade Metodista de Piracicaba.

Marcos Siqueira (VP de Operações) – Possui ampla experiência em Data Center e Telecomunicações já liderou equipes de Operações, Produtos, Pré-Vendas e Pós-Venda para América Latina em empresas como Global Crossing / Level 3. Na Ascenty, lidera as áreas de Serviços de Data Center e Telecom. É formado em tecnologia e possui MBA Executivo pelo INSPER.

Pablo Campagnac (VP Novos Negócios) - Possui ampla experiência em gestão de vendas e operações. Nos últimos quinze anos, participou do startup da Vivax, onde assumiu as diretorias de vendas e operações. Pablo é economista e possui MBA pela Boston University.

Roberto Rio Branco (VP de Marketing e Relações) – Possui ampla experiência em marketing, vendas e operações. Atuou como diretor operacional da Vivax durante quatro anos e anteriormente como COO da TVA TV por assinatura. Também liderou diversas posições gerenciais na Mesbla, no Banco de Boston e no City Bank. Roberto é administrador de empresas pela Faculdade Moraes Jr.

Werner Romera Suffert (VP Finanças) - Possui ampla experiência em grandes empresas brasileiras listadas na B3 no Novo Mercado, ocupando posições executivas, de conselho de administração, comitê de auditoria e conselho fiscal. Foi CEO e CFO/DRI da BB Seguridade, CFO/DRI do IRB Brasil RE, executivo em diversas diretorias do Banco do Brasil. Foi membro do conselho de administração da BB Seguridade, IRB Brasil RE, Brasilprev e Brasildental. Exerceu ainda posição no Comitê de Auditoria do IRB Brasil RE e Conselho Fiscal na Brasildental. Foi presidente do comitê financeiro da Brasilprev, Brasilcap e Brasilseg. Foi ainda Diretor Geral do BB Paris. Possui Mestrado em Administração de empresas pelo COPPEAD/UFRG, MBA em Negócios Internacionais pela FIPE/USP e graduação em Administração na Universidade de Brasília - UNB.

Alberto Lopes (VP de Projetos, Engenharia e Construção) – Possui ampla experiência no setor de mineração em empresas como Vale, Anglo American e MMX, vivenciando numa primeira fase os processos de operação & manutenção em grandes plantas de tratamento de minérios e, na sequência, gerindo a engenharia & implantação de greenfields de grande porte. Atuou também no setor elétrico em grandes players como CPFL Renováveis e Elera (grupo Brookfield) sempre em posições C-level liderando a implantação de projetos de geração eólica, solar e hidrelétricos. Alberto é graduado em Engenharia Mecânica pela UFPA (Universidade Federal do Pará) e Mestre em Energias Renováveis pela UFC (Universidade Federal do Ceará).

Pablo Bonino (VP de Supply Chain & Alianzas) – Possui ampla experiência com mais de 20 anos no setor de vendas e cadeia de suprimentos, especializado em projetos complexos. Com MBA em Gestão Empresarial pela Anhembi Morumbi e graduação em Processos e Marketing pela mesma instituição, ele possui ampla experiência na América Latina, incluindo Brasil, Argentina, Paraguai, Uruguai e Chile. Sua trajetória inclui posições de liderança na Wesco Anixter, onde supervisionou equipes e otimização de processos, e na Anixter, onde desenvolveu programas de fidelidade e gerenciou grandes contas. Pablo é conhecido por sua habilidade em negociação, gestão de equipes e desenvolvimento de relacionamentos de longo prazo com clientes e parceiros.

Ana Letícia Caressato (Diretora de RH) – Profissional altamente qualificada em Psicologia, Gestão de Pessoas e Coaching Organizacional. Possui ampla experiência em RH, atuando em empresas dos segmentos de agronegócio e farmacêutico. Dentro do RH atua de forma generalista, sendo responsável por todos os subsistemas de RH como: treinamento e desenvolvimento, recrutamento e seleção, folha de pagamento e questões estratégicas da organização.

