# Política de Segurança da Informação

Versão 1.0 - 14/04/2021

roadpass

# Sumário





Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

## Introdução

Para proteger os recursos de tecnologia da informação da RoadPass e proteger a confidencialidade dos dados, devem ser tomadas medidas de segurança adequadas. Esta Política de Segurança da Informação reflete o compromisso da RoadPass de cumprir os padrões exigidos que regem a segurança de informações confidenciais e confidenciais.

A RoadPass pode minimizar exposições inadequadas de informações confidenciais ou sensíveis, perda de dados e uso inadequado de redes e sistemas de computadores, cumprindo padrões razoáveis (como o padrão de segurança de dados da indústria de cartões de pagamento), atendendo ao design e controle adequados dos sistemas de informação e aplicar sanções quando ocorrerem violações desta política de segurança.

A segurança é de responsabilidade de todos que usam os recursos de tecnologia da informação da RoadPass. É de responsabilidade dos funcionários, contratados, parceiros de negócios e agentes do <Nome do comerciante>. Cada um deve se familiarizar com as disposições desta política e com a importância de segui-la ao usar os computadores, redes, dados e outros recursos de informação da RoadPass. Cada um é responsável por relatar qualquer violação suspeita de seus termos. Dessa forma, espera-se que todos os usuários de recursos de tecnologia da informação sigam todas as políticas e procedimentos exigidos pelo <Nome da Organização de Tecnologia da Informação da entidade>.

## Objetivo / escopo

O objetivo principal desta política de segurança é estabelecer regras para garantir a proteção de informações confidenciais e garantir a proteção dos recursos de tecnologia da informação da RoadPass. A política atribui responsabilidade e fornece diretrizes para proteger os sistemas e os dados da RoadPass contra uso indevido ou perda.

Esta política de segurança se aplica a todos os usuários de sistemas de computadores, gerenciados centralmente ou computadores autorizados a se conectar à rede de dados da RoadPass. Pode ser aplicado a usuários de serviços de informações operados ou administrados pela RoadPass (dependendo do acesso a dados confidenciais etc.). Os indivíduos que trabalham para instituições afiliadas a RoadPass estão sujeitos a essas mesmas definições e regras quando usam os recursos de tecnologia da informação da RoadPass.

Esta política de segurança se aplica a todos os aspectos da segurança de recursos de tecnologia da informação, incluindo, entre outros, destruição acidental ou não autorizada, divulgação ou modificação de hardware, software, redes ou dados.

Esta política de segurança foi elaborada para abordar especificamente a segurança dos dados usados pelo setor de cartões de pagamento.



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office

Vila Regente Feijó – São Paulo / SP - CEP 03342-000

Os dados do cartão de crédito armazenados, processados ou transmitidos com o ID do comerciante devem ser protegidos e os controles de segurança devem estar em conformidade com o Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS).

Os dados do titular do cartão neste documento são definidos como Número da conta principal (PAN), Código de validação do cartão (CVC, CVV2 e CVC2), PIN do cartão de crédito e qualquer forma de dados de tarja magnética do cartão (Faixa 1, Faixa 2).

## Propriedade e responsabilidades da política de segurança

As <Funções / Títulos> são os custodiantes atribuídos desta Política de Segurança. É da responsabilidade do custodiante (s) desta política de segurança para publicar e divulgar essas diretivas para todos os usuários relevantes da RoadPass sistema (incluindo fornecedores, empreiteiros e parceiros de negócios). Além disso, o (s) guardião (s) deve (m) garantir que a política de segurança endereça e esteja em conformidade com todos os padrões que a RoadPass deve seguir (como o PCI DSS). Este documento de política também será revisado pelo menos anualmente pelo (s) depositário (s) (e quaisquer proprietários de dados relevantes) e atualizado conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente de risco.

Perguntas ou comentários sobre esta política devem ser direcionados ao (s) custodiante (s) listado (s) acima.

## Documentos adicionais de processo e normas referenciados por esta política de segurança

Este documento de política define as políticas de segurança da RoadPass relacionadas à proteção de dados confidenciais e, principalmente, de dados de cartão de crédito. Detalhes sobre os padrões e procedimentos da RoadPass em vigor para permitir que essas políticas sejam seguidas estão contidos em outros documentos referenciados por esta política. A Tabela 2 lista outros documentos que acompanham este documento de política de segurança, que ajudam a definir as melhores práticas de segurança de dados da RoadPass.



