PORTUGAL VILELA

DIREITO DE NEGÓCIOS

Política de Segurança da Informação

2023

PORTUGAL VILELA
DIREITO DE NEGÓCIOS

Sumário

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

Introdução

A Política de Segurança da Informação (PSI) apresenta os principais pontos e objetivos da política. A segurança da informação é uma preocupação cada vez mais importante para o Portugal Vilela Advogados. Com o aumento constante das ameaças cibernéticas, é fundamental que adotemos medidas de segurança robustas para proteger nossos sistemas, dados e informações.

Este documento é um conjunto de diretrizes e procedimentos que visam garantir a confidencialidade, integridade e disponibilidade das informações do escritório. A política estabelece as regras para o acesso, uso, armazenamento e compartilhamento de informações. Além disso, define as responsabilidades dos colaboradores e os procedimentos de resposta a incidentes de segurança. Com uma política de segurança da informação bem definida e implementada, podemos reduzir significativamente os riscos de perda ou comprometimento de informações valiosas.

Objetivo

Assegurar a conformidade com leis e regulamentos aplicáveis relacionados à privacidade e segurança da informação. Isso inclui a implementação de medidas de segurança física e lógica, bem como o treinamento e conscientização dos colaboradores sobre as melhores práticas de segurança da informação. Em resumo, a política de segurança da informação é uma ferramenta essencial para proteger as informações críticas do escritório e garantir sua continuidade de negócios.

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

Política de Requisição e Tratamento de Dados

O Tratamento de dados pessoais sob responsabilidade do Portugal Vilela deverá ser realizado de acordo com as leis aplicáveis, bem como com sua Política Interna de Proteção de Dados, observando os seguintes princípios:

1. Os dados pessoais, incluindo os sensíveis, devem ser obtidos de forma justa e legal. Sempre que necessário, o consentimento expresso do Titular dos dados deverá ser obtido de forma clara e inequívoca;
2. A coleta de dados pessoais deve ser realizada apenas com finalidades específicas, explícitas e legítimas, sendo vedado o tratamento dos dados para outros fins;
3. O compartilhamento dos dados com terceiros somente se dará para as finalidades previamente especificadas ou de outra forma permitida ou exigida pelas leis aplicáveis;
4. O Portugal Vilela sempre implementará os controles e procedimentos técnicos e organizacionais apropriados para garantir a segurança dos dados pessoais, incluindo os sensíveis, evitando acesso e/ou divulgação não autorizados;
5. O Titular dos dados tem o direito à informação sobre os dados tratados, exceto se sua disponibilização for impossível ou exigir esforço desproporcional do Portugal Vilela;
6. A retenção dos dados pessoais será por período não maior que o indispensável para as finalidades específicas para que foram obtidas, exceto quando exigido prazo diverso pela lei ou regulamento aplicável ou quando período diferente constar no consentimento específico obtido;

Política de Conscientização dos Colaboradores Quanto à Utilização de Dados

Para a adequada implantação e cumprimento da Política de Proteção de Dados do escritório, o Portugal Vilela:

1. Realizará um programa de treinamento para orientação de advogados e colaboradores sobre a cautela e os processos necessários para o tratamento dos dados pessoais, nos termos de sua Política. A importância da proteção de dados pessoais será, ainda, reiterada no dia a dia. Os treinamentos terão como base, no mínimo, a Política de Proteção de Dados, o Estatuto da Advocacia e a LGPD;
2. Nomeou um DPO, a quem cabe colaborar para a estratégia de privacidade dos Dados Pessoais tratados pelo escritório, bem como para o controle da sua eficácia. O DPO está encarregado ainda de responder e atender aos Titulares de Dados e à ANPD;
3. Disponibilizará as informações de contato do DPO em todos os seus canais de comunicação;

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

4. Constituiu, para apoiar o DPO, um Comitê de Privacidade e Proteção de Dados Pessoais, composto pelo mínimo de três membros, sendo: o DPO; um representante da área de Tecnologia e Segurança de Informação e um sócio gestor;
5. Treinamentos e reuniões deverão ser sempre registrados, para posterior consulta, seja por atas ou por gravação.

