



Ascenty Data Centers e Telecomunicações S/A

Relatório de Asseguração dos Auditores Independentes sobre a
descrição, o desenho e a efetividade operacional dos Controles de
acesso físico, manutenção e operação de Data Centers (Facilities)

SOC 1 - Tipo 2

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



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 D05E-41D8-86F8-8681.

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 D05E-41D8-86F8-8681.

Índice

Seção I	3
Seção II	8
Seção III	11
Seção IV	26
Seção V	40

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 D05E-41D8-86F8-8681.

Seção I

Relatório de Asseguração dos Auditores Independentes



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 D05E-41D8-86F8-8681.



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”) descrita na Seção III, sobre os Controles de acesso físico, manutenção e operação de Data Centers (Facilities) durante o período de 1º de janeiro a 31 de dezembro de 2024 (“descrição”), e sobre o desenho e a efetividade operacional dos controles relacionados com os objetivos de controle especificados nessa descrição.

Essa descrição considera que certos objetivos de controle especificados 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 fazem parte da nossa avaliação dos Controles de acesso físico, manutenção e operação de Data Centers (Facilities) relacionados aos processos de prestação de serviços 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 eficácia 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 organização prestadora de serviços Ascenty é responsável por: (i) elaborar a descrição e a correspondente afirmação nas Seções II e III, incluindo a integridade, a precisão e o método de apresentação da descrição e da afirmação; (ii) prestar os serviços incluídos na descrição da Seção III; (iii) especificar os objetivos de controle; e (iv) desenhar, implementar e operacionalizar os controles de maneira efetiva para alcançar os objetivos de controle especificados.

Nossa Independência e Controle de Qualidade

Cumprimos com os requisitos de independência e outros requisitos éticos do Conselho Federal de Contabilidade – CFC, baseados nos princípios fundamentais de integridade, objetividade, competência e zelo profissional, confidencialidade e comportamento profissional.

A KPMG Assurance Services Ltda. (“KPMG”) aplica a Norma Brasileira de Gestão de Qualidade (NBC PA 01), que requer que a firma planeje, implemente e opere um sistema de gestão de qualidade, incluindo políticas ou procedimentos relacionados com o cumprimento de requerimentos éticos, normas profissionais e exigências legais e regulatórias aplicáveis.

Responsabilidade dos Auditores Independentes

Nossa responsabilidade é a de expressar uma opinião sobre o desenho e a efetividade operacional dos controles relacionados com os objetivos de controle especificados na descrição, elaborada pela organização prestadora de serviços Ascenty, com base em nossos procedimentos. Conduzimos nosso trabalho de acordo com a Norma Brasileira de Contabilidade NBC TO Nº 3402 – Relatórios de Asseguração de Controles em Organização Prestadora de Serviços, emitida pelo Conselho Federal de Contabilidade (CFC), sua equivalente internacional ISAE 3402 – *International Standard on Assurance Engagements*, emitida pelo *International Auditing and Assurance Standards Board* (IAASB), e sua equivalente americana SSAE Nº 18 – *Statement on Standards for Attestation Engagements*, emitida pelo *American Institute of Certified Public Accountants*. Essas normas requerem o cumprimento de exigências éticas pelos auditores e que o trabalho seja planejado e executado para a obtenção de segurança razoável sobre se a descrição está apresentada adequadamente, em todos os aspectos relevantes, e se os controles foram apropriadamente desenhados e estão operando efetivamente.



Um trabalho de asseguuração para emitir um relatório sobre a descrição, o desenho e a efetividade operacional dos controles da organização prestadora de serviços envolve a execução de procedimentos selecionados para obtenção de evidência sobre as divulgações na descrição do seu sistema, desenho e efetividade operacional dos controles. Os procedimentos selecionados dependem do julgamento do auditor, incluindo a avaliação dos riscos de que a descrição não esteja apresentada adequadamente e de que os controles não foram apropriadamente desenhados ou não estão operando efetivamente. Nossos procedimentos incluíram testes da efetividade operacional dos controles que consideramos necessários para fornecer segurança razoável de que os objetivos de controle especificados na descrição foram alcançados. Um trabalho de asseguuração desse tipo inclui, também, a avaliação dos objetivos de controle da descrição, da adequação dos objetivos nela especificados e da adequação dos critérios especificados pela organização prestadora de serviços e descritos na Seção III.