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

## Tabela 2 - Documentos de processo e padrões de segurança mencionados pela política

**Nota: As referências de nome de documento contidas nesta tabela e em notas de rodapé em toda esta política de segurança devem ser substituídas pelo nome do documento de padrões específicos da empresa**.

| Nome Documento | Local/Departamento |
|---|---|
| Procedimentos de retenção e armazenamento de dados | <Inserir o local e departamento> |
| Processo de validação de conformidade do provedor de serviços | < Inserir o local e departamento > |
| Plano de resposta a incidentes | < Inserir o local e departamento > |



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

# 1 Não use os padrões fornecidos pelo fornecedor para a senha do sistema e outros parâmetros de segurança

Os componentes do sistema usados em redes confidenciais geralmente vêm com as configurações padrão do fornecedor (nomes de usuário, senhas, configurações, etc.). A política geral da RoadPass é sempre alterar os padrões fornecidos pelo fornecedor para senhas do sistema e outros parâmetros de segurança antes que os sistemas sejam instalados no ambiente de rede seguro (rede de dados do titular do cartão).

Indivíduos com intenção maliciosa (externa e interna a uma entidade) geralmente usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bem conhecidas pelas comunidades de hackers e são facilmente determinadas por meio de informações públicas.

## 1.1 Alterar padrões fornecidos pelo fornecedor

- Todos os padrões fornecidos pelo fornecedor devem ser alterados em todos os componentes do sistema antes de serem utilizados na rede de dados do titular do cartão. (por exemplo, senhas, cadeias de comunidades SNMP (protocolo de gerenciamento de rede simples) e eliminação de contas desnecessárias etc.). (Requisito 2.1.a, 2.2.d do PCI DSS)
- Todas as contas padrão desnecessárias devem ser removidas ou desativadas antes de instalar o dispositivo na rede. (Requisito 2.1.b do PCI DSS)

# 2 Desenvolver e manter Sistemas e Aplicativos seguros

Indivíduos sem escrúpulos usam vulnerabilidades de segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são corrigidas por patches de segurança fornecidos pelo fornecedor, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os sistemas devem ter todos os patches de software apropriados para proteger contra a exploração e o comprometimento dos dados do titular do cartão por indivíduos e softwares maliciosos.

> **Nota: Os patches de software apropriados são aqueles que foram avaliados e testados o suficiente para determinar que os patches não entram em conflito com as configurações de segurança existentes.**
>
> **Para aplicativos desenvolvidos internamente, inúmeras vulnerabilidades podem ser evitadas usando processos de desenvolvimento de sistema padrão e técnicas de codificação seguras.**

## 2.1 Atualizar Regularmente Sistemas e Software

- Todos os componentes e software do sistema devem ter os patches de segurança mais recentes fornecidos pelo fornecedor instalados. (Requisito 6.2.a do PCI DSS)
- Todos os patches críticos de sistema e software devem ser instalados dentro de 30 dias após a liberação do fornecedor. (Requisito 6.2.b do PCI DSS)



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

# 3 Identifique e autentique o acesso aos componentes do sistema

É fundamental atribuir uma identificação exclusiva (ID) a cada pessoa com acesso a sistemas ou software críticos. Isso garante que cada indivíduo seja o único responsável por suas ações. Quando essa responsabilidade está em vigor, as ações executadas em dados e sistemas críticos são executadas e podem ser rastreadas para usuários conhecidos e autorizados.

## 3.1 Exigir IDs de usuário exclusivos

- IDs exclusivos serão usados para todos os usuários que acessam os componentes do sistema no ambiente de dados do titular do cartão. (Requisito 8.1 do PCI DSS)
- Revogue imediatamente o acesso de qualquer usuário encerrado. (Requisito 8.1.3 do PCI DSS)

## 3.2 Métodos de autenticação do usuário

- Além de atribuir um ID de usuário exclusivo, o acesso aos sistemas na rede exige o uso de pelo menos um dos seguintes itens: (Requisito 8.2 do PCI DSS)
    - Algo que você sabe, como uma senha ou frase secreta
    - Algo que você tem, como um dispositivo token ou cartão inteligente
    - Algo que você é, como um biométrico
- As senhas ou frases devem atender ao seguinte: (Requisito 8.2.3 do PCI DSS)
    - Exigir um comprimento mínimo de pelo menos sete caracteres
    - Contêm caracteres numéricos e alfabéticos

## 3.4 Contas e senhas em grupo ou compartilhadas

- Não use contas ou senhas de grupo, compartilhadas ou genéricas ou outros métodos de autenticação, como a seguir: (Requisito 8.5 do PCI DSS.)
    - IDs de usuário genéricos estão desativados ou removidos.
    - IDs de usuário compartilhados não existem para administração do sistema e outras funções críticas.
    - IDs de usuário compartilhados e genéricos não são usados para administrar nenhum componente do sistema.

# 4 Restringir o acesso físico aos dados do titular do cartão

Qualquer acesso físico a dados ou sistemas que abrigam os dados do titular do cartão oferece a oportunidade para os indivíduos acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, devendo ser adequadamente restrito.