Política de Seleção, Contratação e Gestão de Pessoas

No processo de seleção de advogados e colaboradores, o Portugal Vilela garantirá:

1. Fontes seguras para coleta de dados;
2. Transparência aos titulares que sempre terão informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais. No processo de seleção, logo após a coleta de dados, deverá ser enviado aos candidatos um Aviso de Privacidade, no qual estejam dispostos esclarecimentos sobre o uso dos dados coletados durante o recrutamento;
3. Será coletado somente os dados necessários para a realização de sua finalidade. Assim, os formulários de inscrição devem conter apenas dados pertinentes e não excessivos para que seja feita a seleção. No momento da contratação, no entanto, poderão ser pedidas mais informações para a assinatura do contrato e formalização do ingresso no escritório;
4. Zelo por dados sensíveis eventualmente coletados por serem essenciais ao processo de seleção e admissão. Neste caso, será solicitado o consentimento do candidato para sua coleta e uso de forma clara e destacada;
5. Armazenamento de dados em software seguro com permissões claras e rigorosas;
6. A definição quanto ao prazo de armazenamento e que este esteja atrelado à finalidade para que foi coletado. Em relação ao processo seletivo, os dados coletados devem ser apagados tão logo acabe tal seleção, caso o candidato não seja contratado. Em havendo banco de currículos, o titular dos dados deve concordar com esse uso e ser informado sobre o prazo de manutenção na base de dados do escritório;
7. Canal de atendimento para que o candidato, o advogado e o colaborador, como titulares de dados pessoais, tenham direito de obter informações sobre o uso de seus dados pessoais. Por este canal, o titular poderá solicitar acesso aos dados coletados, correção de seus dados, exclusão, informações sobre compartilhamento, revogação do consentimento e informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
8. A todos os advogados e colaboradores será entregue uma cópia da Política de Proteção de Dados do escritório, mediante recibo e compromisso de cumprimento de seus preceitos;
9. O setor responsável pela seleção, contratação e gestão de pessoas deverá cuidar para que dados pessoais sejam compartilhados exclusivamente para o processo de

seleção e/ou para a execução do contrato firmado com o advogado/colaborador. Em qualquer caso, aquele que recebeu o dado por compartilhamento deverá firmar compromisso formal de respeito irrestrito aos preceitos da Lei Geral de Proteção de Dados.

Política de Gestão de Clientes, Parceiros, Fornecedores e Prestadores de Serviços

O Portugal Vilela requererá que clientes, parceiros, fornecedores e prestadores de serviços com quem porventura compartilhe dados pessoais em razão do exercício de suas atividades, declarem-se expressamente em conformidade com os preceitos da LGPD e com a Política Interna de Proteção de Dados.

Política de Gestão de Recebimento de Dados Pessoais

1. Os dados pessoais devem prioritariamente ser coletados junto aos Titulares com a utilização do e-mail corporativo;
2. Caso os dados coletados não sejam do Titular que contratou com o escritório, deverá: (a) ser obtida autorização expressa e formal do Titular para seu tratamento na consecução de trabalho contratado por terceiro; ou, (b) solicitar ao Titular que envie tais dados por e-mail diretamente ao escritório com a indicação formal a que se destinam;
3. Todos os dados pessoais e documentos que contenham dados pessoais, deverão ser salvos dentro da rede Sharepoint, não sendo permitido que tais documentos e peças estejam no desktop do computador, aplicativos de nuvem que não o do escritório, tablet ou celular do colaborador;
4. Documentos físicos recebidos no escritório ou diretamente pelos colaboradores, seja qual for a forma e o local de recebimento, deverão ser protocolizados no livro de protocolo, que ficará em poder do Setor Administrativo, anotando data de entrada, remetente/destinatário, e, após a digitalização de tal documento, a via física deverá ser devolvida ao cliente, também mediante protocolo, no prazo de 48 horas ou picotado se expressamente autorizado pelo Titular.

Política de Utilização de Dispositivos Pessoais

1. Os advogados e colaboradores do escritório deverão manter senhas atualizadas e autenticação em dois fatores em aplicativos de conversas eventualmente usados para tratar com titulares de dados pessoais;
2. Os advogados e colaboradores do escritório deverão priorizar sempre a comunicação por e-mail quando ela envolver troca de documentos e dados pessoais, evitando ao máximo que esse processo se dê por troca de mensagens via WhatsApp ou outro aplicativo de comunicação;

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

3. Excepcionalmente, se recebidos documentos e dados pessoais por aplicativos de comunicação, deverá o advogado ou colaborador que o recebeu promover o seu imediato salvamento no Sharepoint e sua exclusão definitiva do aplicativo.

