



**ALVES FERNANDES**  
ADVOGADOS

---



**ALVES FERNANDES**  
ADVOGADOS

## *A Empresa*



Devidamente registrada na OAB/GO e inscrita sob o número 582. Foi fundada em 08 de março de 2004 com o nome de **Toscan e Fernandes Advogados** e teve seu nome alterado, devido a uma alteração contratual em 29 de novembro de 2013, quando passou a se chamar **Alves Fernandes Advogados**.

Seus membros possuem vasta experiência nas áreas de contratos de crédito bancário, consorcio, leasing, alienação fiduciária, Finame, contratos de câmbio, operações de desconto e redesconto de títulos, cheque especial, cartões de crédito, crédito imobiliário, títulos de crédito industrial, falências, recuperação judicial, ações revisionais, pedidos indenizatórios, execuções fiscais, recuperação de crédito e outras.

Atua principalmente nos estados de **Amazonas, Amapá, Acre, Goiás, Minas Gerais, Tocantins, Paraíba, Rondônia** e no **Distrito Federal**.



## **Visão**

O constante aprimoramento da equipe e o pleno domínio do conhecimento da legislação, jurisprudência e doutrina que regem o Direito Comercial, Empresarial, do Consumidor e Securitário no Brasil, nos garantem as condições necessárias para oferecermos aos nossos clientes um serviço de qualidade e focado em resultados.

## **Missão**

Oferecer aos clientes da **Alves Fernandes Advogados** as melhores condições para a resolução de problemas jurídicos nas áreas de sua atuação, buscando ao máximo evitar a judicialização das questões jurídicas e longas demandas.

## **Valores**

- EXCELÊNCIA na prestação de serviços.
- AGILIDADE na resolução de problemas.
- TRANSPARÊNCIA nas relações com os clientes.
- PREVENÇÃO buscando evitar longos e demorados processos.
- APRIMORAMENTO constante da equipe profissional.

## *Áreas de Atuação*

Estamos em constante processo de capacitação para melhor atender nossos clientes!

### **Direito Comercial / Empresarial / do Consumidor**

Atuamos no **Direito Comercial, Empresarial e do Consumidor** na elaboração e exame de contratos de crédito bancário, consórcio, leasing, alienação fiduciária, Finame, contratos de câmbio, operações de desconto e redesconto de títulos, cheque especial, cartões de crédito, crédito imobiliário, títulos de crédito industrial, falências, recuperação judicial, ações revisionais, pedidos indenizatórios, execuções fiscais, recuperação de crédito, relações de consumo, disputas envolvendo a propriedade intelectual, relações de prestação de serviços entre duas ou mais empresas, nas esferas judicial e extrajudicial.

### **Recuperação de crédito**

Atuamos na área de **Recuperação de Crédito** buscando a liquidação de dívidas pendentes de clientes das empresas para as quais prestamos serviços judicial e extrajudicialmente.

### **Seguros**

Defendemos os interesses de nossos clientes em assuntos oriundos de questões securitárias, também no âmbito judicial e extrajudicial.



## *A Equipe*

Nossa equipe é composta por advogados, bacharéis e estagiários com larga experiência nas áreas em que atuamos.

## *Alguns Clientes*



## *Dados para contato*

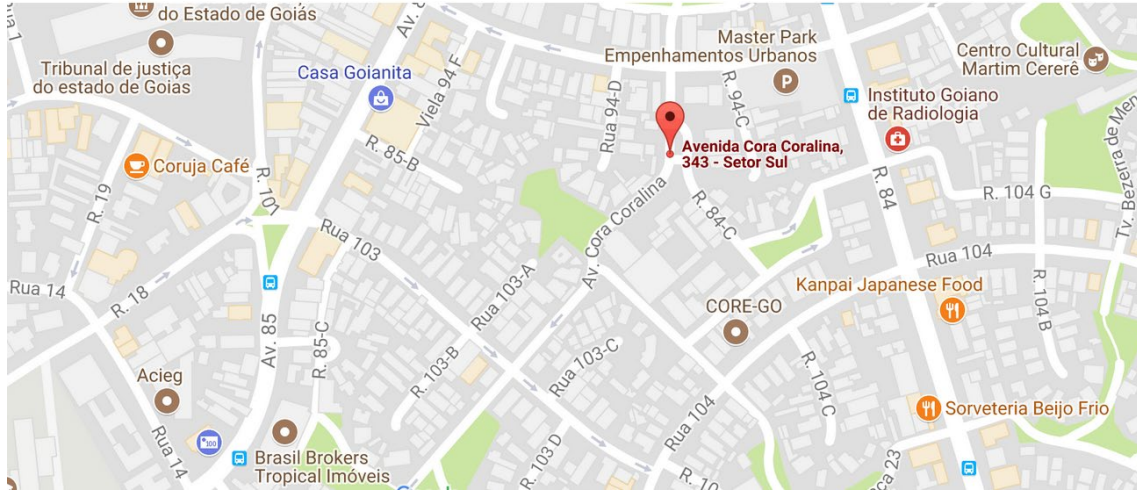
**Endereço:** Av. Cora Coralina, 343, Setor Sul, Goiânia - GO.