**Nota: Para os fins do Requisito 9, "pessoal no local" refere-se a funcionários de tempo integral e meio período, funcionários temporários, contratados e consultores que estão fisicamente presentes nas instalações da entidade. Um "visitante" refere-se a um fornecedor, convidado de qualquer equipe no local, técnicos de serviço ou qualquer pessoa que precise entrar na instalação por um curto período, geralmente não mais que um dia. "Mídia" refere-se a toda mídia em papel e eletrônica que contém dados do titular do cartão.**



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office

Vila Regente Feijó – São Paulo / SP - CEP 03342-000

# 5 Proteja fisicamente todas as mídias

- A RoadPass definirá procedimentos específicos para proteger fisicamente todas as mídias, incluindo, entre outros, computadores, mídia eletrônica removível, recibos em papel, relatórios em papel. (Requisito 9.5 do PCI DSS)

## 5.1 Distribuição de mídia

- Mantenha controle rígido sobre a distribuição interna ou externa de qualquer tipo de mídia, incluindo o seguinte: (Requisito 9.6 do PCI DSS)
    - Classifique a mídia para que a sensibilidade dos dados possa ser determinada.
    - Envie a mídia por correio expresso ou outro método de entrega que possa ser rastreado com precisão. Os logs devem mostrar aprovação da gerência e informações de rastreamento. Reter logs de transferência de mídia.
    - Verifique se o gerenciamento aprova todas as mídias que são movidas de uma área segura, inclusive quando a mídia é distribuída a indivíduos.

## 5.2 Armazenamento e acessibilidade de mídia

- Mantenha controle rígido sobre o armazenamento e acessibilidade da mídia. (Requisito 9.7 do PCI DSS)
- Manter adequadamente os registros de inventário de todas as mídias e realizar inventários de mídia pelo menos anualmente. (Requisito 9.7 do PCI DSS)

## 5.3 Políticas e Procedimentos de Destruição de Mídia

- A mídia que contém dados do titular do cartão deve ser destruída quando não for mais necessária por motivos comerciais ou legais. (Requisito 9.8 do PCI DSS)
- A RoadPass deve definir e documentar procedimentos específicos que serão usados para destruir, além da reconstrução, qualquer material impresso que contenha os dados do titular do cartão. Tecnologias como trituração, incineração, polpação etc. devem ser usadas para destruir a mídia. (Requisito 9.8.1 do PCI DSS)
- Se aplicável, todos os contêineres usados para armazenar mídia contendo os dados do titular do cartão a serem destruídos devem estar sempre trancados e em uma área segura. Esses recipientes devem ser entregues apenas a pessoal autorizado ou a terceiros para fins de destruição. (Requisito 9.8.1.b do PCI DSS)

# Manter uma diretiva de segurança da informação

Sem políticas e procedimentos de segurança fortes, muitas das camadas de controles de segurança se tornam ineficazes para impedir a violação de dados. A menos que políticas e práticas consistentes sejam adotadas e seguidas o tempo todo, os controles de segurança quebram devido à falta de atenção e manutenção deficiente. As políticas de documentação a seguir abordam a manutenção das políticas de segurança da RoadPass descritas neste documento.



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

# 6 Manter uma política de segurança que aborda a segurança da informação para todo o pessoal

Uma política de segurança forte define o tom de segurança para RoadPass e informa os funcionários e fornecedores o que é esperado deles. Todos os funcionários e fornecedores devem estar cientes da sensibilidade dos dados e de suas responsabilidades em protegê-los.

**Nota: "Funcionários" refere-se a funcionários de tempo integral e meio período, funcionários e funcionários temporários e contratados e consultores "residentes" no site da empresa.**

- Resultados em uma avaliação formal de riscos (Requisito 12.2 do PCI DSS)

## 6.1 Políticas para compartilhamento de dados com provedores de serviços

- Para estar em conformidade com as melhores práticas do setor, é necessário que a devida diligência seja realizada antes de se envolver com novos provedores de serviços e seja monitorada pelos provedores de serviços atuais que armazenam, processam ou transmitem dados do titular do cartão em nome da RoadPass. Os provedores de serviços, que podem afetar a segurança dos dados confidenciais do titular do cartão, também estão no escopo desta política.
  - A RoadPass deve manter uma lista documentada de todos os provedores de serviços aplicáveis em uso. (Requisito 12.8.1 do PCI DSS)
  - É necessário um contrato por escrito com todos os provedores de serviços aplicáveis e deve incluir um reconhecimento da responsabilidade dos provedores de serviços de proteger todos os dados do titular do cartão que recebem de ou em nome da RoadPass ou na medida em que possam afetar a segurança de um ambiente de dados do titular do cartão (requisito 12.8.2 do PCI DSS). Além disso, o provedor de serviços deve concordar em fornecer evidências de validação de conformidade anualmente. (Requisito 12.8.4 do PCI DSS). Antes de se envolver com um provedor de serviços aplicável, deve-se seguir um processo completo de due diligence. (Requisito 12.8.3 do PCI DSS)
  - A RoadPass deve revisar anualmente as evidências fornecidas pelos provedores de serviços aplicáveis, demonstrando sua conformidade contínua com o PCI DSS. (Requisito 12.8.4 do PCI DSS)
  - A RoadPass deve manter uma lista de quais requisitos do PCI DSS são gerenciados por cada provedor de serviços e que são gerenciados por <Nome do comerciante>. (Requisito 12.8.5 do PCI DSS)

