SISTEMA DE INTEGRIDADE
PIRONTI ADVOGADOS

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Ver. 003 - Fevereiro de 2024

Melhores Empresas para Trabalhar no Paraná Great Place To Work. BRASIL 2022

Melhores Empresas para Trabalhar Pequenas Empresas Great Place To Work. BRASIL 2022

análise ADVOCACIA 2023/2024 ADVOGADO MAIS ADMIRADO

análise ADVOCACIA 2023/2024 ESCRITÓRIO MAIS ADMIRADO

PIRONTI ADVOGADOS

#OUSADIAEMSONHAR

# OBJETIVO

A Política de Segurança da Informação (“PSI”) tem como objetivo definir critérios e diretrizes com relação aos processos a serem estabelecidos e seguidos por todos os colaboradores, bem como com relação aos recursos digitais e físicos disponibilizados pelo Escritório Pironti Advogados (“Escritório”), para prevenir incidentes, acrescentar maior segurança observando os pilares de confidencialidade, integridade e disponibilidade relacionados à segurança da informação.

- Orientar sobre a adoção de controles e processos para atender aos requisitos de Segurança da Informação; A partir destas orientações, é possível padronizar as práticas de comportamento seguro, adequados às metas e necessidades do Escritório, acrescentando maior segurança e credibilidade ao trabalho realizado. Além disso, esta Política tem como premissa: Orientar sobre a adoção de controles e processos para atender aos requisitos de Segurança da Informação;

- Resguardar as informações do Escritório, garantindo os pressupostos básicos da confidencialidade, integridade e disponibilidade;

- Prevenir possíveis causas de incidentes e responsabilidade legal do Escritório e seus colaboradores, clientes e parceiros;

- Minimizar os riscos de prejuízos financeiros, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo nos negócios do Escritório consequentes de falhas de segurança.

## 2. ÂMBITO DE APLICAÇÃO

A Política de Segurança da Informação é destinada aos sócios de capital, sócios de serviço, advogados associados, empregados e estagiários/trainees, bem como aos terceiros, tais como fornecedores, intermediários, despachantes, consultores, correspondentes, pres-

tadores de serviço e parceiros de negócios, que se relacionam com o Escritório, direta ou indiretamente, sendo que suas condutas sejam pautadas em boas práticas do mercado nacional e internacional, conforme padrões indicados a seguir:

- ISO 27001 – Gestão da Segurança da Informação;
- ISO 27002 – Políticas para segurança da Informação;
- ISO 27701 – Gestão da Privacidade da Informação;
- ISO 31000 – Gestão de Risco.

É imprescindível que todos os colaboradores do Escritório Pironti Advogados observem as determinações contidas na presente Política, a fim de fomentar o desenvolvimento da transparência, integridade, confidencialidade e ética dentro do ambiente do Escritório.

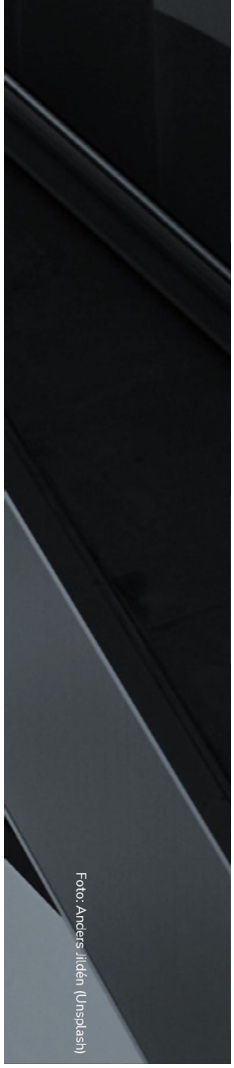
Foto: Anders Jildén (Unsplash)