Política de Mesas e Telas Limpas

1. Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devendo ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário de expediente;
2. Informações sensíveis devem ser trancadas em local separado e seguro;
3. Não anotar informações pessoais em quadros brancos;
4. Anotações, recados e lembretes não devem ser deixados a mostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;
5. Não deixar ou guardar pastas com documentos pessoais em locais de fácil acesso;
6. Picotar/fragmentar documentos impressos antes de jogá-los fora;
7. Evitar imprimir documentos apenas para leitura, priorizando a leitura digital sempre que possível;
8. Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
9. Computadores pessoais e terminais de computadores e impressoras terão configuração de desligamento automático por inatividade durante 10 (dez minutos), ainda assim, deverão ser bloqueados em caso de afastamento da estação de trabalho;
10. Pertences pessoais devem ser evitados, mas os necessários devem ser mantidos em gavetas ou armários;
11. Nunca escrever senhas em lembretes e nem escondidas no local de trabalho;
12. Não deixe mídias, como pen drives ou certificados digitais, nos drivers;
13. Evitar que telas de monitores fiquem voltados para a entrada do escritório;
14. Ao final do dia de trabalho, ou no caso de ausência prolongada da estação de trabalho, limpar a mesa, guardar documentos, trancar as gavetas e armários e desligar o computador;
15. Manter gavetas e armários fechados, evitando deixar as chaves na fechadura.

Política de Atendimento aos Titulares

Quanto o Titular formular qualquer solicitação ao escritório sobre o tratamento de seus dados pessoais, devem ser adotados os seguintes procedimentos:

1. Toda solicitação relacionada a dados pessoais deve ser formalizada através do e-mail lgpd@portugalvilela.com.br, direcionado ao DPO do escritório. Se implantada ferramenta de Portal do Titular no site do escritório, as solicitações somente serão aceitas por esta ferramenta;

2. Recebido o e-mail de que trata o item anterior, o DPO deve, primeiramente, conferir se o endereço do remetente confere com o endereço do Titular constante em seu cadastro junto ao setor administrativo. Caso:
    a. não haja a coincidência, o e-mail recebido deve ser respondido no sentido de que o Titular deve reenviar sua solicitação pelo e-mail cadastrado, sem que esse e-mail seja fornecido, evitando-se, assim, o fornecimento de dados para não titulares;
    b. não haja endereço de e-mail no cadastro do Titular, o DPO deverá convocar o Comitê para decidirem a melhor forma de conferir a identidade do Titular que solicitou informações;
    c. havendo coincidência nos endereços de e-mail, o DPO deverá iniciar os procedimentos de resposta ao Titular.
3. Para resposta ao Titular, o DPO deve iniciar as pesquisas relacionadas aos dados do Titular, sejam os estruturados, por varredura em sistemas, e não-estruturados, por consulta a planilhas, e-mails e outros aplicativos de armazenamento, e físicos, por consulta aos arquivos do escritório.
4. Também deverá o DPO verificar se houve compartilhamento de dados do Titular e por qual motivo.
5. Levantados os dados, o DPO deve convocar o Comitê para formularem a resposta ao Titular, enviando-a na sequência.
6. Todo o processo acima descrito deve ser realizado em no máximo 03 (três) dias úteis.

Política de Proteção de Dados no Uso dos Recursos de Ti

O Portugal Vilela permanentemente busca soluções e inovações tecnológicas capazes de proporcionarem a proteção de dados pessoais, senso que atualmente tem-se:

1. O estabelecimento de controle de acesso às informações;
2. A utilização do ambiente Firewall de Borda;
3. A utilização de Antivírus Corporativo Endpoint;
4. O acesso externo para o ambiente interno em que as permissões e autenticações seguem os sistemas de segurança interno;
5. A utilização do Programa Office 365, com serviço de correio embarcados com serviços de antivírus e antispywares, além de ferramentas de Compliance e Segurança;
6. Arquivos salvos em drive específico, com todos os níveis de segurança e permissões definidos pelo escritório;
7. A utilização de sistema interno para acompanhamento de processos, cujo controle de acesso é realizado pelos Servidores Windows e pelo próprio sistema;
8. A exigência de substituição de senha regular para o Sistema Windows;
9. A utilização de autenticação em dois fatores para o Programa Office/Teams;
10. Consolidação do armazenamento de dados não estruturados em único repositório.