Alexandre Magalhães (Diretor Executivo de Engenharia e Projetos de DC) – Profissional altamente qualificado com experiência nas áreas de Engenharia Elétrica e Engenharia de Telecomunicações com Graduação em Engenharia Elétrica-Eletrônica/Eletrotécnica. Expertise em implantação de grades projetos e obras de telecomunicações, infraestrutura de telecomunicações e engenharia elétrica. Atuação no desenvolvimento de diversos sistemas telecomunicações e instalações elétricas com ênfase em plataformas petrolíferas, refinarias de petróleo, indústrias químicas e petroquímicas, plantas de fertilizantes, mineração, siderúrgica, geração de energia, papel de celulose, farmacêutica, hospitais, aeroportos, instalações comerciais e ou administrativas e implantação de data centers. Registro e Certificações no CREA-SP como Eng.º Eletricista/Técnico em Eletrotécnica, EM-Projetista CAE Elétrica Prominp/Escola Politécnica POLI-USP, Certificação Integrador Indigo Vision para sistemas de CFTV analógico e sobre IP, formação profissional em cabeamento estruturado FCP Furukawa-Projetista e Instalador, formação profissional em cabeamento estruturado ACT-1 AMP/Tyco Electronics-Projetista, Basic SCS Certificate BICSI Brasil.

Arturo Wheeler (Diretor de Data Center Regional) – Possui ampla experiência liderando equipes altamente eficazes em funções de TI de missão crítica em ambientes globalizados para o México e América Latina. Desenvolveu sua carreira principalmente no setor financeiro com atuação no Citibank, onde foi responsável por diversas áreas de operação e engenharia de Telecomunicações e Data Centers. O executivo também fez parte das equipes de liderança regional das Américas para o banco, onde foi responsável por estabelecer modelos operacionais e transições de equipes locais, regionais e globais por meio das quais foram alcançadas eficiência operacional, melhorias de serviço e redução de custos.

Arthur Perini (Diretor de Engenharia de Data Center) – Possui ampla experiência em Engenharia multidisciplinar, Construção e Operação de Infraestrutura e Energia, Sistemas de Automação e Telecomunicações, Arthur se destaca pela sua profunda expertise e habilidade em liderança de equipes. Antes de se juntar à Ascenty, Arthur construiu uma carreira sólida em empresas de prestígio como Areva Renewable, CPFL Renováveis e Essentia Energia (Pátria Investimentos). Sua experiência inclui a Engenharia, Implantação e Operação de usinas solares, eólicas e hidráulicas, além da liderança em projetos complexos de Subestações e Sistemas de Automação.

Carlos Parra (Diretor de Data Center Regional) – Possui ampla experiência em engenharia elétrica com mais de 20 anos de experiência na indústria de infraestrutura e tecnologia. Começou sua carreira na Associação Colombiana de Engenheiros, um órgão de assessoria técnica ao Governo Nacional. Trabalhou com o Banco Interamericano de Desenvolvimento BID para fortalecer a cadeia de produção da engenharia. Trabalhou durante vários anos no Ministério Colombiano de Tecnologia da Informação e Comunicações em um de seus programas de inclusão tecnológica. Ele participou de diferentes projetos de inovação tecnológica com o Estado, bancos alternativos (Fintech) e empresas privadas.

Hatila de Aquino (Diretor Jurídico) – Profissional altamente qualificado em Direito Empresarial, direito tributário e infraestrutura, possui ampla experiência na liderança de departamentos jurídicos, atuando diretamente nas áreas de Infraestrutura, energia e telecomunicações. Antes de iniciar suas atividades na Ascenty, passou por empresas como CPFL Energia, Pátria Investimentos e SIIF Energies do Brasil, atuando na implantação de diversos projetos como concessões de rodovias, transporte por embarcações, datacenters, **usinas solares, eólicas e hidráulicas**, além de ter gerido vários M&A's do mercado, IPO's, reorganizações societárias e captações de dívidas.

