DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Building a better working world

Semantix
Relatório SOC 2 Tipo 2

System Organization Controls Report sobre os Critérios de *Trust Services* para as categorias de Segurança (TSP Seção 100 - 2017)

Relatório SOC 2 Tipo 2 realizado por auditoria independente sobre os controles relacionados à segurança e à integridade da Trust Services de Segurança da informação, para a Semantix Tecnologia em Sistema de Informação S.A. (Service Organization)

01/01/2022 à 30/09/2022

Building a better working world

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Sumário

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Seção 1: Declaração da Administração da Semantix Tecnologia em Sistema de Informação S.A.

Afirmação da Administração Semantix Tecnologia em Sistema de Informação S.A.

29 de Dezembro de 2022

Preparamos a documentação sobre os critérios de Trust Services de Segurança da informação (Descrição), para a Semantix Tecnologia em Sistema de Informação S.A. (Organização de Serviço), de acordo com os critérios para a descrição do Sistema (processos, pessoas e ferramentas) de uma organização prestadora de serviços estabelecidos na *Description Criteria DC* (Critérios de Descrição) seção *200* do documento *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Critério de descrição). A Descrição do Sistema tem o intuito de fornecer aos usuários do relatório informações do sistema SDP (Semantix Data Plataform) que podem ser úteis na avaliação de riscos da operação do Sistema (processos, pessoas e ferramentas) no período de 01 de Janeiro a 30 de Setembro de 2022, em particular, informações sobre os controles da Semantix Tecnologia em Sistema de Informação S.A. desenhados, implementados e em operação neste período, a fim de prover segurança razoável que seus requerimentos enquanto prestadora de serviço e requisitos do Sistema foram alcançados no período referido, com base no critério de segurança estabelecidos na *TSP* seção *100* do documento *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

A Semantix Tecnologia em Sistema de Informação S.A. se utiliza de serviços do GCP (Google Cloud Platform), para hospedar os serviços de cloud do SDP. A descrição do Sistema inclui apenas os controles da Semantix Tecnologia em Sistema de Informação S.A. e exclui os controles da GCP. A descrição também indica que determinados critérios de confiança dos serviços especificados pela GCP só podem ser atendidos se os controles assumidos pela Semantix Tecnologia em Sistema de Informação S.A. estiverem adequadamente desenhados e operando de maneira eficaz, juntamente com os controles relacionados a organização de serviço. A descrição do sistema, portanto não se estende aos controles de responsabilidade do GCP.

Controles de Entidade Complementares: A descrição do sistema também indica que determinados critérios de confiança dos serviços especificados na descrição, só podem ser atendidos se os controles de entidade complementares assumidos pela Semantix Tecnologia em Sistema de Informação S.A., estiverem adequadamente desenhados e operando de maneira eficaz, juntamente com os controles relacionados a organização de serviço. A descrição não se estende aos controles de responsabilidade de entidades.

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Portanto, declaramos como verdadeiro o seguinte:

a. A descrição do Sistema apresenta os respectivos controles desenhados, implementados no período de 01 de janeiro a 30 de setembro de 2022, de acordo com o critério de descrição.

b. Os controles apresentados na descrição do sistema, no período de 01 de janeiro a 30 de setembro de 2022, estavam adequadamente desenhados e implementados para fornecer segurança razoável, de que os compromissos de serviços e requisitos de sistema foram alcançados com base nos critérios de segurança, caso o controle opere conforme descrito, e as entidades aplicaram os controles de entidade complementares e a organização de subserviço aplicou os controles assumidos no desenho de controle da Semantix Tecnologia em Sistema de Informação S.A.

Leonardo Santos Poca D Agua
CEO
CNPJ: 09.162.524/0001-53

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Seção 2: Opinião dos auditores

Relatório tipo 2 de Asseguração independente sobre os critérios de *Trust Services* de segurança no processamento de dados da Semantix Tecnologia em Sistema de Informação S.A..

Escopo

Examinamos a documentação sobre a descrição, o qual a Semantix Tecnologia em Sistema de Informação S.A. é responsável pelo desenho e eficácia operacional dos critérios da Trust Services de segurança a informação do sistema SDP (Semantix Data Platform), no período de 01 de janeiro a 30 de Setembro de 2022, de acordo com os critérios de uma organização prestadora de serviços estabelecidos no *Description Criteria DC* - seção 200 do documento *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Descrição dos Critérios) e a aptidão do desenho dos controles inclusos na descrição de 01 de Janeiro a 30 de Setembro de 2022. Nossas análises foram realizadas a fim de prover asseguração razoável que seus requerimentos enquanto prestadora de serviço e requisitos de Sistema (processos, pessoas e ferramentas) foram alcançados com base nos critérios de segurança, estabelecidos na TSP seção 100 do documento *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Os demais critérios de Disponibilidade, Processamento, Integridade, Confidencialidade e Segurança não fazem parte do escopo aqui avaliado.

