INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
SÃO PAULO
Câmpus Guarulhos

**DIRETORIA ADJUNTA EDUCACIONAL**
**COORDENADORIA DO TÉCNICO EM INFORMÁTICA PARA INTERNET**

## Segurança da Informação

Essa Política de Segurança da Informação foi elaborada como material didático do componente curricular Segurança da Informação, onde o aluno desenvolverá as habilidades para implantar essa política na prática e obter a competência em configurar ambientes mais seguros.


**DR Advocacia S/A**

# Política de Segurança da Informação

Versão 1.0

Guarulhos
2018

# Carta de Apoio à política de segurança da informação

Somos Daniel Matos e Ricardo Caro e entendemos a importância das nossas informações e por isso buscamos uma equipe de tecnologia da informação que se elabora um documento com as normas e regras para uso dos ativos da informação da DR Advocacia S/A.

Num cenário repleto de problemas com relação a roubo de informação e os prejuízos que uma ameaça por meio de uma vulnerabilidade possa nos afetar entendemos e por isso apoiamos o documento da política de segurança da empresa e aprovamos todo o documento.

Esperamos que todos os colaboradores leiam o documento e sigam para que tenhamos mais segurança nas nossas informações.

**Daniel Matos**
Advogado

**Ricardo Caro**
Advogado

**Política de Segurança - DR Advocacia**

# 1. Apresentação

A Política de segurança da informação, na DR Advocacia foi construído conjuntamente com a diretoria, colaboradores e departamento de tecnologia da informação tem como principal função disciplinar o uso dos ativos que manipulam informação dos clientes da DR Advocacia. Todos os colaboradores, clientes, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes a ela.

Todo e qualquer usuário de recursos computadorizados da DR Advocacia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A violação desta política de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

## 1.1 A Organização

A DR Advocacia ou DRA é um escritório de advocacia idealizado por Daniel Matos e Ricardo Caro, sua atuação é no ramo do direito do consumidor com foco nas classes C, D e E que por muitas vezes não tem seus direitos são respeitados por conta da sua renda e da dificuldade de encontrar um advogado que os represente, está instalada num escritório na praça oito de dezembro, nº. 100, no bairro do Taboão, em Guarulhos os horários de atendimentos são de segunda a sexta das 8h às 12h e das 14h às 17h e aos sábados das 9h às 12h.

**Política de Segurança - DR Advocacia**

A DR Advocacia entende que as informações de seus clientes são importantes bem como a tecnologia da informação, por isso, buscamos criar um departamento de tecnologia da informação (DTI), reorganizaram o escritório de modo a torna-lo mais fluido e implantou um projeto de redes com a implantação de servidores e estações para gestão de toda a informação da empresa. Essa equipe trabalhou na criação, implantação e a administração de política de segurança informação.

Por fim, esse investimento trouxe a DR Advocacia S/A ampliou a proposta de valor da empresa, aumentou a agilidade, melhorou atendimento, diminuiu excesso de trabalho e uma melhor a qualidade de vida dos colaboradores.

### 1.2 Objetivo da política de segurança da informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização do negócio da DR advocacia S/A

#### 1.2.1 Diretrizes da política de segurança

- Assegurar a confidencialidade, integridade e disponibilidade das informações da DR Advocacia S/A, mediante utilização de mecanismos de segurança da informação;
- Garantir a proteção adequada das informações e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados.
- Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização.
- Assegurar que os colaboradores estejam cientes e conscientizados sobre com relação a proteção das Informações
- Garantir o cumprimento dessa Política e das Normas Segurança da Informação da Organização.

#### 1.2.2 Missão da empresa

Considerar a informação de seus clientes como sendo um bem maior para a organização, que não deixará de disponibilizar os recursos necessários para sua proteção buscando garantir a continuidade do negócio.

**Política de Segurança - DR Advocacia**

### 1.2.3 Missão do departamento de tecnologia da informação

Propor, coordenar, administrar e implantar está política de segurança da informação a fim de proteger as informações da organização.