**Fone:** (62) 3237-1100

**E-mail:** [sac@alvesfernandes.adv.br](mailto:sac@alvesfernandes.adv.br)

**Horário:** Segunda - Sexta: 8:00 - 18:00.

## Localização



## *Segurança da Informação*

- Diretrizes de Segurança da Informação
- Política de Segurança da Informação
- Política de Confidencialidade
- Política de Privacidade
- Plano de Controle e Monitoramento de Riscos
- Plano de Contingência

## **Diretrizes de Segurança da Informação**

### **DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO**

## **DIRETRIZES**

1. Assegurar a confidencialidade, integridade e disponibilidade das informações da Organização, mediante utilização de mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo.
2. Garantir a proteção adequada das informações e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados.
3. Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização, estando sujeitos à monitoração e auditoria.
4. Assegurar o acesso dos colaboradores à Política de Segurança da Informação na íntegra, e em local de fácil acesso.
5. Garantir o cumprimento dessa Política e das Normas de Segurança da Informação da organização.

**ALVES FERNANDES ADVOGADOS**

## Política de Segurança da Informação

Departamento de Tecnologia da Informação

Goiânia

2023

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Departamento de Tecnologia da Informação

**Responsável por estudo e elaboração:**

Silvério Silva Ribeiro – Especialista em Segurança da Informação

**Responsável pela revisão e aprovação:**

Ailton Alves Fernandes – Sócio Gestor



## **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

### **1. OBJETIVO**

A Política de Segurança da Informação é uma declaração formal da **ALVES FERNANDES ADVOGADOS** acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos envolvidos diretamente e indiretamente com a organização.

### **2. ABRANGÊNCIA**

Todos os colaboradores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da **ALVES FERNANDES ADVOGADOS**, suas Unidades, subsidiárias e/ou coligadas.

### **3. MISSÃO**

Garantir a integridade, confidencialidade, legalidade e autenticidade das informações necessárias para a realização dos negócios da **ALVES FERNANDES ADVOGADOS**.

### **4. DOCUMENTOS DE REFERÊNCIA**

ISO/IEC 27001

ABNT 21:204.01-010

Lei 9.609/1998 – Lei do Software

Lei 12.965/2014 – Marco Civil

Lei 13.709/2018 - LGPD

### **5. TERMOS E DEFINIÇÕES**

TI: Tecnologia da Informação

Software: é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

**Backup:** é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

**Mídias Removíveis:** dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

**USB:** é um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

**VPN (Virtual Private Network):** modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por Colaboradores em trânsito.

**Softwares de Mensageria:** são programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

**Firewall:** é um dispositivo de rede que tem por objetivo aplicar uma política de segurança e regras na rede de computadores.

**Modem 3G:** é um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G), notebooks, netbooks, desktops, etc. objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G.

## **6. DIRETRIZES**

### **6.1. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO**

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, que é a disponibilização das informações conforme as regras de negócios.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

A Política de Segurança da Informação da **ALVES FERNANDES ADVOGADOS** deverá ser aprovada e revisada anualmente pela Diretoria.

## **6.2. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO**

### **6.2.1. Definição**

Cabe a todos os Colaboradores (Colaboradores, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **ALVES FERNANDES ADVOGADOS**; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a organização quando do descumprimento ou violação desta política.

## **6.2.2. Diretoria, Gerências e Coordenações**

Cabe à Diretoria, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação. Para tal após treinamento de integração ou reciclagem, o colaborador deverá assinar o termo de responsabilidade; e comunicar imediatamente eventuais casos de violação de segurança da informação.

## **6.2.3. Área de Governança de TI**

Cabe à área propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

## **6.3. PROPRIEDADE INTELECTUAL**

6.3.1. É de propriedade da **ALVES FERNANDES ADVOGADOS**, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a **ALVES FERNANDES ADVOGADOS**.

## **6.4. ENGENHARIA SOCIAL**

6.4.1. Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

6.4.2. A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos à organização:

6.4.2.1. Diretos: são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

6.4.2.2. Indiretos: caracterizam-se pela utilização de softwares ou técnicas, como, por exemplo, vírus, cavalos de Tróia ou através de sites maliciosos e e-mails falsos para obter informações privilegiadas desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a oferta tentadora e apagar o e-mail imediatamente.

