

# *Diretrizes de Criptografia*

*Santos Bevilaqua Advogados*

## Sumário

1. Introdução.....	3
2. Abrangência .....	4
3. Objetivos .....	4
4. Diretrizes da Utilização de Criptografia .....	5
5. Chaves.....	7
6. Usuários .....	7
7. Implementação e Atualização .....	7

## 1. Introdução

O Santos Bevilaqua Advogados estabelece regras de segurança da informação com o objetivo de proteger seus ativos de informação contra ameaças e minimizar riscos e perdas. Buscamos garantir a disponibilidade de recursos e manter um programa de segurança eficaz, conscientizando todos os colaboradores sobre a importância da proteção de dados.

Reconhecemos a informação como um ativo crucial, e seu acesso é rigorosamente gerenciado para manter a confidencialidade, integridade e disponibilidade. A criptografia é uma ferramenta essencial para mitigar a interceptação e o acesso não autorizado, aplicada na proteção de dados armazenados, processados e transmitidos, além de credenciais de usuários e comunicações seguras.

Esta política detalha a abordagem do Santos Bevilaqua Advogados para controles e gerenciamentos criptográficos, definindo os requisitos e responsabilidades para alcançar os objetivos de segurança da informação e governança de dados. A criptografia assegura a ilegibilidade dos dados para não autorizados, conferindo confidencialidade, integridade e autenticação.

Em consonância com a Lei Geral de Proteção de Dados (LGPD), que exige medidas técnicas apropriadas para a proteção de dados em repouso e em trânsito, a criptografia é uma solução fundamental. Ela também é vital para prover integridade a dados que, embora acessíveis publicamente, requerem transmissão e armazenamento seguros.

O Santos Bevilaqua Advogados está comprometido em aprimorar continuamente uma cultura corporativa de segurança da informação, alinhada ao uso aceitável de informações e seus ativos de suporte, visando minimizar riscos e criar um ambiente seguro. Esta política deve ser seguida por todos os colaboradores, independentemente de seu nível ou função, ou vínculo empregatício.

## 2. Abrangência

Esta política de segurança abrange todos os ativos e ambientes do Santos Bevilaqua Advogados, sejam eles físicos ou digitais, onde informações são processadas ou armazenadas.

Especificamente, ela se aplica a:

- ⇒ **Ambientes Físicos:** Incluindo as unidades, CPD e qualquer outra propriedade ou local sob a custódia do Santos Bevilaqua Advogados.
- ⇒ **Ativos e sistema de Informação:** Todos os recursos de TI, sistemas de processamento de informações que empregam criptografia ou necessitam de proteção de dados sob a guarda do Santos Bevilaqua Advogados devem aderir aos termos desta política.
- ⇒ **Pessoal:** Abrange todos os colaboradores, prestadores de serviços com o Santos Bevilaqua Advogados.

## 3. Objetivos

Nossa política de segurança da informação visa alcançar os seguintes objetivos essenciais:

- ⇒ **Reduzir riscos:** Minimizar os riscos de segurança da informação para níveis aceitáveis.
- ⇒ **Proteger ativos:** Assegurar a confidencialidade, integridade e disponibilidade dos ativos, serviços e dados digitais do Santos Bevilaqua Advogados.
- ⇒ **Prevenir perdas:** Proteger as informações do escritório contra roubo ou perda acidental em dispositivos de armazenamento.

- ⇒ **Garantir segurança em transferências:** Assegurar que as informações do escritório estejam protegidas durante a transferência entre sistemas.
- **Fortalecer a resiliência cibernética:** Adotar os pilares da resiliência cibernética: Identificar, Proteger, Detectar, Responder e Recuperar.
- **Padronizar criptografia:** Definir padrões mínimos e responsabilidades para a criptografia de ativos digitais.
- **Gerenciar criptografia de forma consistente:** Garantir que a criptografia seja gerenciada de maneira uniforme e apropriada.
- **Assegurar a proteção de dados:** Proporcionar aos proprietários das informações a certeza de que seus dados estão protegidos.