Acreditamos que a evidência obtida é suficiente e apropriada para fundamentar nossa opinião.

Limitações de controles na organização prestadora de serviços

A descrição, elaborada pela organização prestadora de serviços Ascenty, foi elaborada para atender às necessidades comuns de ampla gama de clientes e de seus auditores independentes e, portanto, pode não incluir todos os aspectos do sistema que cada cliente possa considerar importante em seu próprio ambiente específico. Além disso, devido à sua natureza, os controles da organização prestadora de serviços podem não prevenir ou detectar todos os erros ou omissões no processamento ou no relato das transações. Ainda, a projeção de qualquer avaliação da efetividade operacional para períodos futuros está sujeita ao risco de que os controles em uma organização prestadora de serviços podem se tornar inadequados ou falharem.

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 de acesso físico, manutenção e operação de Data Centers (Facilities) 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 objetivos de controle 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 objetivos de controle 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 testados e a natureza, a época e os resultados desses testes estão relacionados na Seção IV.

Usuários previstos e objetivo

Este relatório e a descrição dos testes de controle na Seção IV são destinados exclusivamente aos clientes que utilizaram os Controles de acesso físico, manutenção e operação de Data Centers (Facilities) relacionados aos processos de prestação de serviços da Ascenty e seus auditores independentes, que possuem entendimento suficiente para considerá-los, em conjunto com outras informações, incluindo aquelas sobre controles operacionalizados pelos próprios clientes, na avaliação dos riscos de distorções relevantes nas suas demonstrações contábeis.

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

A descrição (Seção 3) foi elaborada para clientes que usaram os Controles de acesso físico, manutenção e operação de Data Centers (Facilities) e seus auditores que têm entendimento suficiente para considerar a descrição, juntamente com outras informações sobre controles operacionalizados pelos próprios clientes, na avaliação dos riscos de distorções relevantes nas demonstrações contábeis de clientes. A Ascenty Data Centers e Telecomunicações S/A confirma que:

- a) a descrição da Seção III apresenta adequadamente os Controles de acesso físico, manutenção e operação de Data Centers (Facilities) para processamento de transações de clientes durante o período de 1º de janeiro a 31 de dezembro de 2024. Os critérios usados na elaboração dessa afirmação foram que a descrição:
 - i. apresenta como o sistema foi projetado e implementado, incluindo:
 - os tipos de serviços prestados, incluindo, conforme apropriado, as classes de transações processadas;
 - os procedimentos dos sistemas de tecnologia da informação (TI) e manuais, usados para iniciar, registrar, processar, corrigir conforme necessário e transferir essas transações para os relatórios elaborados para clientes;
 - os respectivos registros contábeis, informações de suporte e contas específicas que foram usadas para iniciar, registrar, processar e comunicar as transações, incluindo a correção de informações e como as informações foram transferidas para os relatórios elaborados para clientes;
 - como o sistema tratou de eventos e condições significativos que não eram transações;
 - o processo usado para elaborar relatórios para clientes;
 - os objetivos de controle relevantes e os controles projetados para alcançar esses objetivos;
 - os controles que, no projeto do sistema, seriam implementados por entidades 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 o processamento e a comunicação de transações de clientes;
 - ii. inclui detalhes relevantes de mudanças nos Controles de acesso físico, manutenção e operação de Data Centers (Facilities) da organização prestadora de serviços durante o período de 1º de janeiro a 31 de dezembro de 2024;
 - iii. não omite ou distorce informações relevantes para o alcance dos Controles de acesso físico, manutenção e operação de Data Centers (Facilities) que estão sendo descrito, apesar de saber que a descrição foi elaborada para atender as necessidades comuns de ampla gama de clientes e seus auditores e, portanto, pode não incluir todos os aspectos do sistema que cada cliente individualmente possa considerar importante em seu próprio ambiente específico;
- b) os controles relacionados com os objetivos de controle especificados na descrição foram adequadamente projetados e operaram de maneira efetiva durante o período de 1º de janeiro a 31 de dezembro de 2024. Os critérios usados na elaboração dessa afirmação foram que:
- i. os riscos que ameaçaram o alcance dos objetivos de controle especificados na descrição foram identificados;
 - ii. 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
 - iii. os controles foram aplicados de maneira uniforme conforme projetados, incluindo que foram aplicados controles manuais por pessoas com competência e autoridade adequadas, durante o período de 1º de janeiro a 31 de dezembro de 2024.