### 1.3 Abrangência

Esta política abrange todos os colaboradores que possuam acesso à rede da DR advocacia S/A, a informações confidenciais, aos equipamentos computacionais ou ambientes controlados que necessitem de *login* ou cartão de acesso, para que lhe sejam disponibilizadas tais informações.

Terão acesso às informações confidenciais e ambientes controlados da DR Advocacia, dentro dos limites definidos, os advogados, secretárias e estagiários devem concordar com a política registrando o aceite por meio da assinatura do TERMO DE COMPROMISSO apresentado quando de sua admissão. Este termo determina a adesão do profissional a todas as políticas e normas internas, incluindo esta política.

O uso indevido dos recursos, em desacordo com a política poderá implicar em advertência, suspensão e demissão a critério da direção da empresa, sofrerá as sanções impostas neste documento.

### 1.4 Papéis e responsabilidades

| Papel | Perfil | Descrição |
|---|---|---|
| Advogados | | |
| Estagiários | | |
| Secretarias | | |
| Gestor de TI | | |
| Equipe de TI | | |
| Clientes | | |

## 2. Definições e conceitos

**Política de segurança da informação:** Segundo Tribunal de Contas da União (TCU) Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações. (BRASIL, 2012).

**Informação Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

**Informação Interna:** É toda informação que só pode ser acessada pelos colaboradores da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

**Informação Confidencial:** É toda informação que pode ser acessada por todos os usuários da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

**Informação Restrita:** É toda informação que pode ser acessada pelos advogados. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a organização.

**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 funcionários em trânsito.

**Mensagens Instantâneas**: 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 uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

## 3. Políticas

A apresentamos as políticas de segurança da informação pelo da DR Advocacia S/A que foram definidas em conjunto com a alta direção da empresa e a equipe de TI contratada para implantar a rede e a segurança no seu ambiente de trabalho. Essas políticas vão comprovar as garantias propostas pela empresa e também a garantia da continuidade no negócio.

### 3.1 Política de Classificação da Informação

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

Os colaboradores devem ser orientados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

### 3.2 Política de diretores e colaboradores.

**Dos diretores**

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

**Dos colaboradores**

A DR Advocacia se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores além daqueles relevantes na condução do seu negócio.

Todos os dados pessoais de colaboradores são considerados confidenciais.

Os dados pessoais de colaboradores sob a responsabilidade da DR Advocacia não serão usados para fins diferentes daqueles para os quais foram coletados.

**Política de Segurança - DR Advocacia**

Os dados pessoais de colaboradores não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos colaboradores da DR Advocacia S/A.

### 3.2.1 Gestão de pessoas

O recrutamento de pessoas deverá informar à DTI toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de colaboradores.

O departamento de TI é quem oferece o acesso por meio de usuário e senha para acessar a rede e os serviços da DR advocacia.

Nenhum colaborador, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

**Da Contratação**

Cabe solicitante da contratação a comunicação ao DTI sobre as rotinas a que o novo contratado terá direito de acesso.

No caso de temporários e/ou estagiários o recrutamento de pessoas deve informar o tempo em que prestará serviço à DRA e a data de seu desligamento.

O setor de recrutamento dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da DR Advocacia S/A.

**Da demissão**

No caso de demissão, o setor de Recursos Humanos deverá comunicar antes da ocorrência ao DTI, para que o colaborador demitido tenha os acessos bloqueados e logo depois excluídos do sistema.

**Da transferência ou promoção**

Quando um colaborador for promovido ou transferido de seção ou gerência, o setor de recursos humanos deverá comunicar o fato ao DTI para que sejam feitas as adequações nas permissões de o acesso do referido colaborador.

## Política de Segurança - DR Advocacia

**Das informações da empresa**

É de propriedade da DR Advocacia, todos os dados, planilhas ou documentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício.