## **6.5. CLASSIFICAÇÃO DA INFORMAÇÃO**

6.5.1. É de responsabilidade do coordenador de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

6.5.1.1. Pública: é uma informação da **ALVES FERNANDES ADVOGADOS** ou de seus colaboradores com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional.

6.5.1.2. Externa: é destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

6.5.1.3. Interna: é uma informação da **ALVES FERNANDES ADVOGADOS** que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à organização deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da **ALVES FERNANDES ADVOGADOS**.

6.5.1.4. Confidencial: é uma informação crítica para os negócios da **ALVES FERNANDES ADVOGADOS** ou de seus colaboradores. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou ainda, sanções administrativas, civis e criminais à **ALVES FERNANDES ADVOGADOS** ou aos seus colaboradores. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, colaboradores e/ou fornecedores.

6.5.1.5. Restrita: é toda informação que pode ser acessada somente por usuários da **ALVES FERNANDES ADVOGADOS** explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

## **6.6. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO**

6.6.1. As máquinas (servidores) que armazenam os sistemas da ALVES FERNANDES ADVOGADOS estão em área protegida – Centro de Processamento de Dados localizado na unidade de Goiânia / GO.

6.6.2. As entradas ao CPD têm acesso devidamente controlado e monitorado.

6.6.3. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo, Colaboradores, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

6.6.4. Nenhum funcionário deverá sem autorização expressa remanejar equipamentos ou ativos de TI.

6.6.5. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

## **6.7. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA ORGANIZAÇÃO**

6.7.1. Cuidado ao tratar de assuntos da organização dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

6.7.2. Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da organização ou próximos a pessoas desconhecidas.

6.7.3. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da organização.

## **6.8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO**

### **6.8.1. Diretrizes Gerais**

6.8.1.1. Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

## **6.8.2. Diretrizes Específicas**

### **6.8.2.1. Sistemas**

6.8.2.1.1. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

6.8.2.1.2. Cópia de segurança (Backup) deve ser testada e mantida atualizada para fins de recuperação em caso de desastres.

6.8.2.1.3. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços, salvo os colaboradores de infraestrutura de tecnologia da informação.

6.8.2.1.4. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da organização.

6.8.2.1.5. Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”.

### **6.8.2.2. Máquinas – Estação de Trabalho**

6.8.2.2.1. É terminantemente proibido a remoção ou traslado das estações de trabalho ou periféricos sem a expressa autorização da área de tecnologia da informação, via abertura de

chamado. Caso haja inobservância o responsável pelo ato ficará sujeito às penas cabíveis de acordo com as medidas administrativas da organização. Ressaltamos que neste caso a área de tecnologia da informação não se responsabiliza por qualquer dano, extravio, perda de dados ou invasão causado pela inobservância.

6.8.2.2.2. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

6.8.2.2.3. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

6.8.2.2.4. Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os Colaboradores com estações de trabalho, incluindo equipamentos portáteis.

6.8.2.2.5. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da **ALVES FERNANDES ADVOGADOS**, só devem ser utilizadas em equipamentos com controles adequados.

6.8.2.2.6. Os usuários da organização devem utilizar apenas softwares licenciados pela área de Infraestrutura de Tecnologia da informação, nos equipamentos da organização.

6.8.2.2.7. A área de Infraestrutura de Tecnologia da informação deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

6.8.2.3. Boas práticas de segurança para seu notebook

6.8.2.3.1. Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

6.8.2.3.2. Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.

6.8.2.3.3. Não coloque o notebook em carrinhos de aeroportos ou despache junto à bagagem.



6.8.2.3.4. Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

6.8.2.3.5. Evite utilizar o notebook em locais públicos.

6.8.2.3.6. Nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

6.8.2.3.7. Avalie se em pequenas viagens é realmente necessário levar o notebook.

6.8.2.4. Utilização de equipamentos particulares / terceiros dentro da organização

6.8.2.4.1. Notebooks particulares para serem usados dentro da rede da organização abrangidas neste documento, precisam ser avaliados pelo pessoal responsável de TI.

6.8.2.4.2. Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

6.8.2.4.3. É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

#### **6.8.2.5. Boas práticas de segurança para Impressões**

6.8.2.5.1. Documento enviado para a impressão deverá ser retirado imediatamente.

6.8.2.5.2. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da organização.

#### **6.8.2.6. A Instalação de Softwares**

6.8.2.6.1. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

6.8.2.6.2. A organização respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da organização. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na **ALVES FERNANDES ADVOGADOS**.

6.8.2.6.3. A gestão de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

#### **6.8.2.7. Diretrizes quanto à utilização da Rede Corporativa**

6.8.2.7.1. Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

6.8.2.7.2. Somente os empregados que estão devidamente autorizados a falar em nome da organização para os meios de comunicação podem escrever em nome da organização em sites de Bate Papo (Chat Room), grupos de Discussão (fóruns, newsgroups) e mídias sociais. Em caso de dúvidas, procurar a área de Comunicação.