DocuSigned by:



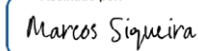
461CD50EE4D1424...

Fabio Trimarco

Diretor de Compliance e Qualidade

Ascenty Data Centers e Telecomunicações S/A

Assinado por:



6842EE54AA9248D...

Marcos Siqueira

VP de Operações

Ascenty Data Centers e Telecomunicações S/A

Seção III

Descrição elaborada pela
Organização Prestadora de
Serviços



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 (QRO11), inaugurado em junho de 2022;
22. Na cidade de Querétaro/México (QRO22), inaugurado em junho de 2022;
23. Na cidade de Hortolândia/SP (HTL5), inaugurado em setembro de 2022; e
24. Na cidade de Osasco/SP (SP4), inaugurado em junho de 2023.

Compromisso e requisitos junto aos clientes

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

Escopo do Relatório

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

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

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

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

Gerenciamento de Acesso Físico ao Data Center.

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

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

Controle de Concessão de Acesso

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

O processo de concessão de acessos para funcionários está detalhado na política de acessos ao Data Center “POL-SE-0001 - Política de Segurança Física”, no procedimento

“PRC-SE-0001 - Procedimento Acesso Físico ao DC”, neste último caso discriminamos os principais passos abaixo:

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

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

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

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

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

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

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

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

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

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

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

Revogação de Acessos ao Data Center

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

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

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

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

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

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

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

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

Revisão periódica dos acessos ao Data Center

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

Gerenciamento de organização e sinalização do Data Center

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

Gerenciamento de Facilities e Gerenciamento de Mudanças.

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

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

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

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

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

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

1. IF-0002 - Manual de Infraestrutura – 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 (CL) 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; e,
- PRC-ST-0025(BR) - Plano de Atendimento a Emergência – Hortolândia;
- 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 “PROFN-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.

Descritivo dos controles

Objetivo dos Controles: Os controles da Ascenty devem prover segurança razoável de que apenas pessoas autorizadas possuem acesso aos ambientes restritos do Data Center.	
#	Descrição do controle especificado pela organização prestadora de serviços
ASC.1.1	Os acessos aos ambientes críticos do Data Center são controlados por dispositivo único de acesso de dupla identificação (crachá e biometria).
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.1.5	Semestral 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.
ASC.1.6	Trimestral é realizado um processo de revisão de acessos de terceiros ao Data Center. Esta revisão é formalizada na ferramenta Service Now, onde são listados todos os terceiros com acesso ativo, e o responsável pela área de Acesso e Monitoramento revisa e solicita qualquer ajuste de acesso necessário.
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.1.8	Os ambientes do Data Center possuem sinalizações de regras / avisos claras, objetivas e de fácil acesso a todas acessando o ambiente.

Objetivo dos Controles: Os controles devem prover segurança razoável de que os diferentes tipos de equipamentos no Data Center tenham requisitos específicos de instalação e são adequadamente geridos quanto à instalação, manutenção e retirada do Data Center.

#	Descrição do controle especificado pela organização prestadora de serviços
ASC.2.1	Para as instalações de equipamentos de clientes e facilities é realizado a criação de um ticket na ferramenta Service Now com a descrição do que será realizado, o período necessário e responsável pela atividade. O Data Center possui espaço físico sinalizado adequadamente para realização de recebimento de materiais.
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.2.3	Para as desinstalações ou retiradas de equipamentos do Data Center é realizado a criação de um ticket na ferramenta Service Now com a descrição do que será realizado, o período necessário e o responsável pela atividade.
ASC.2.4	Anualmente é realizado um processo de inventário de todos os equipamentos do Data Center. Este processo é registrado através de um ticket na ferramenta de ITSM

Objetivo dos Controles: Os controles devem prover razoável segurança de que existam requerimentos de gerenciamento de energia, equipamentos no Data Center.

