

Descrição do Serviço

Padrão de Segurança de Dados do Setor de Cartões
de Pagamento

Consultoria de Autoavaliação

Sumário

PCI DSS – Consultoria de Autoavaliação	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
Fase I: Assistente de SAQ do Gerenciador de PCI e Varredura do PCI	4
Fase II: Consultoria de Autoavaliação de PCI DSS	4
RESPONSABILIDADES DA SECURETRUST.....	4
RESPONSABILIDADES E ACEITES DO CLIENTE	5

PCI DSS – Consultoria de Autoavaliação

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

DESCRIÇÃO DO SERVIÇO

O Serviço de Consultoria de Autoavaliação do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS – Payment Card Industry Data Security Standard) da SecureTrust é um serviço por inscrição (o “Serviço”) que inclui serviços de consultoria profissionais e acesso aos aplicativos do Portal SecureTrust para auxiliar organizações na conclusão de seus questionários de autoavaliação (SAQ – self-assessment questionnaire) do Setor de cartões de pagamento (PCI – Payment Card Industry) e no gerenciamento de suas varreduras de vulnerabilidade externa do PCI para ajudar na obtenção da 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 disponível em <https://www.trustwave.com/en-us/legal-documents/contract-documents/> or a similar agreement signed between SecureTrust and Client.

RECURSOS DO SERVIÇO BÁSICO

O Serviço inclui os seguintes recursos padrão:

Portal SecureTrust

O Portal SecureTrust consiste, entre outros, nos seguintes aplicativos e funções principais:

Gerenciador de PCI, Varredura do PCI – O aplicativo para gerenciar as varreduras ilimitadas de vulnerabilidades externas do PCI, com um scanner certificado como fornecedor de varreduras aprovado (ASV – Approved Scanning Vendor) e gerar relatórios de varreduras do PCI ASV.

Gerenciador de PCI, Assistente de SAQ – Uma ferramenta de Assistente de SAQ de fácil utilização para auxiliar o Cliente na conclusão do SAQ do PCI a fim de satisfazer os requisitos de relatório dos aquirentes e das bandeiras dos cartões.

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 Autoavaliação de PCI DSS – Consultoria e orientação para ajudar o Cliente a concluir um SAQ de PCI.

ENTREGA E IMPLEMENTAÇÃO

Início do projeto

A equipe de GCRS da SecureTrust facilita a entrega do Serviço, o que inclui a criação remota de uma instância para o Cliente no Portal SecureTrust e o agendamento e a condução da reunião de abertura remota para definir e acordar um plano de projeto de alto nível que consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos, requisitos de recursos e procedimentos de escalamento.

Fase I: Assistente de SAQ do Gerenciador de PCI e Varredura do PCI

O Gerenciador de PCI da SecureTrust fornece uma ferramenta de Assistente de SAQ de fácil utilização para auxiliar o Cliente na conclusão do SAQ do PCI a fim de satisfazer os requisitos de relatório das associações de cartões. O questionário está disponível em inglês (americano e britânico), francês, francês canadense, sueco, grego, espanhol, japonês e chinês (simplificado e tradicional).

O Gerenciador de PCI da SecureTrust fornece varreduras ilimitadas de vulnerabilidade externas do PCI durante a vigência do Serviço.

Suporte por email e telefone está disponível em vários idiomas para os aplicativos do Portal SecureTrust.

Fase II: Consultoria de Autoavaliação de PCI DSS

O QSA da SecureTrust e o Cliente trabalharão juntos para revisar e examinar os requisitos para a obtenção e manutenção da conformidade com o Padrão. As atividades do Serviço podem incluir, entre outras:

- Identificar áreas de não conformidade.
- Fornecer orientação para redução de escopo.
- Fornecer orientação de políticas e procedimentos.
- Fornecer orientação de infraestrutura e arquitetura de segurança de rede e fornecer orientação para auxiliar na conclusão da autoavaliação de conformidade de PCI DSS do Cliente.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente.

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 de planos.
- Estabelecer e manter contato com a SecureTrust.
- Concorde 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 as solicitações das equipes da SecureTrust no estabelecimento de contato e na coleta de informações.
- Fornecer detalhes completos e precisos sobre o ambiente relevante e outras informações sobre as operações de negócios.
- Tornar disponíveis recursos do Cliente 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 incluídos em atualizações de versões principais.
 - O Serviço é um engajamento remoto.
 - 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.