Política de Proteção Contra Malware

Uma das principais ameaças relacionadas à segurança da informação é a infecção por softwares maliciosos (malware), que tem o objetivo de comprometer o ambiente tecnológico das instituições. Essa norma de uso tem a finalidade de garantir que medidas de proteção, detecção e correção sejam estabelecidas para resguardar a estrutura tecnológica da informação e comunicação do Portugal Vilela. Tem como objetivo orientar aos advogados e colaboradores na utilização de soluções de proteção contra *malware*.

1. Usar a política de controles criptográficos nas máquinas do Portugal Vilela como uma forma de precaver contra ataques de malware que tenham como objetivo modificar informações sensíveis, armazenadas, processadas ou compartilhadas no parque computacional;
2. Definir um software de antivírus que possua uma base de dados atualizada com relação aos novos ataques, interface de usuário intuitiva, mecanismos de detecção e remoção de malware eficazes, escaneamento completo do sistema e ferramentas integradas, tais como: módulos de firewall, AntiSpam, controle de conteúdo na web, verificador de versões de softwares, dentre outras;
3. A solução contra vírus e malwares deve observar uma atualização célere para com as novas ameaças. Convém que o antivírus realize o monitoramento do tráfego de dados do Portugal Vilela e realize o bloqueio sempre que o administrador e/ou o comitê julgue necessário;
4. Só é permitido a utilização de softwares devidamente licenciados e originais. É vedado a instalação, armazenamento e execução de softwares e sistemas piratas e/ou sem licença de uso. A utilização de softwares originais nas máquinas do Portugal Vilela garante maior segurança, estabilidade e proteção aos negócios;
5. Um plano de ação deve ser definido quando ocorrer uma invasão e/ou ataque de ransomware, cybercriminosos, infecção por malwares dentre outros, e os papéis e responsabilidades sejam definidos especificando suas atuações durante o processo a fim de mitigar e eliminar os potenciais riscos envolvidos. Convém que este plano defina os responsáveis pela decisão de mitigar, evitar, transferir ou aceitar os riscos que este representa para o Portugal Vilela. Todas as tomadas de decisões efetuadas por cada responsável devem ser registradas;
6. Convém que o administrador geral das máquinas faça uma análise, sempre que necessário, a necessidade de uso de IDS e IPS para evitar ataques do tipo DoS e DDoS;
7. Convém que simulações de invasão e ataques de malware dentro do Portugal Vilela, seja executado periodicamente a fim de verificar se as medidas de precaução adotadas são eficazes e coerentes aos objetivos para qual foram projetadas. Os resultados deste teste devem ser registrados em relatórios e armazenados para consulta;

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

8. É vedado aos usuários finais a instalação de aplicativos e/ou softwares nas máquinas do Portugal Vilela, tal prerrogativa é da equipe de TI, que possui autorização e treinamentos apropriados;
9. Convém que seja realizado a implementação de controles para proteção dos equipamentos do Portugal Vilela, que permitam a filtragem de rede de envio, bem como a criação de deny list;
10. Todos os softwares padrões do Portugal Vilela devem ser testados e analisados pela equipe de TI, sendo verificados e atualizados com periodicidade de 6 meses ou em caso de uma necessidade repentina, como por exemplo, o ciclo de vida vencido ou mal funcionamento;
11. Documentar procedimento para difusão de notícias relevantes que possam orientar os usuários finais para evitar que sofram ataques e/ou exponha a rede do Portugal Vilela para cybers criminosos.

Política de Gerenciamento de Mudanças

O processo de Gerenciamento de Mudanças é responsável por garantir que métodos e procedimentos padronizados sejam utilizados para avaliar, aprovar, implantar e revisar todas as mudanças na infraestrutura e desenvolvimento de TI de maneira eficiente, a fim de minimizar o impacto relacionado aos serviços e aos clientes. O processo de Gerenciamento de Mudanças tem como objetivo:

1. Responder aos requerimentos de mudanças necessárias nos serviços, maximizando o valor e reduzindo incidentes, rupturas e retrabalhos;
2. Responder às solicitações de negócio e de TI para mudanças que alinharão os serviços com as necessidades do escritório;
3. Assegurar que as mudanças sejam registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas e implementadas.
4. As diretrizes gerais desta política, são:
5. Documentar a mudança dos sistemas operacionais, avaliando o seu impacto e o desempenho das partes interessadas;
6. Deve possuir um plano de mudança analisando se realmente é necessário efetuar essa mudança no ambiente tecnológico;
7. Realizar atualizações de softwares e sistemas só após a validação e verificação dessas atualizações e analisar se essas mudanças não irão oferecer algum tipo de impacto;
8. Implementar medidas que sirvam como precaução, antes de realizar a mudança, para garantir e resguardar a informação sensível;
9. Monitorar mudanças nas políticas de implementação dos cookies do site do Portugal Vilela, analisando se estes não estão armazenando dados sensíveis dos usuários;

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br

Política de Classificação da Informação

A informação é um elemento essencial para todos os processos de negócio de qualquer organização, sendo por tanto o ativo mais valioso, devendo ser protegido e cuidado através de normas, regras, procedimentos e políticas. O propósito deste documento é estabelecer e apresentar diretrizes de condutas adequadas de Segurança da Informação e Proteção de Dados do Portugal Vilela e Advogados, além do compromisso em resguardar as informações que estão sob a guarda do escritório.

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos advogados e colaboradores, são de propriedade e direito exclusivo do Portugal Vilela e Advogados.

Os advogados e colaboradores devem zelar para que as informações inseridas nos sistemas, ou quando enviadas ao cliente, sejam livre de erros, transparentes e verídicas.

Todo e qualquer documento correspondente, bem como produzido pelo Portugal Vilela, não poderão sair da empresa sem que seja por meio de protocolo de envio de documentos.

Quando necessária troca de informações com os clientes para cumprimento legal de obrigações, é necessário utilizar os canais oficiais disponibilizados pela empresa. Qualquer canal distinto ao que foi definido pelo Portugal Vilela é considerado um descumprimento das regras de segurança da informação.

Concessão, Revogação, Revisão e Descarte

A concessão de acesso aos recursos tecnológicos do Portugal Vilela deve estar atrelada aos perfis de acesso previamente atribuídos ao colaborador em razão da sua atividade profissional exercida.

A solicitação de acesso deve ser realizada pelo gestor do advogado ou colaborador, ao responsável de tecnologia via sistema de chamados com todas as informações do usuário cadastrado.

Todos os acessos concedidos serão revisados, no mínimo, a cada 6 (seis) meses, a fim de garantir que continuam ativos e atualizados. Assim como, será realizado uma alteração nas senhas de acesso para um controle efetivo da segurança das informações.

A revogação de acesso deve ocorrer mediante solicitação do gestor responsável pelo advogado ou colaborador, ao responsável de tecnologia. No entanto, os direitos de acesso podem ser alterados e/ou revogados a qualquer tempo pelo Portugal Vilela, sem a necessidade de aviso prévio.

O acesso aos recursos tecnológicos será revogado imediatamente em caso de encerramento das atividades entre o Portugal Vilela e as partes envolvidas. Portanto, assim que algum advogado ou colaborador for demitido ou solicitar demissão, o responsável de TI tomará as providências necessárias.

Nos casos em que houver a inutilização de mídias móveis, como pen-drive, HD, CD, dentre outros, quando forem descartados deverão ser eliminados definitivamente, sendo triturado todo seu conteúdo.

Objetivo

A Política de Segurança da Informação tem por objetivo instituir diretrizes estratégicas que permitam aos advogados e colaboradores seguirem padrões de comportamento e conduta relacionados à segurança da informação e proteção de dados.
A finalidade desta Política é preservar as informações no que diz respeito à:

- **Confidencialidade**: a informação só pode ser acessada, manuseada e atualizada por pessoas devidamente credenciadas;
- **Integridade**: fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações, exclusões e processamentos, com a garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Ética**: assegurar que as informações sejam utilizadas dentro dos preceitos aqui estabelecidos e em hipótese alguma, violando as normas internas desta política ou das leis vigentes;
- **Sigilo**: assegurar que as informações sejam utilizadas apenas para finalidade autorizada;
- **Autenticidade**: garantia de veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Uso dos Recursos de Tecnologia da Informação e Comunicação

O advogado ou colaborador deve utilizar apenas softwares e hardwares previamente homologados ou autorizados pelo responsável de tecnologia da Portugal Vilela.
A gestão (instalação, manutenção e configuração) de todos os recursos tecnológicos é de responsabilidade exclusiva do responsável de tecnologia.
Todo advogado e colaborador que se distanciar de sua estação de trabalho ou dispositivo móvel, deve imediatamente realizar o processo de bloqueio do equipamento.
Os equipamentos disponibilizados aos advogados e colaboradores são de propriedade do Portugal Vilela, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da organização, bem como cumprir as recomendações e normas mencionadas neste documento.