#	Descrição do controle especificado pela organização prestadora de serviços
ASC.3.1	Mensalmente a equipe de controle Técnico do Data Center emite um relatório de consumo de energia para todos os Diretores da companhia de forma a assegurar que os recursos de energia estão sendo devidamente utilizados e gerenciados.
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.

Objetivo dos Controles: Os controles devem prover razoável segurança de que o Data Center seja mantido em níveis corretos para otimização das operações de TI.

#	Descrição do controle especificado pela organização prestadora de serviços
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.4.3	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.
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.

Objetivo dos Controles: Os controles devem prover razoável segurança de que sejam estabelecidas normas de segurança.

#	Descrição do controle especificado pela organização prestadora de serviços
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

Objetivo dos Controles: Os controles devem prover razoável segurança para o recebimento e entrega de dispositivos.

#	Descrição do controle especificado pela organização prestadora de serviços
ASC.7.1	Os contratos com empresas terceiras /prestadores de serviço críticos do Data Center são devidamente gerenciadas de forma que os SLAs, vencimentos e serviços acordados são monitorados verificando se estão de acordo com o contratado.

Objetivo dos Controles: Os controles devem suportar às práticas de segurança dos dados e informações sigilosas.

#	Descrição do controle especificado pela organização prestadora de serviços
ASC 8.2	Testes quanto a tentativas de intrusão aos sistemas de controle de acesso físico ao Data Center e CFTV, são realizados periodicamente pelo time de segurança da Ascenty.

Seção IV

Objetivos de Controle, Controles
Relacionados, Teste de Desenho
e de Efetividade 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.

Objetivo dos Controles: Os controles da Ascenty devem prover segurança razoável de que apenas pessoas autorizadas possuem acesso aos ambientes restritos do Data Center.

#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
ASC.1.1	Os acessos aos ambientes críticos do Data Center são controlados por dispositivo único de acesso de dupla identificação (crachá e biometria).	<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 nos Data Centers em escopo, a fim de observar se os acessos aos ambientes críticos somente podem ser realizados mediante dupla autenticação (crachá e biometria).</p>	Não identificamos exceções.
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.	<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.



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.	Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleções de revogações de acesso aos Data Centers, a fim de observar os chamados foram tempestiva e devidamente registrados na ferramenta de ITSM.	Não identificamos exceções.
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.	Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de concessões de acesso a visitantes aos Data Centers, a fim de observar os chamados foram devidamente registrados na ferramenta de ITSM.	Não identificamos exceções.
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.	Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de semestre, para os quais foi solicitada documentação suporte para cada um dos data centers, a fim de observar se as revisões de acesso foram realizadas e, se necessário, as ações corretivas foram tomadas.	Não identificamos exceções.
ASC.1.6	Trimestralmente é realizado um processo de revisão de acessos de terceiros ao Data Center. Esta revisão é formalizada na ferramenta Service Now, onde são listados todos os terceiros com acesso ativo, e o responsável pela área de Acesso e Monitoramento revisa e solicita qualquer ajuste de acesso necessário.	Indagação aos responsáveis pelo processo de gestão de acesso aos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de trimestres vs Data Centers, para os quais foi solicitada documentação suporte, a fim de observar se as revisões de acesso de terceiros foram realizadas e, se necessário, as ações corretivas foram tomadas.	Não identificamos exceções.



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	<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.
ASC.1.8	Os ambientes do Data Center possuem sinalizações de regras / avisos claras, objetivas e de fácil acesso a todas acessando o ambiente.	<p>Indagação aos responsáveis pela sinalização 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 as sinalizações foram dispostas adequadamente, com regras e avisos objetivos e de fácil visualização.</p>	Não identificamos exceções.

