

Descrição do Serviço

Padrão de Segurança de Dados do Setor de Cartões
de Pagamento

Consultoria de Correção

Sumário

| | |
|--|----------|
| Serviço de Correção do PCI DSS | 3 |
| Descrição do Serviço | 3 |
| Recursos do Serviço básico..... | 3 |
| Portal SecureTrust..... | 3 |
| Serviços Globais de Conformidade e Risco | 3 |
| Entrega e implementação | 4 |
| Início do projeto | 4 |
| Consultoria de correção de PCI DSS | 4 |
| RESPONSABILIDADES DA SECURETRUST..... | 4 |
| RESPONSABILIDADES E ACEITESDO CLIENTE | 4 |

Serviço de Correção do PCI DSS

A SecureTrust™ é uma divisão da Trustwave Holdings, Inc.

DESCRIÇÃO DO SERVIÇO

A Consultoria de Correção do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS – Payment Card Industry Data Security Standard) da SecureTrust (o “Serviço”) foi desenvolvida para auxiliar e orientar organizações a atingir e manter a conformidade com o PCI DSS, conforme estabelecido pelo Conselho de Padrões de Segurança do PCI (o “Padrão”).

Os termos em maiúsculas usados nesta descrição de serviço, mas não definidos aqui, têm seus significados indicados no Contrato Principal de Serviços da Trustwave localizado em <https://www.trustwave.com/en-us/legal-documents/contract-documents/> ou em um contrato similar assinado entre a SecureTrust e o Cliente.

RECURSOS DO SERVIÇO BÁSICO

O Serviço inclui os seguintes recursos padrão:

Portal SecureTrust

Os recursos do Portal SecureTrust consistem, entre outros, em um aplicativo de Gerenciamento de conformidade para administrar o processo de engajamento, bem como para coletar e armazenar com segurança evidências, documentação e produtos finais.

Serviços Globais de Conformidade e Risco

A equipe de Serviços Globais de Conformidade e Risco (GCRS — Global Compliance and Risk Services) é composta, entre outras, pelas seguintes pessoas e funções de destaque:

Avaliador de segurança qualificado (QSA – Qualified Security Assessor) – Um QSA é o recurso principal para a execução do Serviço, sendo responsável pelo agendamento e pela condução das atividades de consultoria.

Consultor gerencial (MC – Managing Consultant) – Um MC fornece orientação, supervisão de projeto e garantia de qualidade de relatórios ao QSA, além de servir como ponto de contato secundário do Cliente para escalamentos e consultas.

Conselho de Revisão de Conformidade (CRB – Compliance Review Board) – O CRB serve como ponto final para a interpretação dos requisitos do Padrão ou para a solução de questões complicadas de conformidade, fornecendo consistência e continuidade ao longo das avaliações da SecureTrust. O CRB também é o ponto final de escalamento para a solução de problemas relativos a status de conformidade contra os requisitos do Padrão ou a revisão de um controle de compensação.

Consultoria de correção de PCI DSS – Consultoria e orientação para atingir e manter conformidade com o Padrão. A SecureTrust fornecerá ao Cliente o Serviço para desenvolver planos de ação e processos priorizados para correção de brechas de conformidade de PCI DSS.

ENTREGA E IMPLEMENTAÇÃO

Início do projeto

A equipe de GCRS da SecureTrust facilita a entrega do Serviço, o que inclui o agendamento e a condução da reunião de abertura remota para definir e chegar a um acordo sobre um plano de projeto de alto nível que consiste em datas de marcos importantes, etapas principais, estimativas de duração, requisitos de recursos e procedimentos de escalamento.

Consultoria de correção de PCI DSS

O QSA da SecureTrust e o Cliente trabalharão juntos, e o QSA fornecerá orientação e recomendações para a criação de planos de ação priorizados e processos-alvo para a correção de brechas de conformidade de PCI DSS. As atividades do Serviço podem incluir, entre outras:

- Criação de um plano de ação de correção para controles ineficazes.
- Design de processos e projetos para corrigir brechas conhecidas para áreas de alta prioridade e alto risco.
- Aproveitamento dos controles comuns ao longo do ambiente de controle do Cliente para corrigir brechas identificadas.
- Determinação de evidências e documentação necessárias para demonstrar conformidade com PCI DSS.
- Identificação dos principais desafios e riscos do Cliente associados à obtenção da conformidade com PCI DSS.
- Estabelecimento de procedimentos de autoanálise para serem executados por proprietários de controle para áreas de alta prioridade.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente, se assim desejado.

RESPONSABILIDADES DA SECURETRUST

- Estabelecer contato e permanecer disponível para comunicações com o Cliente.
- Estabelecer comunicação e planos de escalamento.
- Criar uma conta do Cliente no Portal SecureTrust.
- Definir o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração e requisitos de recursos.
- Agendar e conduzir reuniões de abertura, status periódico e fechamento.

RESPONSABILIDADES E ACEITES DO CLIENTE

- Estabelecer contato e permanecer disponível para comunicações com a SecureTrust.
- Estabelecer comunicação e planos de escalamento.
- Concordar com o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Fornecer com precisão todas as informações necessárias, incluindo principais partes interessadas, informações aplicáveis sobre o ambiente do Cliente e requisitos de configuração.
- Informar à SecureTrust sobre todas as atividades de manutenção do ambiente do Cliente e sobre mudanças que podem impactar o fornecimento do Serviço.
- Responder com precisão às solicitações das equipes da SecureTrust ao estabelecer contato e na coleta das informações necessárias.

- Fornecer detalhes completos e precisos sobre o ambiente relevante e outras informações sobre as operações de negócios.
- Disponibilizar recursos capazes de participar das atividades do Serviço.
- Participar de e compreender os materiais explicados durante as chamadas, reuniões, entrevistas, discussões, inspeções de instalações e análises de controles.
- Aceites do cliente:
 - Todas as atualizações de segurança e recursos do Portal SecureTrust serão incluídas em atualizações de versões principais.
 - O Serviço consiste em consultoria remota.
 - A SecureTrust poderá solicitar evidências dos sistemas e processos do Cliente conforme necessário para comprovar a conformidade com quaisquer requisitos específicos. O Cliente concorda em fornecer todas essas evidências o mais breve possível.
 - A SecureTrust não é responsável por definir sistemas em escopo nem pela exatidão das informações fornecidas pelo Cliente.
 - A SecureTrust reserva-se o direito de rejeitar ou aceitar comentários do Cliente baseados nos fatos e circunstâncias do Serviço.
 - A SecureTrust desempenhará o Serviço no idioma inglês.
 - A SecureTrust não oferecerá nenhuma orientação ou aconselhamento legal.
 - A qualidade e a precisão do Serviço dependem do fornecimento pelo Cliente de informações precisas e acesso aos sistemas e recursos do Cliente para a SecureTrust.