6.8.2.7.3. Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de Tecnologia da Informação a recuperação de arquivos que não respeitem a regra acima citada, tão menos se responsabiliza por arquivos perdidos na máquina local.

6.8.2.7.4. Arquivos que estão na rede com mais de 24 meses sem acesso serão excluídos, salvo as exceções que serão tratadas diretamente com o proprietário do arquivo.

6.8.2.7.5. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

#### **6.8.2.8. Diretrizes quanto ao uso de Mídias Removíveis e da porta USB**

6.8.2.8.1. O uso de mídias removíveis na organização não é estimulado, devendo ser tratado como exceção à regra.

6.8.2.8.2. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modems 3G e os pen drives merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios Colaboradores da organização.

6.8.2.8.3. Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da coordenação do departamento do solicitante. Para notebooks de coordenadores e cargos acima esta liberação é efetuada por padrão.

6.8.2.8.4. Dentro da organização dê preferência à utilização da rede evitando a utilização de modem 3G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

6.8.2.8.5. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

6.8.2.8.6. É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

#### **6.8.2.9. Diretrizes quanto ao uso da Internet**

6.8.2.9.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à organização.

6.8.2.9.2. O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprios e de relacionamentos.

6.8.2.9.3. O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

6.8.2.9.4. É vedado qualquer tipo de download, salvo aqueles liberados pelo departamento de tecnologia da informação via Firewall. Como também o upload de qualquer software licenciado à organização ou de dados de propriedade da organização ou de seus colaboradores, sem expressa autorização do gestor responsável pelo software ou pelos dados.

6.8.2.9.5. Os acessos à internet serão monitorados através de identificação e autenticação do usuário na rede corporativa.

#### **6.8.2.10. Recomendações sobre o uso do Correio Eletrônico (e-mail)**

6.8.2.10.1. É vedado o uso de sistemas webmail externo como forma de comunicação oficial. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da **ALVES FERNANDES ADVOGADOS**.

6.8.2.10.2. É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da organização perante seus colaboradores e a comunidade em geral e que possam causar prejuízo moral e financeiro.

6.8.2.10.3. Evitar utilizar o e-mail da organização para assuntos pessoais

6.8.2.10.4. Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da organização e até mesmo vistoriado por direitos de verificação e auditoria.

6.8.2.10.5. Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

6.8.2.10.6. Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de

vírus, avisos da Microsoft/Avast, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

6.8.2.10.7. Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

6.8.2.10.8. A utilização do e-mail/webmail da organização fora do horário de trabalho deverá seguir as diretrizes quanto ao uso interno.

#### **6.8.2.11. Antivírus**

6.8.2.11.1. Antivírus dos servidores e estações são atualizados automaticamente.

6.8.2.11.2. A varredura por vírus é feita diariamente nas estações e nos servidores.

#### **6.8.2.12. Uso de Softwares de Mensageria**

6.8.2.12.1. A organização permite somente a utilização do Software da Microsoft como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da organização e até mesmo vistoriado por direitos de verificação e auditoria.

6.8.2.12.2. A instalação de software de mensageria e a liberação do acesso são restritas e sua utilização deve ser justificada à Gestão de TI.

6.8.2.12.3. O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

6.8.2.12.4. Sistemas de mensageria possuem histórico de riscos associados à malwares (p.ex. vírus, worms e etc.), de forma que deve ser utilizado com zelo e cuidado.

6.8.2.12.5. O uso de sistemas de mensageria em redes de relacionamento pessoais deve ser evitado no ambiente corporativo, por conta da natural assincronia das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que usualmente torna-se contraproducente.

6.8.2.12.6. O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

#### **6.8.2.13. Controle de Acesso a VPN**

6.8.2.13.1. O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

6.8.2.13.2. É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros Colaboradores.

6.8.2.13.3. O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações da organização abrangidas neste procedimento.

6.8.2.13.4. Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

6.8.2.13.5. Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

#### **6.8.2.14. Controle de Acesso Lógico (Baseado em Senhas)**

6.8.2.14.1. Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

6.8.2.14.2. Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar

informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

6.8.2.14.3. Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

6.8.2.14.4. Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função.

6.8.2.14.5. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.

6.8.2.14.6. A troca ou desbloqueio de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário, através de abertura de chamado.

## **7. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES**

7.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

7.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato e à Diretoria.