Objetivo dos Controles: Os controles devem prover segurança razoável de que os diferentes tipos de equipamentos no Data Center tenham requisitos específicos de instalação e são adequadamente geridos quanto à instalação, manutenção e retirada do Data Center.

#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
ASC.2.1	Para as instalações de equipamentos de clientes e facilities é realizado a criação de um ticket na ferramenta Service Now com a descrição do que será realizado, o período necessário e responsável pela atividade. O Data Center possui espaço físico sinalizado adequadamente para realização de recebimento de materiais.	<p>Indagação aos responsáveis pela gestão de acesso Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Inspecção dos Data Centers, a fim de observar o as sinalizações foram dispostas adequadamente, com regras e avisos objetivos e de fácil visualização.</p> <p>Seleção de entregas de material, a fim de observar se os chamados na ferramenta de ITSM foram devidamente registrados e encerrados.</p>	Não identificamos exceções.
ASC.2.2	Anualmente é realizada 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.	<p>Indagação aos responsáveis pela manutenção dos equipamentos de Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia.</p> <p>Seleção de manutenções planejadas e emergenciais, a fim de observar se foram realizadas conforme cronograma parametrizado no ServiceNow.</p>	Não identificamos exceções.



ASC.2.3	Para as desinstalações ou retiradas de equipamentos do Data Center é realizado a criação de um ticket na ferramenta Service Now com a descrição do que será realizado, o período necessário e o responsável pela atividade.	Indagação aos responsáveis pela gestão de acesso Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de retiradas de material, a fim de observar se os chamados na ferramenta de ITSM foram devidamente registrados e encerrados.	Não identificamos exceções.
ASC.2.4	Anualmente é realizado um processo de inventário de todos os equipamentos do Data Center. Este processo é registrado através de um ticket na ferramenta de ITSM	Indagação aos responsáveis pela gestão de inventários, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de Data Centers, para a qual foi solicitada documentação suporte referente à revisão anual de inventário, a fim de observar se foram devidamente registradas e encerradas.	Não identificamos exceções.

Objetivo dos Controles: Os controles devem prover razoável segurança de que existam requerimentos de gerenciamento de energia, equipamentos no Data Center.			
#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
ASC.3.1	Mensalmente a equipe de controle Técnico do Data Center emite um relatório de consumo de energia para todos os Diretores da companhia de forma a assegurar que os recursos de energia estão sendo devidamente utilizados e gerenciados.	Indagação aos responsáveis pelo gerenciamento do consumo de energia, 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 relatórios de consumo de energia foram devidamente confeccionados e disponibilizados.	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 para os quais foram solicitados contratos com fornecedores de energia, a fim de observar se estes dispunham dos requisitos necessários pela companhia, tais como a manutenção preventiva e o fornecimento de energia.	Não identificamos exceções.



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.	Indagação aos responsáveis pelo gerenciamento dos equipamentos de fornecimento de energia em redundância, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos consoles de monitoramento dos equipamentos de energia, a fim de observar se estão funcionando em redundância.	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 D05E-41D8-86F8-8681.

Objetivo dos Controles: Os controles devem prover razoável segurança de que o Data Center seja mantido em níveis corretos para otimização das operações de TI.			
#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
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.	Indagação aos responsáveis pelo gerenciamento dos equipamentos de refrigeração, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos Data Centers, a fim de observar se estes possuem equipamentos de ar condicionado e de monitoramento de qualidade, umidade e de temperatura.	Não identificamos exceções.
ASC.4.2	O Data Center possui mecanismos de detecção de incêndio (sensores de fumaça) com acionamento precoce de incêndio.	Indagação aos responsáveis pelo gerenciamento dos equipamentos de detecção de incêndio, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos Data Centers, a fim de observar se estes possuem equipamentos de detecção de incêndio.	Não identificamos exceções.
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.



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.	Indagação aos responsáveis pelo cabeamento dos Data Centers, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos Data Centers, a fim de observar o cabeamento foi feito respeitando a segregação entre cabos de dados e de energia.	Não identificamos exceções.
----------------	--	--	-----------------------------



Objetivo dos Controles: Os controles devem prover razoável segurança de que sejam estabelecidas normas de segurança.			
#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
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	Indagação aos responsáveis pelo plano de evacuação, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção de normativos internos, a fim de observar se as diretrizes para execução de evacuação estão devidamente formalizados. Seleção de Data Centers para os quais foi solicitada documentação suporte referente aos simulados de evacuação, a fim de observar se foram devidamente documentados.	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 D05E-41D8-86F8-8681.