As estações de trabalho e servidores contêm softwares de antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus, problemas na funcionalidade ou identificação de dispositivo estranho conectado ao computador, deverá acionar o responsável de TI.
Documentos imprescindíveis para as atividades dos advogados e colaboradores deverão ser salvos em drives de rede conforme orientação do responsável de TI. Esses arquivos não podem ser gravados apenas localmente nos computadores, para evitar perda ou não abrangência da garantia de backup.

Gestão da Informação

Todas as informações sigilosas, físicas ou digitais, independente do formato ou local de armazenamento, do Portugal Vilela ou de seus clientes, devem ser classificadas e rotuladas de forma a permitir facilmente a identificação e o tratamento adequado, ou seja, deve ficar claro quem pode ter acesso a ela e qual nível de proteção que deve receber.

Os dados terão tratativa conforme definido na LGPD, com tratamento, armazenamento, *backup*, consulta, modificação, anonimização, compartilhamento, exclusão, e todos os demais pontos definidos em lei.

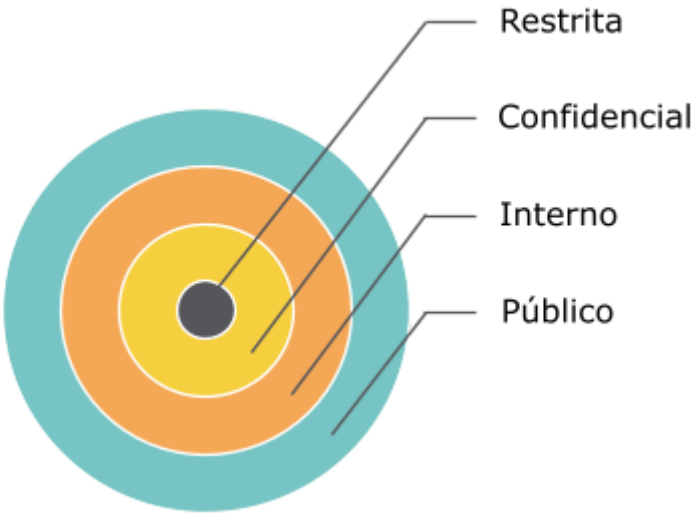
Permissões Privilegiadas

Alguns cargos, de acordo com a definição de alçadas, cargos ou funções, podem ter permissões diferenciadas para o acesso e uso dos recursos tecnológicos, a fim de atender aos objetivos da empresa.
Excepcionalmente, podem ser concedidas autorizações adicionais, temporárias ou não, aos demais advogados e colaboradores, desde que tal solicitação seja aprovada, justificada e necessária para a execução de determinadas tarefas ou projetos.

Níveis De Sensibilidade Para Informações

Os níveis de sensibilidade abaixo permitem que os dados e informações possam ser identificados como:

+55 (31) 3506 8200 • Rua Paraíba, 1.000, 9º andar • Savassi • Belo Horizonte/MG • CEP 30130-145 • portugalvilela.com.br



Público: Qualquer informação que seja declarada pública ou aprovada para uso público. Sua divulgação não causa qualquer dano ao Portugal Vilela.

Acesso: Pode ser acessado por:
- ✔ Usuários internos e externos;
- ✔ Clientes e prestadores de serviço;
- ✔ Público em geral.

Cópia: Sem restrições.
Guarda: Sem restrições.
Correio Convencional: Sem restrições.
Correio Eletrônico: Sem restrições.
Destruição: Sem procedimento especial.

Interno: Determina o acesso exclusivo por advogados e colaboradores do escritório Portugal Vilela Advogados. Se refere a informações que não possuem segredo de negócio ou que não comprometem a imagem e reputação do escritório.

Acesso: Usuários internos.
Cópia: Para fins de conhecimento e replicação interna.
Guarda:
- ✔ Física: Dentro do ambiente do escritório Portugal Vilela;
- ✔ Digital: Nos repositórios do escritório Portugal Vilela.