## 3. GLOSSÁRIO

| | |
|---|---|
| Ameaça: | Causa potencial de um incidente, que pode acarretar eventual prejuízo aos negócios do Escritório; |
| Ativo: | Tudo aquilo que possui valor para o Escritório; |
| Ativo de informação: | Patrimônio intangível do Escritório, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao Escritório por parceiros, clientes, colaboradores autônomos e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do Escritório ou por infraestrutura externa contratada pelo Escritório, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física; |
| Confidencialidade: | Garantia de que a informação é acessível somente por pessoas autorizadas; |
| Comitê de Privacidade e Proteção de Dados: | Grupo de trabalho multidisciplinar permanente, nomeado pela diretoria do Escritório, que tem por finalidade tratar questões também ligadas à Segurança da Informação; |

| | |
|---|---|
| Controle: | Medida de segurança adotada pelo Escritório para o tratamento de um risco específico; |
| Disponibilidade: | Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário; |
| Gestor da Informação: | Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário; |
| Incidente de Segurança da Informação: | Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do Escritório; |
| Integridade: | Salvaguarda da exatidão e totalidade da informação e dos métodos de processamento. |
| Portadores da Informação: | Terceiros que manipulem qualquer ativo de informação de responsabilidade do Escritório para o desempenho de suas atividades profissionais |
| Sistema de segurança da Informação: | Conjunto de controles, políticas, práticas e procedimentos que visam proteger a informação |
| Vulnerabilidade: | Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do Escritório |

## 4. PAPÉIS E RESPONSABILIDADES

As informações tratadas nos processos internos do Escritório podem ser utilizadas por todos aqueles envolvidos nas operações internas. Sendo assim, é responsabilidade de todos (colaboradores, fornecedores ou terceiros prestadores de serviços) proteger os bens, informações e recursos do Escritório aos quais possuem acesso de acordo com as suas funções, incluindo aqui a responsabilidade pela gestão de risco e segurança das informações, bem como o cumprimento das normas e procedimentos desta Política.

Além disso, é de competência do Comitê de Privacidade e Proteção de Dados, com o auxílio da equipe de Tecnologia da Informação:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à Segurança da Informação;

- Avaliar a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

- Garantir que as atividades de Segurança da Informação sejam executadas em conformidade com este documento;

- Promover a divulgação desta Política e adotar as medidas necessárias para disseminar uma cultura de Segurança da Informação no ambiente do Escritório;

- Identificar e avaliar as principais ameaças à Segurança da Informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

- Tomar as ações cabíveis para se fazer cumprir os termos desta Política;

- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

Ainda, aos portadores da informação, compete:

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, assim como as demais normas e procedimentos de segurança aplicáveis;

- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos ao Encarregado de Dados (DPO) responsável pela empresa de referência;

- Comunicar o Encarregado de Dados (DPO) responsável pela empresa de referência sobre a ocorrência de qualquer evento que represente violação a esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do Escritório;

- Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

É de responsabilidade dos gestores da informação:

- Gerenciar as informações geradas ou sob a responsabilidade da sua área interna durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme os procedimentos adotados pelo Escritório;

- Identificar, classificar e rotular as informações geradas sob a responsabilidade da

sua área de negócio conforme normas, critérios e procedimentos adotados pelo Escritório;

- Revisar, de forma periódica, as informações geradas ou sob a responsabilidade da sua área interna, ajustando a classificação e rotulagem delas, conforme necessário;

- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo Escritório.

Serão consideradas condutas incoerentes com a presente Política, mas não se limitando, as seguintes:

- Compartilhar e/ou armazenar informações pessoais de titulares que confiaram seus dados ao Escritório através de plataformas não autorizadas, como por exemplo Facebook, e-mail pessoal, e/ou com terceiros não autorizados;

- Armazenar ou compartilhar informações confidenciais ou sigilosas, sem autorização;

- Fotografar os colaboradores do Escritório ou terceiros, ou capturar a tela do computador, que contenha dado pessoal, como também compartilhar essas informações quando não determinado pelo Escritório;

- Omitir informações referentes à incidentes de segurança ao Comitê de Privacidade e Proteção de Dados;

- Tratar os dados pessoais, confidenciais ou sigilosos de forma negligente ou imprudente, de forma a desrespeitar o dever de sigilo ou facilitar o vazamento de informações;

- Impedir ou dificultar que os titulares de dados efetivem os seus direitos previstos na LGPD;

- Copiar informações do Escritório em qualquer tipo de dispositivos de armazenamento pessoal, físico (ex: pendrive, HD externo) ou lógico (exemplo: OneDrive, Google Drive, Dropbox) sem autorização por escrito/e-mail do seu gestor ou da diretoria.