#### 4. Diretrizes da Utilização de Criptografia

O Santos Bevilaqua Advogados assegura a segurança de suas informações por meio de um sistema robusto de criptografia, gerido pela equipe de Segurança da Informação.

Essa equipe é a única responsável por aprovar todas as tecnologias e técnicas de criptografia utilizadas, bem como pela distribuição e gerenciamento de todas as chaves. É crucial que, mesmo com a criptografia, os funcionários autorizados do Santos Bevilaqua Advogados tenham acesso imediato aos dados, garantindo a continuidade dos negócios e possibilitando investigações. A equipe também é responsável por criar e publicar os padrões de criptografia. Esses padrões incluem, no mínimo, o tipo, a força e a qualidade dos algoritmos de criptografia exigidos para diferentes níveis de proteção, e um gerenciamento completo do ciclo de vida das chaves (geração, armazenamento, recuperação, distribuição, fim de uso e destruição).

A Equipe de Segurança da Informação

Todas as informações confidenciais do Santos Bevilaqua Advogados devem ser criptografadas nas seguintes situações:

- ⇒ Ao serem transferidas eletronicamente ou por redes públicas.

- ⇒ Ao serem armazenadas em dispositivos móveis (como celulares ou notebooks).
- ⇒ Quando estiverem em repouso (paradas em um servidor ou sistema).

A política de criptografia aborda tanto os dados em trânsito (durante a movimentação) quanto os dados em repouso (armazenados em servidores e sistemas). Para a proteção de dados em repouso, as medidas podem incluir:

- ⇒ Criptografia de disco completo.
- ⇒ Criptografia de arquivo completo.
- ⇒ Criptografia de aplicativo completo.
- ⇒ Criptografia de banco de dados completo.

Vale ressaltar que todos os sistemas do Santos Bevilaqua Advogados usam certificado HTTPS desde a autenticação para garantir a segurança das conexões.

A implementação da criptografia deve sempre usar métodos e tecnologias aprovadas. Padrões, algoritmos, protocolos e chaves devem seguir as normas aceitáveis, e quaisquer cifras, protocolos ou algoritmos não suportados devem ser desativados sempre que possível.

Por fim, as chaves criptográficas devem ser geradas, armazenadas e gerenciadas de forma segura para evitar perdas, roubos ou comprometimento. O acesso às chaves deve ser feito por métodos confiáveis e seguros para manter a confidencialidade e a integridade. É crucial que canais de comunicação separados sejam usados para a transferência de chaves e dados, nunca os transferindo juntos pelo mesmo meio. Além disso, o Santos Bevilaqua Advogados segue procedimentos e controles rigorosos para a revogação de chaves e certificados em caso de comprometimento ou expiração.

## 5. Chaves

A política de criptografia do Santos Bevilaqua Advogados estrutura o ciclo de vida das chaves em quatro fases principais:

- ⇒ **Pré-operacional:** As chaves estão em processo de criação ou ativação e ainda não estão prontas para uso.
- ⇒ **Operacional:** As chaves estão ativas e disponíveis para uso normal.
- ⇒ **Pós-operacional:** As chaves não são mais usadas regularmente, mas ainda podem ser acessadas em situações específicas.
- ⇒ **Destruição:** As chaves são permanentemente eliminadas, juntamente com todos os registros de sua existência.

## 6. Usuários

A política de criptografia do Santos Bevilaqua Advogados verifica a identidade de um usuário. Somente após a autenticação, é possível utilizar as informações do usuário autenticado no sistema para definir as autorizações deste usuário. O uso das chaves criptográficas só é permitido após a identificação do usuário. Assim, para o gerenciamento adequado das chaves, o sistema deve fornecer mecanismos de autenticação e autorização ou permitir a utilização das chaves nos sistemas já existentes.

## 7. Implementação e Atualização

A Política de Criptografia do Santos Bevilaqua Advogados ser atualizada sempre que necessário.