



Política de Segurança da Informação

Código:	PO SGSI 03
Versão:	1.2
Data da versão:	18/08/25
Criado por:	Henrique Haveroth
Aprovado por:	Joani Maria de Assis Asckar
Nível de confidencialidade:	Pública



Sumário

1. SEGURANÇA DA INFORMAÇÃO	2
2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	2
2.1. Proteção da Informação	2
2.2. Responsabilidades	3
2.3. Informações Confidenciais	3
2.4. Violação da Política, Normas e Procedimentos de Segurança da Informação	4
3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	5
3.1. Classificação da Informação	5
3.2. Acesso a Sistemas e Recursos de Rede	6
3.3. Utilização dos Recursos de Informação	6
3.4. Autenticação e Senha	6
3.5. Direito de Acesso (Autorização)	7
3.6. Direitos de Propriedade	7
3.7. Equipamentos particulares/privados	7
3.8. Mesa Limpa – Organização do Ambiente de Trabalho	7
3.9. Conversas em Locais Públicos e Registro de Informações	8
3.10. Leis e Regulamentos	8
4. SEGURANÇA EM REDES E SISTEMAS	9
4.1. Proteção da Infraestrutura de Rede e Sistemas	9
5. TREINAMENTO E CONSCIENTIZAÇÃO	10
5.1. Objetivo	10

Controle de Versões					
Versão	Causa da Mudança	Elaborado por	Data	Vistoriado por	Data
01	Versão Original	Aloisio	26/11/2018	Henrique Haveroth	27/11/2018
02	LGPD	Henrique Haveroth	10/08/2021	Joani Maria de Assis Asckar	
03	LGPD	Joaquimn Albuquerque	18/08/2025	Henrique Haveroth	



1. SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de Informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas. Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao Cartório e prejudicar o crescimento e vantagens competitivas.

Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação do **Serviço Notarial e Registro de Imóveis – 6º Ofício de Cuiabá – Mato Grosso**.

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando o Cartório do 6º Ofício de Cuiabá a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

- **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.
- **Autenticidade:** Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1. Proteção da Informação

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos do Cartório, a informação deve ser adequadamente manuseada e protegida. A informação pode estar presente em diversas formas, tais como:

- Sistemas de informação,
- Diretórios de rede,
- Bancos de dados,
- Mídia impressa, magnética ou ótica,
- Dispositivos eletrônicos,
- Equipamentos portáteis,
- Microfilmes,
- E...até mesmo por meio da comunicação oral.

Toda informação relacionada às operações do Cartório do 6º Ofício de Cuiabá,



gerada ou desenvolvida nas dependências do mesmo ou de algum colaborador, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios do Cartório.

É diretriz que toda informação de propriedade do Cartório do 6º Ofício de Cuiabá seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

2.2. Responsabilidades

É missão e responsabilidade de cada colaborador, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente *Política de Segurança da Informação*. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pelo Colaborador, por meio de seus funcionários e estagiários, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à Segurança da Informação.

Para auxiliar a todos os usuários nessa missão, o Cartório do 6º Ofício de Cuiabá criou a área de Segurança da Informação, que administra as disciplinas de conhecimento que dão suporte a essa ciência. A área de Tecnologia da Informação (T.I.) do Cartório é responsável por editar as políticas e padrões que apoiam a proteção dos ativos de informação e estar preparada para auxiliar na resolução de problemas relacionados ao tema.

2.3. Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais de apoio, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em quaisquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pelo Cartório do 6º Ofício de Cuiabá e/ou obtidas pelos Colaboradores em decorrência da execução do contrato de prestação de serviços. São responsáveis pela observância desta Política os:

- Tabeliões,
- Escreventes,
- Colaboradores em geral (analistas, auxiliares, menor aprendiz, estagiários,...),
- Consultores (incluindo advogados, auditores e consultores de T.I.).

Os Colaboradores e Consultores que receber as informações confidenciais deverão mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar

quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais poderão ser repassadas para terceiros sem consentimento por escrito do Cartório do 6º Ofício de Cuiabá. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pelo Cartório do 6º Ofício de Cuiabá.

As informações confidenciais somente poderão ser utilizadas para fins de execução de atividades, conforme acordadas com o Cartório.

O Colaborador e/ou Consultor deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.

O Colaborador e/ou Consultor deverá informar prontamente ao Cartório do 6º Ofício de Cuiabá sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política:

- O atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, Tribunais e de Órgãos Públicos Administrativos;
- A divulgação das informações confidenciais aos agentes e representantes (incluindo, mas não se limitando, a advogados, procuradores, auditores e consultores);
- Informações confidenciais que forem divulgadas somente após o consentimento, por escrito, do Cartório do 6º Ofício de Cuiabá.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o Colaborador e/ou Consultor de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

2.4. Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de Segurança da Informação e/ou ao seu Responsável Imediato. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política possuem total



aderência da administração do Cartório do 6º Ofício de Cuiabá e devem ser observados por todos na execução de suas funções.