## 5. GESTÃO DE RISCOS

O Comitê de Privacidade e Proteção de Dados do Escritório será responsável pela gestão dos riscos de segurança de informação. Dessa forma, irá mapear e identificar os possíveis riscos, para elaboração de planos de ação visando sua mitigação.

Além disso, o Encarregado de Dados (DPO) será responsável pelo monitoramento contínuo relacionado ao Sistema de Privacidade e Proteção de Dados do Escritório.

## 6. ACESSO A SISTEMAS E RECURSOS

Os colaboradores são integralmente responsáveis pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas e e-mails. Consequentemente, são responsáveis pelas ações decorrentes da má utilização destes recursos em caso de acessos indevidos.

As senhas ou códigos de acesso à dispositivos e sistemas do Escritório não deverão ser compartilhadas, sendo de uso pessoal e intransferível.

Nas hipóteses de roubo de senha ou impossibilidade de acesso, é dever do colaborador do Escritório comunicar, de forma imediata, ao seu gestor direto, para que este proceda com as diligências necessárias à normalização do incidente.

## 7. USO DE RECURSOS DO ESCRITÓRIO

Os equipamentos disponíveis nas dependências do Escritório Pironti Advogados constituem sua propriedade, devendo ser utilizados de maneira ética e correta, para fins profissionais, relacionados às atividades do Escritório.

Os colaboradores devem formalmente concordar com o conteúdo da presente Política antes de utilizar os equipamentos de propriedade do Escritório.

O uso de equipamentos do Escritório para fins particulares é permitido desde que não prejudique a produtividade dos colaboradores durante o desempenho de suas atividades.

Os colaboradores são responsáveis pelo uso e conservação dos bens do Escritório sob

sua guarda. É vedada a utilização destes para acesso, disseminação e/ou armazenamento de conteúdos pornográficos, discriminatórios, violentos, que desrespeitem terceiros ou contrariem os valores e políticas do Escritório.

O Escritório Pironti Advogados se compromete em manter atualizados todos os equipamentos de sua titularidade, garantindo a modernização dos softwares antivírus instalados, bem como equipamentos devidamente atualizados.

## 8. PROPRIEDADE INTELECTUAL

As informações produzidas pelos colaboradores no exercício de suas funções e as informações a eles disponibilizadas em razão das suas atividades profissionais são de propriedade e/ou direito de uso exclusivo do Escritório Pironti Advogados.

Os colaboradores não devem copiar, transferir, compartilhar, alterar, adulterar ou utilizar indevidamente ou para propósitos particulares, quaisquer informações ou equipamentos de tecnologia da informação de propriedade ou sob a responsabilidade do Escritório Pironti Advogados, além de não praticar quaisquer atos que possam causar pré-juízo ao Escritório.

## 9. TRABALHO REMOTO

O trabalho remoto poderá ocorrer desde que previamente autorizado pelo gestor da área, sendo os colaboradores responsáveis pelo uso e conservação dos bens do Escritório sob sua guarda.

O colaborador deve se atentar ao local onde está trabalhando, a rede wi-fi que está conectado, bem como aos programas e os websites que acessar, podendo ser responsabilizado por qualquer vazamento de informações que ocorrer, seja por meio físico ou digital.

Em caso de eventual incidente de segurança, o colaborador deve informar imediatamente ao gestor de sua área e o Encarregado de Dados (DPO) do Escritório, para que sejam aplicadas as medidas de mitigação cabíveis.

## 10. MONITORAMENTO E INSPEÇÃO

O Escritório Pironti Advogados monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação, bem como a identificação de uso de equipamentos corporativos para fins particulares.

O Escritório pode auditar ou inspecionar os equipamentos de tecnologia da informação que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, ainda que sem aviso prévio, atendendo aos princípios da proporcionalidade e razoabilidade.

O Escritório Pironti Advogados eventualmente poderá ter acesso às informações de caráter pessoal de seus colaboradores, em razão da auditoria, se estes utilizarem os equipamentos corporativos indevidamente para armazenar seus dados pessoais.

## 11. PENALIDADES

É responsabilidade de todos os colaboradores o dever de comunicar, através dos meios disponíveis, qualquer violação e suspeita de violação à presente Política. É imprescindível que cada integrante compreenda o papel que possui em relação à segurança da informação e a proteção de dados em suas atividades diárias.