Objetivo dos Controles: Os controles devem prover razoável segurança para o recebimento e entrega de dispositivos.

#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
ASC.7.1	Os contratos com empresas terceiras /prestadores de serviço críticos do Data Center são devidamente gerenciadas de forma que os SLAs, vencimentos e serviços acordados são monitorados verificando se estão de acordo com o contratado.	Indagação aos responsáveis pela gestão de contratos, a fim de inspecionar o desenho do controle adotado pela companhia. Inspeção dos contratos vigentes para os fornecedores escopo, a fim de observar se estes estão devidamente providos de cláusulas de SLA. Seleção de meses a fim de observar se a avaliação dos fornecedores escopo quanto ao atendimento foi realizada e documentada.	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 D05E-41D8-86F8-8681.



Objetivo dos Controles: Os controles devem suportar às práticas de segurança dos dados e informações sigilosas.

#	Descrição do controle especificado pela organização prestadora de serviços	Procedimentos aplicados pela KPMG sobre o teste do projeto e da eficácia operacional do controle	Resultados dos testes
ASC 8.2	Testes quanto a tentativas de intrusão aos sistemas de controle de acesso físico ao Data Center e CFTV, são realizados periodicamente pelo time de segurança da Ascenty.	Indagação aos responsáveis pela gestão de acesso físico aos data centers, a fim de inspecionar o desenho do controle adotado pela companhia. Seleção de data centers, para os quais foi inspecionada documentação suporte, a fim de observar se os testes anuais realizados por meio de simulação foram devidamente realizados e registrados.	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 D05E-41D8-86F8-8681.

Seção V

Outras informações fornecidas pela Organização
Prestadora de Serviços



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.

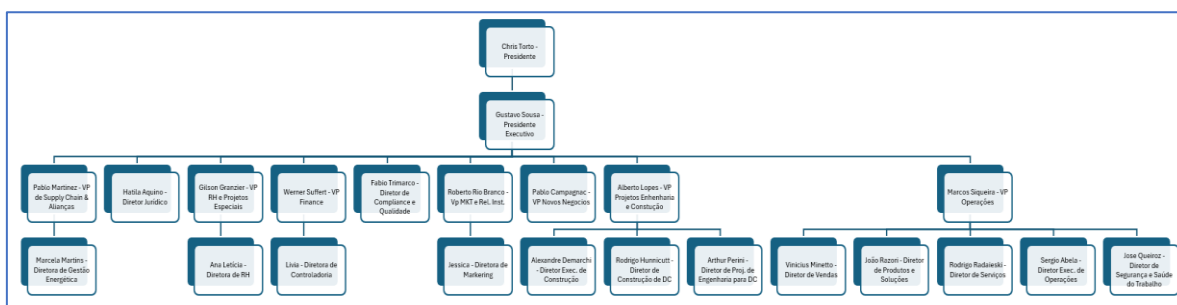


Figura 1: Estrutura Organizacional da Ascenty

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 & Alianças) – 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/D05E-41D8-86F8-8681>.

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

Código para verificação: D05E-41D8-86F8-8681



Hash do Documento

3B6A955CED085F6FEBED1ECEEAF896E33CABC632ECF60E06049E5142D82534F6

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 15:10 UTC-03:00

Tipo: Assinatura Eletrônica

Identificação: Por email: dcarra@kpmg.com.br; Código de acesso: 1418095

Evidências

Client Timestamp Tue Jan 28 2025 15:10:31 GMT-0300 (Brasilia Standard Time)

Geolocation Location not shared by user.

Email dcarra@kpmg.com.br

IP 10.201.227.202

Assinatura:



Hash Evidências:

5E72BE9F504877441782BC0C2A150333E99147EC1106D3D6B655D017D6459E50