## 6.2 Políticas do plano de resposta a incidentes

Incidentes ou suspeitos relacionados à segurança da rede de dados do titular do cartão ou dos próprios dados do titular do cartão devem ser tratados rapidamente e de maneira controlada, coordenada e específica. Um plano de resposta a incidentes (IRP) deve ser desenvolvido e seguido no caso de uma violação ou suspeita de violação. As políticas a seguir abordam especificamente o IRP da RoadPass:



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000

- A RoadPass deve manter um IRP documentado e estar preparado para responder imediatamente a uma violação do sistema. (Requisito 12.10 do PCI DSS)

# Apêndice A – Funções e responsabilidades de gerenciamento

## Atribuição de funções de gerenciamento e responsabilidades de segurança

Conforme exigido pela política na Seção 12.5 desta política de segurança, a tabela a seguir contém a atribuição de funções de gerenciamento para processos de segurança.

### Tabela A1 - Responsabilidades de segurança de gerenciamento

| Nome da função, grupo ou departamento | Data atribuída | Descrição da Responsabilidade |
|---|---|---|
| | | Estabelecer, documentar e distribuir políticas de segurança |
| | | Monitorar, analisar e distribuir alertas e informações de segurança |
| | | Estabelecer, documentar e distribuir políticas de resposta e escalação de incidentes de segurança |
| | | Administração de contas de usuário em sistemas na rede de dados do titular do cartão |
| | | Monitorar e controlar todo o acesso aos dados do titular do cartão |

# Apêndice B – Acordo de Cumprimento

## Acordo para Cumprir as Políticas de Segurança da Informação

Todos os funcionários que trabalham com dados do titular do cartão devem enviar uma cópia impressa assinada deste formulário. A gerência da RoadPass não aceitará modificações nos termos e condições deste contrato.



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office

Vila Regente Feijó – São Paulo / SP - CEP 03342-000

_____

Nome impresso do funcionário

_____

Departamento de funcionários

_____

Número de telefone do funcionário

_____

Endereço físico e localização do correio do funcionário

Eu, o usuário, concordo em tomar todas as precauções razoáveis para garantir que as informações internas da RoadPass ou as informações confiadas ao RoadPass por terceiros, como clientes, não sejam divulgadas a pessoas não autorizadas. No final do meu emprego ou contrato com a RoadPass, concordo em retornar a RoadPass todas as informações às quais tive acesso como resultado de minha posição com RoadPass. Entendo que não estou autorizado a usar essas informações para meus próprios fins, nem tenho a liberdade de fornecer essas informações a terceiros sem o consentimento expresso por escrito do gerente interno de RoadPass que é o proprietário designado das informações.

Tenho acesso a uma cópia do Manual de diretivas de segurança da informação RoadPass, li e compreendi o manual e entendo como isso afeta meu trabalho. Como condição de emprego contínuo em RoadPass, concordo em cumprir as políticas e outros requisitos encontrados nesse manual. Entendo que o não cumprimento será motivo de ação disciplinar, incluindo revogação de privilégios do sistema, demissão de RoadPass e talvez penalidades criminais e / ou civis.

Concordo em escolher uma senha difícil de adivinhar, conforme descrito no Manual de Políticas de Segurança da Informação RoadPass, concordo em não compartilhá-la com nenhuma outra pessoa e concordo em não anotar essa senha, a menos que tenha sido transformada em uma maneira irreconhecível.

Também concordo em relatar imediatamente todas as violações ou suspeitas de violações das políticas de segurança da informação ao <diretor do departamento de Segurança da Informação ou equipe, grupo responsável identificado etc.>.

_____

Assinatura do funcionário



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office

Vila Regente Feijó – São Paulo / SP - CEP 03342-000

## Aprovadores da Política

| Diretorias | Aprovador | Data |
|---|---|---|
| Gerente de Negócios | Fernando Cândido | |
| Gerente de Projeto | Rafael Siqueira | |
| Gerente Administrativo e Comercial | Carla do Carmo Cruz | |



Av. Regente Feijó, 944 – Sala 1403 B - Edifício Anália Franco Office
Vila Regente Feijó – São Paulo / SP - CEP 03342-000