Cielo S.A

Termo de Aceite - Requisitos de Segurança em Fornecedores

TERMO DE ACEITE

Título:	Requisitos de Segurança em Fornecedores		
VP/Diretoria:	VPTI	Versão:	01
Área:	Ger. Segurança da Informação	Data da revisão:	13/06/2019

Histórico de Revisões

Versão:		Histórico:
01	13/06/2019	Elaboração do Documento.

A proponente, cuja Razão Social_____ , com sede em: _____ , Cidade: _____, Estado: _____ , inscrita no CNPJ/MF sob nº_____, neste ato representada de acordo com seus atos constitutivos, doravante "Proponente".

Por este instrumento, a Proponente manifesta sua adesão aos Requisitos de Segurança em Fornecedores, de acordo com os seguintes termos e condições:

Índice

I. Objetivo 1
II. Abrangência 1
III. Requisitos de Segurança 1
1. Fornecedores com serviço PCI 1
2. Demais Fornecedores 2

I. Objetivo

Definir os requisitos mínimos de Segurança da Informação para prestadores de serviços e parceiros da Cielo que processem quaisquer informações da Cielo.

II. Abrangência

Todas as empresas prestadoras de serviço e parceiros da Cielo.

III. Requisitos de Segurança

1. Fornecedores com serviço PCI

1.1. O fornecedor que prestar serviço que se enquadre na categoria PCI, ou seja, que **processe, transmita ou armazene número de cartão de pagamento completo**, deve ter a Certificação PCI atualizada anualmente.

1.2. Adicionalmente os fornecedores devem enviar o relatório PCI com os GAPs identificados e plano de ação para atender a auditoria PCI.

1.3. Os fornecedores que não possuem o certificado PCI atualizado devem preencher anualmente o formulário de auto avaliação do PCI e enviar evidencias para luiz.baptista@cielo.com.br para embasar o formulário preenchido.

1.4. Anexo formulário de auto avaliação para preenchimento

PCI DSS Auto Avaliação.pdf

2. Demais Fornecedores

2.1. Política de Segurança da Informação

2.1.1. A proponente deve possuir uma política de segurança da informação publicada e disseminada para seus colaborados.

2.1.1.1. Todos os colaboradores envolvidos com serviços desta RFP devem conhecer a política de segurança da informação e ter ciência de seu conteúdo.

2.1.1.2. A proponente deverá treinar todos seus colaboradores nos itens de sua política de segurança da informação.

2.2. Segurança Lógica

2.2.1. Todos os sistemas e aplicações da proponente que processam, armazenam e transmitam dados da CIELO, devem ser integrados ao sistema de Identidades da Cielo via protocolo de mercado SAML.

2.2.2. Informações da CIELO não poderão ser publicadas através da Internet, salvo quando for aprovado pela área contratante e pela área de Segurança da Informação da CIELO.

2.2.3. A proponente deverá segregar, por firewall, dos ativos de seus demais clientes, os ativos que processam e armazenam informações CIELO e não permitir nenhum tipo de comunicação lógica entre estes ambientes.

2.2.4. Os sistemas e aplicações utilizados pela proponente, deverão gerar trilhas de auditorias das seguintes ações abaixo, pelo menos:

2.2.4.1. Ações administrativas

2.2.4.2. Entrada e saída de usuários administrativos

2.2.4.3. Acesso aos dados confidenciais da CIELO

2.2.5. As trilhas de auditoria devem ser enviadas para a CIELO.

2.2.6. As trilhas de auditoria devem ficar disponíveis por pelo menos 1 (hum) ano.

2.3. Transmissão de Dados

2.3.1. A proponente será responsável por disponibilizar o meio de transmissão de dados para envio das bases, caso necessário.

2.3.2. O meio de transmissão deverá ser criptografado, não sendo permitido uso de software de transmissão de mensagens pessoais ou e-mail.

2.3.2.1. Meios de transmissão inseguros, como FTP, não serão permitidos.

2.4. Armazenamento de Dados

2.4.1. A proponente será responsável pelo armazenamento seguro dos dados enviados pela CIELO.

2.4.2. Dados classificados como confidenciais, pela CIELO, deverão ser criptografados pela proponente, em seu armazenamento.

2.4.3. A proponente deverá armazenar as bases CIELO em ambiente exclusivo da CIELO.

2.4.4. Em caso de finalização de contrato, a proponente deve se comprometer a enviar todos os dados relacionados à operação CIELO para a CIELO e apagar (realizar wipe) todas as informações geradas durante o tempo de contrato.

2.5. Segurança dos Ativos

2.5.1. A proponente deverá ter um processo de atualização dos seus ativos tecnológicos, instalando as correções críticas de segurança em até 30 dias.

2.5.2. A proponente deverá utilizar somente softwares, programas e aplicações com contenham suporte de seus fabricantes.

2.5.2.1. Não será aceito o uso de software sem suporte do fabricante (backlevel) para atender a operação CIELO.

2.5.3. A proponente deverá realizar verificação de vulnerabilidades, no ambiente que atende a CIELO, no mínimo a cada 3 meses e os relatórios poderão ser requisitados pela CIELO para verificação.

2.5.4. A proponente deve ter instalado antivírus em todos os seus ativos de rede. Deve existir política e indicadores de gestão de antivírus e atualização.

2.5.5. A proponente deve ter política e indicadores de gestão de patches nos ativos de rede.

2.5.6. A proponente deve ter política e indicadores de gestão de vulnerabilidades nos ativos de rede.

2.5.7. A proponente deve ter política e indicadores de gestão de hardening nos ativos de rede.

2.5.8. A proponente deve ter política e controles que permitam prevenir que as informações da Cielo possam ser extraídas do ambiente tecnológico e físico da empresa

2.5.9. A proponente deve ter política e controles que garantam a identificação de todos os usuários que tenham acesso aos sistemas e ativos de rede.

2.6. Análises de Segurança da Informação

2.6.1. A CIELO poderá realizar análise, com foco em Segurança da Informação, no ambiente da proponente, a fim de validar se todos os requisitos de segurança da informação estão implementados e recorrentes.

2.6.2. A Proponente se compromete a certificar seu ambiente ao PCI DSS, caso venha a trabalhar com dados do portador de cartão de pagamento (Ex: Número de Cartão Completo) proveniente da CIELO.

2.6.2.1. A CIELO se exime de responsabilidade sobre qualquer custo, aquisição, modificação do ambiente, modificação de infraestrutura e qualquer outro item necessário para a certificação PCI DSS da proponente.

2.6.3. A proponente deve ter plano de resposta a incidente testado e atualizado anualmente.

2.6.4. A proponente deve ter plano de continuidade de negócio testado e atualizado anualmente.

Este instrumento é firmado em duas vias de igual teor e forma, na presença das testemunhas abaixo:

São Paulo, _____ de Julho de 2019.

Razão Social