A Semantix Tecnologia em Sistema de Informação S.A. utiliza serviços do GCP (Google Cloud Platform) – Organização de Subserviço, que fornece a hospedagem dos serviços de Cloud do GCP. A Descrição indica que os controles complementares da organização subcontratada efetivamente desenhados e operando são necessários, juntamente aos controles da Semantix Tecnologia em Sistema de Informação S.A., para que a Semantix Tecnologia em Sistema de Informação S.A. atinja seus requerimentos enquanto prestadora de serviço e requisitos de Sistema com base nos critérios de segurança. A descrição do Sistema da Semantix Tecnologia em Sistema de Informação S.A., apresenta aspectos sobre o ambiente de controles relevantes; e que os tipos de controles complementares desenhados e implementados pela GCP, estão adequadamente desenhados, implementados e em operação no período de 01 de janeiro a 30 de setembro de 2022. Nossa asseguração não se estende aos serviços prestados pela GCP e não avaliamos se a gestão de controles que foram assumidos foi implementada ou se tais controles estão adequadamente desenhados e operando efetivamente na no período de 01 de janeiro a 30 de setembro de 2022.

Controles de Entidade Complementares: A descrição também indica que os controles da Semantix Tecnologia em Sistema de Informação S.A. podem fornecer uma garantia de que o compromisso de serviço e os requerimentos do sistema podem ser alcançados apenas se os controles de entidade complementares forem assumidos no desenho dos controles da Semantix Tecnologia em Sistema de Informação S.A., sendo adequadamente desenhados e implementados, juntamente com os controles relatados

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

pela organização de serviço. Nossa análise não se estende aos controles de entidade complementares, e não avaliamos se os desenhos ou a eficácia da operação desses controles de entidade complementares estão adequados.

Responsabilidades da Semantix Tecnologia em Sistema de Informação S.A.

A Semantix Tecnologia em Sistema de Informação S.A. é responsável por desenhar, implementar e operar controles eficazes para fornecer asseguração razoável de que os requerimentos enquanto prestadora de serviço e de seu sistema (processos, pessoas e ferramentas) foram alcançados. A Semantix Tecnologia em Sistema de Informação S.A.forneceu em sua declaração, Semantix Tecnologia em Sistema de Informação S.A. System Organization Controls sobre os Critérios de Trust Services de Segurança da informação, a descrição do Sistema baseada no *Description Criteria* e a afirmação sobre a operação dos controles para fornecer asseguração razoável de que os requerimentos de serviço e a exigência do sistema seriam alcançados com base nos critérios de segurança, se estiverem operando de maneira eficaz. A Semantix Tecnologia em Sistema de Informação S.A. é responsável por (1) preparar a descrição do sistema e a Declaração da Administração; (2) a integridade, precisão e método de apresentação da descrição de sistema e sua respectiva afirmação; (3) fornecer os serviços contemplados na descrição do sistema; (4) identificar os riscos que ameaçariam a realização dos requerimentos de serviços e de sistema da organização prestadora de serviços; e (5) desenhar, implementar, operar e documentar controles que sejam adequadamente desenhados para atender os critérios de segurança e integridade no processamento de dados estabelecidos na descrição do sistema.

Responsabilidade da Auditoria

A responsabilidade da EY é a de expressar uma opinião sobre a apresentação da descrição do sistema e sobre a adequação da operação dos controles no período de 01 de janeiro a 30 de setembro de 2022 para atender aos critérios de serviços aplicáveis, com base nos procedimentos de auditoria realizados.

A auditoria realizada pela EY foi conduzida de acordo com os padrões de atestação estabelecidos pelo AICPA. Essa norma requer que a EY planeje e realize sua avaliação a fim de obter asseguração razoável sobre se, em todos os aspectos materiais, (1) a descrição do sistema é apresentada de acordo com o *Description Criteria*, e (2) os controles descritos estão operando de forma adequada para fornecer segurança razoável de que os requerimentos enquanto prestadora de serviço e os requisitos de seu sistema foram alcançados considerando a operação no período de 01 de Janeiro a 30 de Setembro de 2022, com base nos critérios de segurança e integridade no processamento de dados. A natureza, época e a extensão dos procedimentos observados dependem do julgamento da auditoria, incluindo uma avaliação material do risco de existirem descrições incorretas, causadas por fraude ou erro. A EY acredita que

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

as evidências obtidas são suficientes e apropriadas para fornecer um embasamento razoável para sua opinião.