Jéssica Braga (Diretora de Marketing) – Possui ampla experiência e atuação nas áreas de marketing e comunicação de grandes empresas. Foi responsável por conduzir todo o processo de posicionamento da Ascenty no mercado, desde a sua entrada como uma startup, até os dias de hoje como líder no segmento. Com formação em Comunicação Social, possui pós-graduação e MBA em marketing pela FGV

José Carlos Marques Queiroz (Diretor de Segurança e Saúde do Trabalho) – Possui ampla experiência em segurança do trabalho em ambiente de TI, possuindo formação pela universidade Unicamp –(Campinas) em engenharia de segurança do trabalho.

Livia Agessi Gonçalves (Diretora de Controladoria) – Possui ampla experiência na área contábil, tributária e financeira em empresas de grande porte e consultoria. Foi responsável pelas demonstrações financeiras em IFRS e BACEN GAAP de mais de 30 divulgações de resultado de empresa de capital aberto, com liderança técnica no relacionamento com auditores independentes e órgãos reguladores. Possui formação em administração pública e contabilidade na UNESP e PUC-SP, respectivamente, e MBA Executivo em Finanças pelo INSPER.

Marcela Martins (Diretora de Controladoria) – Possui ampla experiência no setor de energia elétrica, Marcela é uma especialista em comercialização e geração de energias renováveis. Ela possui um MBA em Gestão Empresarial pela FGV e é graduada em Engenharia de Produção Civil pela UTFPR. Sua trajetória inclui passagens por importantes empresas como Auren Energia, 2W Energia, CPFL Renováveis, AES Tietê e Tradener, onde atuou em áreas cruciais como planejamento energético, gestão de energia, portfólio, middle office e pós-vendas. Na Ascenty, ela lidera a área de Gestão Energética, garantindo soluções eficazes e sustentáveis para o desenvolvimento e otimização das nossas operações energéticas.

Rodrigo Radaieski (Diretor de Serviços) – Possui ampla experiência no mercado de Internet e Data Center nestes segmentos desde o seu surgimento no Brasil. Com sólida carreira como gestor em áreas de TI com foco na prestação de serviços. Possui formação em informática pela universidade católica do Rio Grande do Sul.

Rodrigo Hunnicutt (Diretor de Construção de DC) – Possui ampla experiência em implantação de projetos de infraestrutura de Data Center na modalidade “Built to Suit” e em terrenos próprios Ascenty. Gerenciou a construção de vários data Center no Brasil e Mexico. Tem larga experiência em elaboração de projetos, planejamento, gerenciamento e construção. É graduado em arquitetura desde 1991 e possui MBA em Tecnologia e Gestão da Produção de Edifícios” pela Politécnica da USP.

Sergio Abela (Diretor de Operações) – Possui ampla experiência em infraestrutura de Data Center, gerenciando projetos de infraestrutura da Ascenty. Possui formação de engenheiro civil pela universidade de São Paulo.

João Walter (Diretor de Produtos e Soluções) – Possui ampla experiência no mercado de Data Center e Telecomunicações há mais de 20 anos. Em sua carreira, passou por grandes empresas do segmento e iniciou a sua trajetória na Ascenty em 2013 com o objetivo de reforçar o time de Arquitetura de Soluções. Durante esses anos, o executivo assumiu novos desafios e hoje lidera os times de Produtos e Arquitetura de Soluções.

Vinicius Camiloti Minetto (Diretor de Vendas) – Possui ampla experiência no mercado de Data Center e Telecomunicações, onde atua há mais 15 anos. Atuou em grandes players do mercado nacional e ingressou na Ascenty em 2012, reforçando a equipe comercial. Graduado e Pós-

Graduado pela FATEC e com MBA em Gestão Comercial pela Fundação Getúlio Vargas (FGV). Na Ascenty é responsável pelo time Comercial, de Arquitetura de Soluções e Produtos.