**Dos dados**

Os colaboradores deverão assinar no ato da contratação, um documento de confidencialidade da informação.

### 3.3 Política dos ativos da informação

O DTI é responsável pela aplicação da Política de Segurança da Informação da DR Advocacia S/A em relação a definição de compra e substituição de "software" e "hardware".

**Dos softwares**

- Qualquer necessidade de novos programas ("softwares") deverá ser discutida com o responsável pela DTI.
- O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva da DTI assim como a manutenção, alteração e atualização de equipamentos e programas.
- Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

**Dos Computadores**

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da A EMPRESA, devem estar cientes de que:

- Qualquer necessidade de novos equipamentos de informática (hardware) deverá ser discutida com o responsável da DTI.
- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto:

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

### 3.4 Política de controle de acesso

Conforme consta na norma NBR 27002 todo acesso aos servidores e computadores da empresa deve seguir uma política de acesso definida baseado os itens a seguir

#### 3.4.1 Política de usuários

**Do usuário administrador**

- Os usuários administradores não devem ser usados diretamente nos servidores;
- Os usuários administradores se possível devem ser bloqueados ou desativados nos servidores;
- Convém não utilizar o usuário administrador nas estações da rede;
- Convém que o administrador da rede possua seu usuário com as permissões necessárias para administração total da rede.

- Convém a criação de um usuário com as permissões necessárias para manipulação nas estações

### 3.4.2 Política de senhas

**Do usuário administrador**

- Os usuários dos administradores devem ser configurados com uma senha complexa ou uma frase secreta de no mínimo 14 caracteres respeitando as boas práticas de senhas.
- Os usuários administradores das estações receberam uma senha complexa para acesso das configurações locais de cada estação
- Da senha dos usuários de administração
- Convém que a senha tenha requisitos de complexidade;
- Convém que não tenha permissão de alteração;
- Convém que não deve expirar;
- Convém que seja armazenada em local seguro.
- Da senha dos usuários comuns
- Convém que a senha tenha requisitos de complexidade;
- Convém que os usuários alterem a senha no primeiro acesso;
- Convém que a senha expire em 90 dias;
- Convém que as senhas não remetam as características ou a dados pessoais;

**Do cartão de senhas**

- O cartão de senhas é um documento formal que faz parte da política de segurança da informação da DR advocacia S/A, nesse cartão o administrador de sistemas deve elaborar uma forma de colocar aqui as senhas de modo que somente o Administrador ou Gestor de TI possa reconhecer se precisar recuperar senhas importantes para infraestrutura de rede que está administrando.
- Nesse documento serão colocadas as senhas cruciais como as de administração de servidores e equipamentos de rede.

- Para nosso cenário a política do cartão de senhas será incluir todas as senhas ou formar de identificar a senha dos principais usuários do cenário, quando o documento estiver pronto será produzido uma cópia do documento onde um ficara com gerente de TI da empresa (aqui representado pelo representante de cada grupo) e o dono da empresa (aqui representado pelo professor).

**Recuperação de Senhas**

- Em caso do colaborador esqueça a senha, o departamento de TI deve ser acionado por telefone, pode ser solicitado pessoalmente se a equipe estiver na empresa realizando alguma tarefa de administração.
- Departamento de TI pode verificar se a pessoa é realmente ela mesma por meio alguns questionamentos sobre o seu local de trabalho.
- A senha deve ser reiniciada e os procedimentos para alteração serão os mesmos do primeiro acesso.