Caberá ao Comitê de Privacidade e Proteção de Dados do Escritório, avaliar os incidentes de Segurança da Informação identificados, em conjunto com a área de Tecnologia da Informação. Posteriormente, a estrutura organizacional poderá averiguar o grau de responsabilidade dos envolvidos em procedimento próprio, sugerindo penalidades e sanções à Alta Administração, para que essa se manifeste quanto a aplicação aos infratores.

As comunicações podem ser realizadas através do e-mail da Encarregada de Dados (DPO) do Escritório: dpo@pirontiadvogados.com ou por meio do Canal de Relatos no site.

Qualquer denúncia sobre uma possível violação das políticas internas do Escritório, bem como a legislação vigente serão rigorosamente investigadas pelo Comitê de Ética, e caso haja a confirmação dos fatos relatados, o Comitê deliberará sobre as sanções disciplinares cabíveis, que poderão incluir advertência verbal ou escrita, ação disciplinar, repreensão, suspensão, demissão e/ou rescisão contratual por justa causa, sem prejuízo de responsabilização civil e/

ou criminal podendo o Escritório pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio de medidas legais cabíveis.

Não será tolerada nenhuma forma de retaliação contra aqueles que apresentarem denúncias sobre possíveis condutas inadequadas, já que o Comitê tem total imparcialidade e confidencialidade ao relatante.

Caso o incidente ocorra com terceiros contratados pelo Escritório, caberá ao Comi-te analisar a ocorrência e deliberar sobre quais medidas deverão ser tomadas conforme termos previstos em contrato.

## 12. CASOS OMISSOS

As diretrizes de segurança da informação e proteção de dados pessoais adotadas pelo Escritório não se esgotam na presente Política, em razão da constante evolução tecnológica e atualização de normas legais ligadas ao tema. Será de responsabilidade do Comitê analisar tais casos para posterior deliberação e resolução da ocorrência.

## 13. REVISÕES

A presente Política de Segurança da Informação será revisada anualmente, mas não há qualquer empecilho para que, em sendo necessário, haja revisão e ajustes anteriores para garantir de que o tratamento de dados permanece sendo realizado em conformidade com a legislação vigente, conforme a necessidade considerada pelo Comitê de Privacidade e Proteção de Dados, o que será devidamente informado a todos os interessados.

## CONTROLE DE REVISÕES

| Versão | Descrição | Elaboração | Revisão | Aprovação |
|---|---|---|---|---|
| 001 | **Emissão Inicial** “Política de Segurança da Informação, Privacidade e Proteção de Dados“ | Pironti Advogados | - | **Data:** 05/08/2020 **Aprovador:** Alta Administração |
| 002 | **1° revisão** “Política de Segurança da Informação, Privacidade e Proteção de Dados“ | Pironti Advogados | - | **Data:** 13/10/2020 **Aprovador:** Alta Administração |
| 003 | **2° revisão** “Política de Privacidade” | Equipe de Compliance | Mariana T. Keppen (**CCO**) | **Data:** 13/09/2022 **Aprovador:** Comitê de Gestão |
| 004 | **3° revisão** “Política de Segurança da Informação” | Equipe de Compliance e Proteção de Dados | Marcela Féder **(DPO)** | **Data:** 29/02/2024 **Aprovador:** DPO |

PIRONTI
ADVOGADOS

#OUSADIAEMSONHAR

Av. João Gualberto, 780 - 3º, 4º e 5º andares
Alto da Glória - CEP 80.030-000 - Curitiba (PR)

Tel. +55 (41) 3209-7200 | Tel. +55 (41) 3209-7300

Melhores Empresas para Trabalhar no Paraná
Great Place To Work. BRASIL 2022

análise ADVOCACIA 2023/2024 ADVOGADO MAIS ADMIRADO

Melhores Empresas para Trabalhar Pequenas Empresas
Great Place To Work. BRASIL 2022

análise ADVOCACIA 2023/2024 ESCRITÓRIO MAIS ADMIRADO

@pirontiadvogados_ Pironti Advogados Pironti Advogados Pironti Advogados

www.pirontiadvogados.com