Principais funções: Conduzir a elaboração e implementação dos planos estratégicos e operacionais, em todas as áreas da empresa, visando a assegurar o seu desenvolvimento, crescimento e continuidade. Identificar oportunidades, avaliar a viabilidade e fazer recomendações sobre novos investimentos ou desenvolvimento de novos negócios, visando a garantir um retorno adequado aos acionistas, resguardar a segurança dos ativos da empresa e garantir que as ações tomadas não causem impactos significativos no meio Sistema. Manter contatos com a direção das empresas clientes para identificar oportunidades de ampliação ou melhoria nos produtos / serviços prestados ou solução de eventuais problemas contratuais ou operacionais, visando manter a satisfação do cliente e projetar uma imagem positiva da empresa no mercado. Conduzir os processos de mudanças na cultura da organização, visando conquistar o engajamento de todos os seus integrantes e garantir a consolidação de uma cultura organizacional orientada para a contínua busca da qualidade e de altos padrões de desempenho individual e coletivo.

Os Vice-presidentes e Diretores da Ascenty está plenamente comprometida com o código de conduta, incentivando um Sistema ético e transparente, exigindo o cumprimento das normas e leis.

Compliance e Qualidade

Fábio Trimarco (Diretor de Compliance e Qualidade) – Possui ampla experiência em TI, passado pelas áreas de desenvolvimento, planejamento e operação, sendo os últimos 10 anos com foco na governança corporativa de TI, Bacharel em ciências da computação e MBA em governança de TI pelo Universidade de Ensino de São Caetano do Sul e extensão da graduação em Compliance Empresarial pela PUC. Atualmente responsável pelo departamento de Compliance e Qualidade da Ascenty, com foco na ética, conduta e qualidade embasada na implementação e gestão de normas e certificações como ISOs 9001 gestão da qualidade, 14001 gestão ambiental, 20000-1 gestão dos serviços de TI, 22301 gestão de continuidade de negócios, 27001\27701 gestão da segurança da informação\gestão da privacidade de dados, 37001\37301 gestão antissuborno\gestão de compliance, 45001 gestão saúde e segurança do trabalho, 50001 gestão energética, PCI DSS, SOC, UPTIME TIER III e TÜV TR3 (TIA942).

Principais funções: A Função de Compliance foi estabelecida com autoridade e independência dentro da organização com livre acesso aos executivos e acionistas para o desempenho de sua função. É área representante que gere os sistemas de gestão e demais certificações implementadas na empresa, assegurando que:

- Os objetivos estejam alinhados com a realidade;
- O desempenho e as oportunidades de melhoria sejam relatados a alta direção;
- Desenvolver e manter os processos padronizados de entrega de serviços em linha com as recomendações de melhores práticas do ITIL, CobiT e PMI em linha com as ofertas;
- Verificar a eficiência e eficácia da utilização dos processos nos departamentos;
- Prover treinamento e melhoria contínua dos processos para toda a empresa;
- Notificar e orientar a correta operação quando verificado o desvio do processo escrito;
- Gerenciar o programa de melhoria contínua de processos;
- Gerenciar auditorias internas visando garantir aderência aos processos certificados;
- Identificar e propor novas ferramentas de gestão de serviço, quando aplicável; e,
- Manter os processos alinhados com as certificações.

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/2A80-C293-C965-6220>.

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

Código para verificação: 2A80-C293-C965-6220



Hash do Documento

E4C8541499DAB252C71AC8A9747A2F6FF8AB03E86FDE6B977D974C994E298F61

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 11:50 UTC-03:00

Tipo: Assinatura Eletrônica

Identificação: Por email: dcarra@kpmg.com.br; Código de acesso: 1418096

Evidências

Client Timestamp Tue Jan 28 2025 11:50:03 GMT-0300 (Brasilia Standard Time)

Geolocation Location not shared by user.

Email dcarra@kpmg.com.br

IP 10.201.227.202

Assinatura:



Hash Evidências:

99B95BF7EA15CB7FD09EA0D22CEFDEF47C63D9854052D3CB299BCFCEAABAFD25