POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

2025

Sumário

1. APRESENTAÇÃO 3
2. OBJETIVO 3
3. ABRANGÊNCIA 5
4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO 5
5. CLASSIFICAÇÃO DA INFORMAÇÃO 6
5.1. DIRETRIZES DA CLASSIFICAÇÃO 6
5.2. TRATAMENTO DAS INFORMAÇÕES POR NÍVEL 7
5.3. PROTEÇÃO POR MEIO E FORMA 7
5.4. RESPONSABILIDADES 7
5.5. CONFORMIDADE COM A LGPD 8
6. DIRETRIZES ESPECÍFICAS 8
7. DA GESTÃO DE ATIVOS 9
8. ACESSO REMOTO 9
9. POLÍTICA DE BYOD 10
10. RESPONSABILIDADES 10
11. GESTÃO DE INCIDENTES 11
12. CONSCIENTIZAÇÃO E TREINAMENTO 11
13. PENALIDADES 12
14. REVISÃO DA POLÍTICA 12

1. APRESENTAÇÃO

Segurança da Informação é o conjunto de práticas, políticas e medidas que tem como destino central proteger as informações contra acessos não autorizados, alterações indevidas, perda ou destruição, garantindo quatro pilares que são fundamentais: disponibilidade, integridade, confidencialidade e autenticidade.

O Decreto nº 9.637/2018 instituiu a Política Nacional de Segurança da Informação no âmbito da administração pública federal. No mesmo sentido, a norma ISSO 27001 é a norma padrão e referência internacional para a gestão da segurança da informação. Por conseguinte, ela define a segurança da informação como "*a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio*".

Sendo assim, é uma declaração formal acerca do compromisso com a proteção, o controle, a privacidade e o monitoramento das informações que são processadas, armazenadas, transmitidas ou custodiadas pelo escritório, que sejam sua propriedade e/ou estejam sob sua guarda e posse.

Diante do exposto, visando garantir e satisfazer os requisitos que são aplicáveis com relação a segurança da informação, é que o escritório promove a Política em epígrafe.

2. OBJETIVO

Esta política tem como objetivo estabelecer para proteção da informação no âmbito da Cenize Sociedade de Advogados, especializado em serviços jurídicos voltados à recuperação de crédito, ressarcimento e litígios relacionados ao setor de seguros.

Sendo assim, visa garantir a confidencialidade, integridade e disponibilidade das informações, inclusive dados pessoais e sensíveis, conforme a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e demais normas aplicáveis ao setor jurídico e securitário.

A referida Política será publicada e divulgada no site do Escritório, em atendimento ao público interno e externo.

Os principais objetivos são:

a) Proteger os ativos de informações de qualquer tipo de ameaça, interna ou externa, deliberada ou acidental, assegurando sua integridade, disponibilidade, autenticidade e confidencialidade;

b) Assegurar que o escritório esteja em conformidade com as leis e regulamentos aplicáveis, como a LGPD e demais normas aplicáveis ao setor jurídico e securitário;

c) Promover uma cultura de segurança entre todos os colaboradores, parceiros e partes interessadas, tendo por visão uma conscientização e responsabilidade no tratamento das informações;

d) Mitigar riscos que estejam associados à segurança da informação, através de uma abordagem estruturada de gestão de riscos, com ações preventivas e corretivas voltadas à proteção dos dados;

e) Manter a privacidade e a proteção dos dados pessoais, conforme disposto na LGPD, assegurando a integridade e os direitos dos titulares;

f) Garantir a continuidade dos negócios, através do estabelecimento de processos resilientes e planos de respostas a incidentes, visando minimizar os impactos de falhas e lacunas de segurança.

3. ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores, advogados, sócios, estagiários, parceiros, correspondentes e prestadores de serviços que, direta ou indiretamente, tratem informações jurídicas, contratuais, processuais, financeiras ou pessoais de seguradores, segurados, terceiros ou demais partes envolvidas nas demandas jurídicas conduzidas pelo escritório.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Para que exista uma boa política de segurança da informação, alguns pilares são essenciais, garantindo, desta forma, a defesa cibernética, a segurança física e a proteção de dados organizacionais, assegurando seus quatro pilares: confidencialidade, integridade, disponibilidade e autenticidade.