A auditoria da descrição do sistema de uma organização prestadora de serviços e a adequação da operação de seus controles envolve:

- obter um entendimento do sistema, os requerimentos de serviço e de sistema da organização prestadora de serviços;
- executar procedimentos para obtenção de evidências sobre se a descrição apresentada está de acordo com o *Description Criteria*;
- executar procedimentos para obtenção de evidências para verificar se os controles apresentados na descrição foram adequadamente desenhados para fornecer uma asseguração razoável de que a organização prestadora de serviços cumpre seus requerimentos de serviço e de sistema com base nos critérios de segurança e integridade, e se os controles operam de forma eficaz no período de 01 de janeiro a 30 de setembro de 2022;
- avaliar os riscos de que a descrição do sistema não é apresentada de acordo com o *Description Criteria* e de que os controles não foram adequadamente desenhados e operacionalizados para atender os critérios de segurança e integridade.
- avaliar a apresentação geral da descrição do Sistema.

Adicionalmente, a avaliação da EY incluem a realização de outros procedimentos que considerou necessários.
Fomos requeridos a sermos independentes da Semantix Tecnologia em Sistema de Informação S.A. e para atendermos nossas outras responsabilidades éticas, aplicáveis para examinação dos compromissos apresentados no prefácio: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Limitações inerentes

A descrição do sistema foi preparada para atender às necessidades comuns de uma ampla gama de entidades e pode, portanto, pode não incluir todos os aspectos do sistema que cada usuário individual possa considerar importantes para suas próprias necessidades específicas.

Devido à sua natureza, os controles de uma organização prestadora de serviços podem nem sempre funcionar de maneira eficaz para atender os critérios de segurança e integridade no processamento de dados. Além disso, as projeções futuras de qualquer avaliação da descrição do sistema, ou conclusões sobre a adequação da operação dos controles estão sujeitas ao risco de que mudanças no sistema podem alterar o desenho e/ou a operação adequada dos controles na organização prestadora de serviços, tornando-os ineficazes.

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

Outras considerações

Nossos procedimentos consistiram em avaliar a operação dos controles no período de 01 de janeiro a 30 de setembro de 2022, e, portanto, avalia a eficácia operacional dos controles declarados na descrição do sistema somente durante este período específico.

Opinião

Em nossa opinião, em todos os aspectos aplicáveis:

a. a descrição apresentada para o sistema SDP, estava desenhada, implementada e em operação no período de 01 de janeiro a 30 de setembro de 2022 de acordo com o *Description Criteria*.

b. os controles apresentados na descrição do sistema estavam adequadamente sendo operados no período de 01 de janeiro a 30 de setembro de 2022, para fornecer segurança razoável de que os requerimentos de serviço e de sistema da Semantix Tecnologia em Sistema de Informação S.A. seriam alcançados com base nos critérios contidos nas categorias de segurança e integridade.

Restrição de Uso

Este relatório destina-se exclusivamente à informação e uso da Semantix Tecnologia em Sistema de Informação S.A., das entidades usuárias do sistema SDP da Semantix Tecnologia em Sistema de Informação S.A. no período de 01 de janeiro a 30 de setembro de 2022, dos auditores independentes, e demais profissionais e entidades reguladoras que tenham conhecimento e compreensão suficientes sobre os seguintes aspectos:

- A natureza do serviço prestado pela Semantix Tecnologia em Sistema de Informação S.A. (organização prestadora de serviços);
- Como o sistema da organização de serviço interage com as entidades, organização de sub serviço, ou outras partes, incluindo os controles de entidade complementares e organizações de sub serviço assumidos no desenho dos controles da organização de serviço.
- Controles internos e suas limitações;
- Responsabilidades das entidades usuárias e como elas interagem com os controles relacionados a organização prestadora de serviços;

DocuSign Envelope ID: BA7732D9-78E4-43A7-945B-572452608161

- Os critérios de *Trust Services* de segurança e integridade no processamento de dados;
- Os riscos que podem ameaçar a cobertura dos critérios de *Trust Services* e como os controles lidam com esses riscos.

Este relatório não se aplica e não deve ser usado por alguém que não seja uma das partes especificadas.

São Paulo, 29 de Dezembro de 2022

Ernst & Young Auditores Independentes S.S
CNPJ 61.366.936/0001-25

CLAUDIA MARONA SANTOS

Claudia Marona
Sócia
CRC-1SP341085/O-9