# **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Departamento de Tecnologia da Informação

## **VIGÊNCIA E VALIDADE**

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

### **Aprovação:**

Tecnologia da Informação

Sócio Gestor



## Política de Confidencialidade

### **POLÍTICA DE CONFIDENCIALIDADE ALVES FERNANDES ADVOGADOS**

#### **1. Objetivo da Política de Confidencialidade**

O objetivo da Política de Confidencialidade é a preservação do sigilo de todos os dados, informações, documentos e materiais, de qualquer natureza e espécie, dos clientes que forem disponibilizados ou obtidos no exercício de funções ou atividades realizadas pelo escritório **ALVES FERNANDES ADVOGADOS**, salvo aqueles necessários para a defesa do interesse dos clientes nos processos judiciais, administrativos ou arbitrais, sendo que no caso de dados sigilosos, serão adotadas as medidas processuais para assegurar a confidencialidade.

#### **2. Definições**

Pode-se definir por “INFORMAÇÕES CONFIDENCIAIS”, mas não se limitando, toda e qualquer informação escrita, computadorizada, oral ou visual atinente aos seus clientes, recebidas ou obtidas pelas partes abrangidas pela presente Política, no exercício de seu ofício, que não devem ser divulgadas de caráter pessoal, comercial, intelectual ou industrial.

Exemplo de informações/dados considerados sigilosos: concernentes a negócios da própria vida da família; sua apresentação puder violar dever de honra; sua publicidade redundar em desonra à parte ou ao terceiro, bem como a seus parentes consanguíneos ou afins até o terceiro grau, ou lhes representar perigo de ação penal; sua exibição acarretar a divulgação de fatos a cujo respeito, por estado ou profissão, devam guardar segredo; por disposição legal; subsistirem outros motivos graves que justifiquem a confidencialidade; em que o exija o interesse público ou social; que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; em que constem dados protegidos pelo direito constitucional à intimidade; que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

E mais: informações e dados, sejam eles provisórios ou definitivos, de natureza técnica, comercial, financeira, jurídica, estratégica, ou outra, inclusive, e sem limitação, segredos comerciais, rol e dados de clientes, interessados ou parceiros, dados negociais, know-how, sistema de trabalho, informação relacionada à pesquisa, desenvolvimento, tecnologia, invenções, sistemas de informação, planos comerciais, preparação e participação em concorrências públicas ou privadas, ou qualquer outra informação financeira ou econômica, contabilidade, engenharia, marketing, merchandising, vendas e procedimentos judiciais, arbitrais ou administrativos, ajuizados ou não, conflitos potenciais ou efetivos; fontes potenciais de financiamento e capital; e todas as análises, compilações, previsões, estudos, memorandos, anotações, registros de computadores ou outros documentos preparados e fornecidos em conexão com a análise e possível consumação de transações, concorrências públicas ou privadas; os projetos de qualquer espécie, incluindo mas não se limitando a

inovação, desenvolvimento de novos negócios e soluções sustentáveis, investimentos, aportes de capital, negociações com terceiros, seja ente governamental ou privado.

Pode-se definir por “Dono da Informação” - o proprietário do dado/informação; o legítimo possuidor.

### **3. Da Revelação**

Caso seja necessária a revelação de informação protegida pela presente Política de Confidencialidade em razão de obrigação legal de revelar qualquer INFORMAÇÃO CONFIDENCIAL em virtude de ordem judicial ou administrativa, a parte obrigada a revelar as informações deverá notificar o dono da informação para que exerça direito de oposição. Caso a oposição do dono da informação/dado não seja bem-sucedida, a parte instada a revelar informações sigilosas somente poderá revelá-las na extensão exigida pela ordem judicial ou administrativa em questão.

### **4. Do Não Cumprimento**

O não cumprimento da presente Política caracteriza falta grave apta a justificar a rescisão por justa causa de Contrato de Trabalho, se colaborador, e a rescisão motivada do contrato de prestação de serviços, sem prejuízo de outras medidas cabíveis, em especial, indenização por eventuais danos suportados pela quebra de confidencialidade, além da imposição de multa prevista em Termo próprio.

### **5. Das Políticas complementares aplicáveis**

Aplica-se em conjunto com a presente Política, a Política de Privacidade (tratamento de dados pessoais), sem prejuízo de termos e condições adicionais constantes de Termos de Confidencialidade individualmente firmados, com os colaboradores e clientes.

### **6. Da abrangência**

Todo e qualquer profissional que tenha acesso a dados/informações do escritório **ALVES FERNANDES ADVOGADOS** ou de seus clientes/fornecedores em razão do vínculo existente.

### **7. Da Vigência**

Política vigente por deliberação dos sócios e somente poderá ser alterada por deliberação dos mesmos.



**ALVES FERNANDES**  
ADVOGADOS

---

**ALVES FERNANDES ADVOGADOS**

## Política de Privacidade

### POLÍTICA DE PRIVACIDADE ALVES FERNANDES ADVOGADOS

O escritório ALVES FERNANDES ADVOGADOS, atua na prestação de serviços advocatícios e dentre os seus pilares está a proteção de dados e informações pessoais que são compartilhados pelos seus clientes e fornecedores.