Também conhecidos como princípios da segurança da informação, eles estão dispostos no Decreto nº 9.637/2018. Isto posto, confira a seguir os princípios pelos quais seguimos e nos baseamos:

1) **Confidencialidade:** Garantir que dados jurídicos e informações de clientes não sejam acessados por pessoas não autorizadas, e muito menos vazados;

2) **Integridade:** Assegurar a exatidão das informações processuais, contratuais e financeiras, preservando seu conteúdo original;

3) **Disponibilidade:** Manter os dados acessíveis por sistemas seguros para a execução tempestiva das atividades jurídicas;

4) **Autenticidade:** Garantir que a informação é proveniente de uma fonte confiável e que não foi alterada por terceiros não autorizados. Para isso, é preciso utilizar mecanismos de controle de acesso, assinatura digital, certificação e criptografia de dados.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações tratadas devem ser classificadas conforme sua criticidade e impacto. Para isso, existem níveis de classificação, conforme disposto a seguir:

- **Pública:** Informações destinadas ao público em geral, sem restrições. Exemplos: Artigos, jurisprudência, decisões públicas, dentre outras;
- **Interna:** Informações destinadas ao uso interno do escritório, com acesso restrito aos colaboradores. Exemplos: Modelos de petição, planejamento de demandas, dentre outros;
- **Confidencial:** Informações sensíveis que, se divulgadas, podem causar prejuízos ao escritório ou aos clientes. Acesso restrito a pessoas autorizadas. Exemplos: dados de processos, contratos com clientes, dentre outros;
- **Sigilosa:** Informações sensíveis de processos em segredo de justiça, dados bancários e pessoais sensíveis, acesso extremamente restrito. Exemplos: Dados de saúde, dados bancários, processos com segredo legal, biometria, dentre outros.

5.1. DIRETRIZES DA CLASSIFICAÇÃO

Para classificação das informações, necessário se faz seguir algumas diretrizes, conforme disposto a seguir:

- Todas as informações devem ser classificadas no momento de sua criação ou recebimento;

- A classificação deve ser claramente indicada nos documentos e sistemas apropriados;
- A reclassificação deve ser realizada sempre que houver mudança na sensibilidade ou importância da informação.

5.2. TRATAMENTO DAS INFORMAÇÕES POR NÍVEL

- **Pública:** Sem restrições de uso;
- **Interna:** Acesso limitado a colaboradores autorizados;
- **Confidencial:** Acesso apenas a envolvidos no caso; criptografia e controle de acesso obrigatórios;
- **Sigilosa:** Acesso restrito e controlado; proteção legal máxima; registros de acesso obrigatórios.

5.3. PROTEÇÃO POR MEIO E FORMA

MEIO	MEDIDAS
Digital	Senhas, criptografia, backups, VPN, monitoramento de acesso
Físico	Arquivamento trancado, controle de cópias, descarte seguro
Transmissão	E-mail corporativo seguro, plataformas autorizadas, proibição de envio por redes pessoais

5.4. RESPONSABILIDADES

Importante ratificar que todos os colaboradores são responsáveis por classificar corretamente as informações que criam ou manuseiam, sendo fornecidas pelos superiores todas as orientações e suportes necessário para classificação e proteção das informações.

5.5. CONFORMIDADE COM A LGPD

Todas as informações que envolvem dados pessoais devem ser tratadas de acordo com os princípios e requisitos da Lei Geral de Proteção de Dados Pessoais, garantindo a privacidade e os direitos dos titulares dos dados.

6. DIRETRIZES ESPECÍFICAS

A Cenize Sociedade de Advogados adota uma abordagem baseada em riscos, promovendo, desta forma, uma maior agilidade, flexibilidade e responsabilidade nas ações de segurança da informação. Por conseguinte, o tratamento de dados pessoais deve seguir os princípios que regem a Lei Geral de Proteção de Dados Pessoais (LGPD). Isto posto, são as seguintes diretrizes:

- **O acesso a sistemas jurídicos e bancários** será restrito ao pessoal autorizado, com autenticação de dois fatores, sempre que possível;
- **Arquivos, contratos e procurações** devem ser armazenados em ambientes digitais seguros e criptografados, com backup regular;
- **Transmissão de informações** com seguradoras e parceiros deve ser feita por e-mail corporativo seguro ou sistemas específicos com controle de acesso;
- **Processos em segredo de justiça** devem ter controle reforçado de acesso e não podem ser compartilhados sem autorização expressa;
- **Dispositivos móveis** devem ser protegidos por senha, biometria ou PIN, com bloqueio automático e, quando possível, criptografia de disco;
- **Documentos físicos** devem ser arquivados em local extremamente seguro e trancado, com descarte seguro por fragmentação ou trituração;
- **Sistemas** mantidos atualizados com antivírus e firewall;
- **Ambiente de trabalho:** deve-se evitar deixar documentos impressos expostos, telas desbloqueadas ou informações visíveis a terceiros.