Correio Convencional:
- ✔ Envolver em envelope sem identificação do nível de classificação da informação;
- ✔ Utilizar serviço de correspondência normal.

Correio Eletrônico: Enviar sem proteção.
Destruição: Sem procedimento especial.

Confidencial: Indica que tem forte restrição de uso e tem um nível de confidencialidade maior. A divulgação não autorizada desta informação pode causar impacto ao negócio do Portugal Vilela e/ou ao negócio do cliente.

Acesso: Esta informação pode ser acessada por:
- ✔ Usuários internos autorizados;
- ✔ Clientes que tenham relação com as informações.

Cópia:
- ✔ Pode ser copiada para fins comerciais;
- ✔ Para conhecimento interno previamente autorizado.

Guarda:
- ✔ Física: Deve ser mantida trancada quando não estiver sendo usada;
- ✔ Digital: Deve ser armazenada com acesso restrito.

Correio Convencional:
- ✔ Fechar o envelope com a marca da classificação Confidencial;
- ✔ Colocar o envelope no interior de um outro sem classificação;
- ✔ O Gestor deverá avaliar o uso do serviço de correspondência adequado à informação.

Correio Eletrônico:
- ✔ O destinatário é um endereço pessoal e não uma lista de transmissão;
- ✔ Enviar anexos somente com cifrado com senha;
- ✔ Enviar a senha do anexo somente por outro meio de comunicação;
- ✔ Utilizar certificação digital sempre que possível;

Destruição:
- ✔ Internamente: Destruir a informação conforme especificado na Política de Classificação da Informação – Concessão, Revogação, Revisão e Descarte.
- ✔ Em parceiro, clientes e fornecedores: O advogado ou colaborador deverá orientar quanto a destruição das informações categorizadas como confidenciais de forma supervisionada, de modo a garantir a eliminação completa;

Restrita: Indica que esta informação é sensível e somente pode ser acessada por usuário da informação explicitamente indicado pelo nome. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio do escritório Portugal Vilela Advogados.

Acesso: Usuários internos explicitamente indicados.
Cópia: Vedado qualquer modalidade de cópia ou fotocópia.
Guarda:
- ✔ **Física:** Deve ser mantido trancado quando não estiver em uso;

- ✔ **Digital:** Arquivado com restrição máxima;

Correio Convencional:

- ✔ Fechar o envelope com a marca da classificação Restrito;
- ✔ Colocar o envelope no interior de outro sem classificação;
- ✔ Utilizar serviço de correspondência SEDEX ou equivalente.

Correio Eletrônico:

- ✔ O destinatário é um endereço pessoal e não uma lista de transmissão;
- ✔ Enviar anexos somente com cifrado com senha;
- ✔ Enviar a senha do anexo somente por outro meio de comunicação;
- ✔ Utilizar certificação digital sempre que possível.

Destruição:

- ✔ **Internamente:** Destruir a informação conforme especificado na Política de Classificação da Informação – Concessão, Revogação, Revisão e Descarte.
- ✔ **Em parceiros, clientes e fornecedores:** O colaborador deve orientar quanto a destruição das informações categorizadas como confidenciais de forma supervisionada, de modo a garantir a eliminação completa.

Papéis, Responsabilidades e Obrigações

Compete para os assuntos relacionados à política de classificação da informação:

Departamento de TI:

- ✔ Cabe ao TI juntamente com os gestores de área, identificar quais os níveis de proteção necessárias para os ativos de informação alocados nos recursos de TI do escritório;
- ✔ Garantir que os controles sejam eficazes e acessados somente por usuários internos autorizados, que utilizem totalmente as exigências do nível de segurança.

Aos usuários finais, inclusive sócios, seniores, gestores de áreas, dentre outros, quando atuem nessas condições:

- ✔ O gestor de área ou superior deve realizar periodicamente um processo de análise de classificação, para avaliar se as informações permanecem com o mesmo nível de sigilo ou se deve ser solicitada a reclassificação;
- ✔ É dever do gestor de área, revisitar os direitos de acesso aos repositórios partilhados a cada 6 meses e replicar as instruções;
- ✔ É dever do gestor de área, onde houver tratamento de DP, preencher o DPIA e atualizá-lo sempre que houver nova alteração, necessidade, ou a cada 6 meses;
- ✔ Os originadores das informações devem redobrar a atenção quando as informações são acessadas por usuários externos, e aplicar um nível de segurança mais alto para proteger as informações.