#### 1. Considerações iniciais

Os dados são protegidos nos processos de coleta, registro, armazenamento, uso, compartilhamento, enriquecimento e eliminação, em conformidade com a Lei Geral de Proteção de Dados (Lei 13.709/2018).

Portanto, a política de privacidade da ALVES FERNANDES ADVOGADOS se orienta pela legislação e pelos princípios que norteiam sua missão e valores, com a implantação de procedimentos operacionais eficazes na preservação dos dados pessoais e informações pessoais.

Algumas definições legais são importantes para melhor compreensão da política de privacidade:

**Dados Pessoais:** todo aquele que se refira a uma pessoa física identificada ou identificável, podendo ser sensíveis ou não;

**Titular:** pessoa natural a quem se referem dos dados pessoais;

**Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

**Consentimento:** manifestação livre e consciente do titular concordando com o tratamento de seus dados pessoais para uma finalidade determinada.

#### 2. Quais dados são coletados e tratados?

Todos os dados fornecidos pelo titular serão tratados, sendo que a coleta se limita as informações necessárias para melhor eficiência dos serviços jurídicos prestados.

#### 3. Como é feita a coleta dos dados?

- Pelo fornecimento dos clientes e fornecedores, presencial e/ou virtualmente;

- Pelo envio e inserção de dados no site do escritório, para fins de contato com o escritório.

#### **4. Utilização dos dados pessoais**

A **ALVES FERNANDES ADVOGADOS** se torna responsável pelo tratamento dos dados pessoais dos seus titulares, os quais serão tratados para fins de prestação de serviços advocatícios (processo judicial, administrativo ou arbitral), tal como autorizado na Lei 13.709/2018, em seu art. 7º, VI.

O titular dos dados poderá a qualquer momento optar pela exclusão dos dados da base do escritório.

Para manter as informações pessoais seguras, são usadas ferramentas físicas, eletrônicas e gerenciais orientadas para a proteção da privacidade.

A aplicação das ferramentas leva em consideração a natureza dos dados pessoais coletados, o contexto e a finalidade do tratamento e os riscos de eventuais violações poderiam gerar para os direitos e liberdades do titular dos dados coletados e tratados.

Destacam-se as seguintes medidas adotadas:

- Apenas pessoas autorizadas têm acesso a dados pessoais;
- O acesso aos dados pessoais é feito somente após o compromisso de confidencialidade;
- Os dados pessoais são armazenados em ambiente seguro e idôneo.

#### **5. Compartilhamento dos dados pessoais**

Em razão da atuação da **ALVES FERNANDES ADVOGADOS** em processo judicial, administrativo ou arbitral serão compartilhados os dados necessários à defesa do interesse do titular na condição de autor ou réu, sendo que no caso de dados sigilosos, serão adotadas as medidas processuais para assegurar a confidencialidade.

Exemplo de dados considerados sigilosos: concernentes a negócios da própria vida da família; sua apresentação puder violar dever de honra; sua publicidade redundar em desonra à parte ou ao terceiro, bem como a seus parentes consanguíneos ou afins até o terceiro grau, ou lhes representar perigo de ação penal; sua exibição acarretar a divulgação de fatos a cujo respeito, por estado ou profissão, devam guardar segredo; por disposição legal; subsistirem outros motivos graves que justifiquem a confidencialidade; em que o exija o interesse público ou social; que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; em que constem dados protegidos pelo direito constitucional à intimidade; que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

## **6. Transferência dos dados pessoais**

Em caso de necessidade de transferência de dados pessoais, seja a nível nacional ou internacional, os mesmos estarão sujeitos à Lei de Proteção de Dados Pessoais e às demais legislações brasileiras de proteção de dados.

## **7. Direitos do titular dos dados pessoais**

O artigo 18 da Lei Geral de Proteção de Dado determina que:

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- A confirmação quanto a existência de tratamento de dados pessoais e obtenção, a qualquer tempo, do acesso aos seus dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados;
- Informação quanto ao compartilhamento de dados;
- Exclusão dos seus dados pessoais tratados;
- Portabilidade de dados, para outro prestador de serviços, mediante sua requisição;
- Revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

## **8. Conservação dos dados pessoais**

Os dados pessoais são conservados pelo período estritamente necessário para a finalidade que ensejou a coleta e/ou de acordo com prazos legais vigentes. Durante a conservação serão adotados os meios técnicos para evitar a perda, má utilização, alteração, acesso não autorizado e apropriação indevida dos dados pessoais de seus titulares.