7. DA GESTÃO DE ATIVOS

Os ativos de informação da Cenize Sociedade de Advogados devem ser mapeados e protegidos contra divulgação, modificação ou destruição não autorizada, independentemente do meio em que estejam armazenados. Para isso, necessário seguir algumas diretrizes:

- **Inventário de Ativos:** Manter um registro atualizado de todos os ativos de informação, incluindo hardware, software e dados;
- **Responsabilidade pelos Ativos:** Designar responsáveis por cada ativo para assegurar seu uso adequado e seguro;
- **Ciclo de vida dos ativos:** Implementar processos para aquisição, uso, manutenção e descarte seguro dos ativos.

8. ACESSO REMOTO

Algumas diretrizes devem ser seguidas, caso haja necessidade para trabalho remoto:

- O acesso remoto aos sistemas e dados do escritório só serão permitidos através de VPN (rede privada virtual) ou canais criptografados;
- Os colaboradores devem utilizar equipamentos aprovados, além de manter ambientes físicos privados durante o trabalho remoto;
- A conexão com redes públicas deve ser evitada ou obrigatoriamente protegida por VPN;
- A autenticação deve seguir o mesmo padrão de segurança interno, ou seja, senha forte e autenticação de dois fatores.

9. POLÍTICA DE BYOD

O uso de dispositivos pessoais para atividades profissionais será permitido, desde que haja autorização expressa, além de seguir as seguintes diretrizes com relação ao dispositivo:

- O dispositivo deve possuir sistema operacional atualizado e protegido por senha ou biometria;
- O dispositivo deve ter antivírus ativo;
- Não deve haver compartilhamento de dispositivo com terceiros (familiares, amigos etc.);
- O dispositivo deve possuir acesso remoto revogável, em caso de desligamento ou incidente.
- O uso de dispositivos pessoais para as atividades profissionais será permitido, desde que haja autorização expressa

Necessário enfatizar que o usuário é responsável por manter seu dispositivo seguro e deve aceitar que ele possa ser auditado quanto ao cumprimento desta política.

10. RESPONSABILIDADES

Importante ressaltar que a segurança da informação na Cenize Sociedade de Advogados é uma responsabilidade compartilhada, onde os papéis devem ser claramente definidos e atribuídos para que haja eficácia das ações de proteção de dados e mitigação de riscos. Diante do exposto, as responsabilidades são distribuídas da seguinte forma:

- Sócios e gestores jurídicos: Promover a cultura de segurança e zelar pelo cumprimento desta política;
- TI (ou responsável técnico): Garantir infraestrutura segura, backups periódicos e controles de acesso aos sistemas;

- Advogados e colaboradores: Zelar pelas informações acessadas e comunicar qualquer incidente;
- DPO ou responsável pela proteção de dados pessoais: Garantir a conformidade com a LGPD, inclusive quanto aos direitos dos titulares e notificações obrigatórias.

11. GESTÃO DE INCIDENTES

Qualquer falha, vazamento, perda de documentos ou acesso indevido a informações jurídicas, confidenciais, pessoais ou financeiras, deve ser reportado de imediato. A gestão do incidente incluirá:

- Identificação da causa;
- Mitigação de danos;
- Comunicação a partes interessadas, conforme obrigação legal;
- Adoção de medidas corretivas.

Necessário ratificar que, com relação a incidentes referentes a Dados Pessoais, deverá ser seguido o que consta na Política de Incidentes de Segurança de Dados Pessoais.

12. CONSCIENTIZAÇÃO E TREINAMENTO

De forma periódica, os profissionais serão treinados em boas práticas de segurança, proteção de dados e conduta ética, com ênfase nos riscos do tratamento de informações jurídicas e pessoais no setor de seguros.

13. PENALIDADES

O descumprimento desta política poderá acarretar advertência, suspensão, desligamento e/ou responsabilização civil, penal e administrativa, de acordo com a natureza da infração.

14. REVISÃO DA POLÍTICA

Esta política será revisada anualmente ou diante de mudanças relevantes nos processos, legislações aplicáveis, tecnologias utilizadas, estrutura organizacional ou expansão dos serviços.