### 3.5 Política de acesso à internet

O acesso à Internet na DR Advocacia S/A é autorizado para os usuários pois as atividades profissionais necessitam do acesso à rede mundial. Páginas da Internet que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

- O uso da internet será monitorado pelo departamento de tecnologia da informação (DTI) por meio de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.
- É atribuição da Direção da DR Advocacia S/A a definição do que os colaboradores poderão ter permissão para uso (navegação) da internet.
- Não é permitido instalar programas provenientes da Internet nos microcomputadores da DR Advocacia S/A, sem expressa anuência do DTI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

**Política de Segurança - DR Advocacia**

- Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.
- Ao navegar na internet pelos colaboradores da empresa, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a páginas:
- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da DR Advocacia S/A;
- Que promovam discussão pública sobre os negócios da DR Advocacia S/A, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível "Confidencial".
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.
- Não poderão efetuar upload (subida) de qualquer software que não seja licenciado à DR Advogados,
- Não poderão utilizar os recursos da DR Advocacia S/A para propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.
- O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados a pedido da diretoria da DR Advocacia.

- Não é permitido acesso a sites de proxy.

### 3.6 Política de Backup

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da Informática e deverão ser feitas diariamente.

**Do backup**

- Semanalmente deve ser realizado uma cópia completa de todos os dados dos diretórios da empresa
- Semanalmente deve ser realizado cópia (*dump*) da base de dados do sistema para internet da empresa DR Advocacia.
- Os backups devem ser armazenados em disco óptico (CD, DVD ou Blu-Ray) não regravável.
- Ao final de cada processo arquivado ou encerrado no diretório onde ficam os processos do cliente deve-se gravar três cópias uma em cada mídia armazenar numa caixa de plástica e colocado uma etiqueta com as informações do cliente. Uma deve ficar na empresa e as outras duas entregues a cada um dos advogados para que guardem em outro local.

**Dos dados dos usuários:**

- É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos colaboradores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da DR Advocacia.
- No caso das informações consideradas de fundamental importância para a continuidade dos negócios da A EMPRESA o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

### 3.7 Política contra software malicioso

**Política de Segurança - DR Advocacia**

- Todo arquivo em mídia proveniente de entidade externa a DR Advocacia deve ser verificada por programa antivírus pelo DTI
- Todo arquivo recebido / obtido por meio da internet deve ser verificado por programa antivírus.
- Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela DTI.
- O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

## 4. Das sanções

- 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.
- O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

# Referências

ASSOCIAÇÃO BRASILEIRAS DE NORMAS TÉCNICAS (ABNT) NBR 27001 – **Tecnologia da Informação: Técnicas de segurança: Sistemas de gestão da segurança da informação** ABNT: Rio de Janeiro 2013.

ASSOCIAÇÃO BRASILEIRAS DE NORMAS TÉCNICAS (ABNT) NBR 27002 – **Tecnologia da Informação: Técnicas de segurança: Código de prática para controles de segurança da informação**. 2ª Edição ABNT: Rio de Janeiro 2013.

BRASIL Decreto-Lei nº 9609 de 19 de fevereiro de 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9609.htm> acessado em 24 de março de 2019.

BRASIL Decreto-Lei nº 9610 de 19 de fevereiro de 1998. **Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências**. Disponível em: < http://www.planalto.gov.br/Ccivil_03/leis/L9610.htm> acessado em 24 de março de 2019

BRASIL Decreto-Lei nº 12.965 de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> acessado em: 24 de março de 2019.

BRASIL Decreto-Lei nº 13.709 de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art60> acessado em: 24 de março de 2019

BRASIL. Tribunal de Contas da União (TCU). **Boas Práticas em Segurança da Informação.** BRASIL: Brasília. 2012. Disponível em: < http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf> acessado em 24 de março de 2019

RAIZEN. **Política de Segurança da Informação.** 2018. Disponível em <https://www.raizen.com.br/sites/default/files/fornecedores_seguranca_da_informacao.pdf> acessado em 24 de março de 2019

Serviço Nacional de Aprendizagem do Comércio (SENAC). **PSI – Política de Segurança da Informação: Documento de diretrizes e normas administrativas.** Versão 1.0 SENAC: São Paulo. 2013. Disponível em: <http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf> acessado em: 24 de março de 2019.

SANTANDER **Política de segurança da informação para correspondente bancário do SANTANDER**. 2013. Disponível em: <https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf> acessado em: 24 de março de 2019.