## **9. Do descarte**

Os documentos físicos com os dados pessoais após a digitalização serão eliminados, salvo se de caráter histórico ou necessário à manutenção de efeito jurídico considerando o prazo de decadência e prescrição, nos termos da legislação, ou, a critério dos titulares, devolvidos a eles.

## **10. Cookies**

A qualquer tempo e sem qualquer custo as permissões de cookies podem ser alteradas, assim como bloqueadas ou recusadas.

e você deseja remover cookies do seu navegador, as instruções exatas para remoção dependerão do navegador que está sendo utilizado. Na maioria dos navegadores, acesse as Configurações (o ícone de engrenagem), depois, Opções da Internet, e haverá um local para limpar arquivos temporários e cookies.

## **11. Revisão da política de privacidade**

Os termos da presente política serão atualizados ou adaptados no sentido de sempre estarem em consonância com a legislação e as melhores práticas de tratamento de dados e informações pessoais.

## **12. Atendimentos, Reclamações e Dúvidas**

No caso de necessidade de contato relacionado ao tratamento dos dados pessoais e com os direitos que são conferidos pela legislação aplicável e, em especial, referidos nessa política, o **ALVES FERNANDES ADVOGADOS** poderá ser contatado através do e-mail: [sac@alvesfernandes.adv.br](mailto:sac@alvesfernandes.adv.br), [ouvidoria@alvesfernandes.adv.br](mailto:ouvidoria@alvesfernandes.adv.br) ou pelo telefone (62) 3237-1100 ou ainda pelo WhatsApp (62) 98112-1101.

## **13. Encarregado de Proteção de Dados**

O **ALVES FERNANDES ADVOGADOS** disponibiliza os canais de comunicação direta com o encarregado de proteção de dados, Sra. Rhavilla Thuanny Silva Morais: (62) 3237-1100 ramal 1105, e-mail: [advogado1116@alvesfernandes.adv.br](mailto:advogado1116@alvesfernandes.adv.br), celular corporativo (62) 99173-6980.

**ALVES FERNANDE ADVOGADOS**

## Plano de Controle e Monitoramento de Riscos

Risco	Responsável	Ação de controle e monitoramento	Periodicidade
Energia elétrica	Coordenador adm.	Testar as baterias autônomas da empresa, a fim de manter a autonomia máxima de energia. Manter contato com o fornecedor de energia elétrica (gerador), a fim de confirmação da disponibilidade do serviço à empresa.	Semestral
Violação de computadores por vírus, hackers, etc.	Coordenador adm. + Profissionais da TI + Sócios gestores	Confirmar a atualização do antivírus, do firewall e do controle de senhas dos usuários.	Bimestral
Perda de informações/arquivos/sistemas, pane nos recursos de informática reserva.	Coordenador adm. + Profissionais da TI + Sócios gestores	Confirmar o conteúdo das cópias de segurança (back-up) e testar o funcionamento do servidor reserva.	Semestral
Incêndio / Enchente	Coordenador adm. + Sócios gestores + Prestador de serviço	Revisão periódica dos equipamentos de combate a incêndios. Avaliação periódica das Instalações hidráulicas, registros, válvulas, calhas e pontos de infiltração	Anual
Obstrução de acesso principal ao Escritório	Coordenador adm. + Sócios gestores	Revisão periódica dos dois acessos à empresa (principal e secundário), bem como do sistema de acesso remoto aos arquivos e sistema de TI.	Bimestral
Ausência de um ou mais funcionários por um período de tempo significativo	Coordenador adm. + Sócios gestores + Coordenador jurídico	Revisão do sistema de rodízios de funções, a fim de que todos tenham conhecimento das atividades desenvolvidas pela empresa.	Mensal
Acesso a informações sigilosas	Coordenador jurídico + Sócios gestores	Revisão periódica do controle de senhas dos usuários e do sistema de proteção a informações sigilosas.	Semestral
Manutenção e Acondicionamento dos servidores	Coordenador adm. + Sócios gestores + Profissionais da TI	Revisão periódica do sistema de segurança do acesso ao local, do sistema climático e dos equipamentos.	Mensal
Interrupção do serviço de dados e voz	Coordenador adm. + Sócios gestores + Profissionais da telefonia	Avaliação periódica da central telefônica e do aparelho de dados (roteador), bem como dos telefones celulares corporativos.	Semestral
Acesso de terceiro	Coordenador adm + Sócios gestores	Revisão periódica do sistema de identificação e restrição de visitantes no âmbito da empresa, do sistema de cerca elétrica, do sistema do alarme monitorado 24 horas e do sistema de câmeras internas e externas.	Semestral



## Plano de Contingência

Contingência			Procedimento			
Evento	Ação	Responsável	Descrição	Responsável	Tempo objetivado de recuperação em situações de contingência	Prazo máximo / Interrupção tolerável
Interrupção de energia	Comunicar responsável administrativo	Coordenador adm. + Sócios gestores	Manter contato com a Cia elétrica para restabelecer a energia elétrica de forma emergencial e, se houver necessidade, caso a interrupção seja superior ao período de autonomia do escritório (4 horas), contratar energia elétrica de outro fornecedor (gerador) até o retorno através da prestadora de serviço.	Cia elétrica	Imediato, diante do sistema de autonomia do escritório.	24 hs
Violação de computadores por vírus, hackers, etc	Comunicar imediatamente os profissionais da TI	Coordenador a dm. + Sócios gestores	Manter conta to com os profissionais da TI para restabelecimento do computador infecta do, com eliminação da violação e disponibilização do sistema, e, se houver necessidade, substituir a máquina por uma reserva.	Profissionais da TI	Imediato para estação de trabalho e 6 hs para servidor	24 hs.
Perda de informações/arquivos/ sistemas, pane nos recursos de informática	Comunicar imediatamente os profissionais da TI	Coordenador adm. + Sócios gestores	Manter conta to com os profissionais da TI para informática e, se for preciso, restabelecer de forma emergencial as cópias de segurança no servidor de reserva para que os colaboradores possam ter acesso às informações, arquivos e sistemas.	Profissionais da TI	Imediato para estação de trabalho e 6 hs para servidor	24 hs
Perda de informações/arquivos/ sistemas, pane nos recursos de informática	Comunicar imediatamente os profissionais da TI	Coordenador adm. + Sócios gestores	Manter conta to com os profissionais da TI para restabelecimento do sistema de informática e, se for preciso, restabelecer de forma emergencial as cópias de segurança no servidor de reserva para que os colaboradores possam ter acesso às informações, arquivos e sistemas.	Profissionais da TI	Imediato para estação de trabalho e 6 hs para servidor	24 hs
Incêndio/Enchente	Comunicar responsável administrativo	Coordenador adm. + Sócios gestores	Desocupação imediata do prédio pela saída de emergência e manter conta to com engenheiro civil para restabelecimento do prédio, e, se for preciso, acionar o corretor de seguro para cobertura securitária, mormente quanto à despesas para locação de outro prédio para continuidade das atividades do escritório e para aquisição dos equipamentos danificados.	Engenheiro Civil + Corretor de seguro	4 hs	24 hs
Obstrução de acesso principal ao Escritório	Comunicar responsável administrativo	Coordenador adm. + Sócios gestores	Liberação da entrada alternativa (secundária) para acesso ao Escritório, e, se for necessário, acessar os arquivos remotamente de qualquer outro prédio, para continuidade das atividades da empresa.	Responsável adm.	Imediato	24 hs
Ausência de um ou mais funcionários por um período de tempo significativo	Comunicar responsável administrativo + Sócios	Coordenador adm. + Sócios gestores + Coordenador	Remanejar as agendas diárias estabelecendo um acordo de ajuda mútua até o restabelecimento da ausência, e, se for necessário, contratar colaboradores	Responsável administrativo + Sócios gestores	Imediato	24 hs
Acesso a informações sigilosas	Comunicar Sócios	Sócios gestores	Restabelecimento imediato do sistema de proteção a informações sigilosas.	Sócios gestores	Imediato	24 hs
Manutenção e Acondicionamento dos servidores	Comunicar responsável administrativo	Coordenador adm. + Sócios gestores	Acionar os profissionais da TI e do ar-condicionado para imediata manutenção e acondicionamento dos servidores, e, se for necessário, substituir o servidor principal	Profissionais da TI e do ar-condicionado	Imediato	24 hs



**ALVES FERNANDES**

ADVOGADOS

Interrupção do serviço de dados e voz	Comunicar responsável administrativo	Coordenador adm. + Sócios gestores	Disponibilização de telefones celulares quais sejam: (62) 98112-1101, 99298-5292, 99173-6980, 99138-1036, 99137-5671 e 99231-6420.	Profissionais da TI e da telefonia	Imediato	24 hs
---------------------------------------	--------------------------------------	---------------------------------------	--	------------------------------------	----------	-------

Recursos Tecnológicos de Reserva	
Estações de trabalho	2
Servidor	1
Impressora	1
Aparelhos celulares	2

**Observações gerais:** É obrigatória a disponibilização de lista de telefones celulares e residenciais dos colaboradores, para utilização em caso de necessidade de comunicação de situações de contingência, se necessário O PCN deve ser revisado anualmente e será feita pelos sócios gestores, coordenadores administrativo e jurídico.

Eventualmente na ocorrência das seguintes situações:

- a) Alteração em processos (otimização ou adaptação a alterações na legislação);
- b) Introdução de nova tecnologia.