A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os Colaboradores e/ou Consultores às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Caso tenha algumas dúvidas quanto aos princípios e responsabilidades descritas nesta norma, deve-se entrar em contato com o Responsável pela Tecnologia da Informação e/ou com o seu superior imediato.

3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1. Classificação da Informação

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário.

Cabem aos Colaboradores todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem do Cartório do 6º Ofício de Cuiabá, podendo levar à extinção das operações ou prejuízos graves ao crescimento. São exemplos de informações confidenciais:

Informações de clientes que devem ser protegidas por obrigatoriedade legal,

incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;

- Informações sobre produtos e serviços que revelem vantagens competitivas do Cartório do 6º Ofício de Cuiabá frente ao mercado;
- Todo o material estratégico do Cartório do 6º Ofício de Cuiabá (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações do Cartório do 6º Ofício de Cuiabá, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

3.2. Acesso a Sistemas e Recursos de Rede

Os funcionários são totalmente responsáveis pela correta posse e utilização de suas senhas, assim como pelas ações decorrentes da utilização destes poderes.

As autorizações de acesso a sistemas e definições de perfis serão definidas pelo responsável imediato dos funcionários, podendo ter o auxílio e/ou suporte do Setor de Tecnologia da Informação.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções.

Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Periodicamente, os acessos concedidos devem ser revistos pelo Responsável Imediato.

3.3. Utilização dos Recursos de Informação

Apenas os equipamentos e software disponibilizados e/ou homologados pelo Cartório do 6º Ofício de Cuiabá podem ser instalados e conectados à rede do Cartório do 6º Ofício de Cuiabá.

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. *Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.*

3.4. Autenticação e Senha

O Funcionário é responsável por todos os atos executados com seu identificador (login – usuário/senha), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os Funcionários devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum.
 - Ou seja, não contá-la a ninguém e não anotá-la em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

3.5. Direito de Acesso (Autorização)

O Funcionário com cargo superior é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que são atribuídos aos seus funcionários, estagiários, prestadores de serviços, parceiros e visitantes, sendo intransferíveis. A solicitação de acesso à informação deve decorrer da necessidade funcional do Colaborador.

3.6. Direitos de Propriedade

Todo produto resultante do trabalho dos Colaboradores e/ou Consultores (coleta de dados, documentos, sistema, metodologia, dentre outros) é propriedade do Cartório do 6º Ofício de Cuiabá.

Em caso de extinção ou rescisão do contrato de prestação de serviços, por quaisquer motivos, deverá o Colaborador e/ou Consultor devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços ao Cartório do 6º Ofício de Cuiabá, ou emitir declaração de que as destruiu.

3.7. Equipamentos particulares/privados

Equipamentos particulares/privados, tais como computadores ou quaisquer dispositivos portáteis que possam armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, e serão conectados às redes da Organização somente com a anuência do Setor de Tecnologia da Informação.

Os proprietários dos equipamentos particulares/privados terão que garantir que os mesmos possuem antivírus e que estão “vacinados” e livres de quaisquer tipos de ameaças.

3.8. Mesa Limpa – Organização do Ambiente de Trabalho

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos - eletrônicos ou não.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Os dados considerados confidenciais e/ou sigilosos contidos nos documentos impressos, deverão ser picotados e somente após essa ação que devem ser descartados.

3.9. Conversas em Locais Públicos e Registro de Informações

Não discutir ou comentar assuntos confidenciais em:

- Locais públicos;
- Redes sociais e Mensagens de textos



- Exceto quando encaminhadas ao Cartório do 6º Ofício de Cuiabá e com a anuência dos superiores.

3.10. Leis e Regulamentos

É de responsabilidade dos Funcionários, Colaboradores e Consultores conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

Esta Política orienta o comportamento de todos os usuários do Cartório e deve ser considerada em todas as atividades desempenhadas na Companhia.

O descumprimento dos preceitos contidos nesta Política acarretará a purgação de responsabilidades para aplicação de medidas disciplinares.

Impressos, deverão ser picotados e somente após essa ação que devem ser descartados.

4. SEGURANÇA EM REDES E SISTEMAS

4.1 Proteção da Infraestrutura de Rede e Sistemas

Garantir que os recursos de rede e sistemas sejam protegidos contra acessos não autorizados, uso indevido, falhas e ataques.

Utilizamos diversas ferramentas para manter a segurança em nossas redes segue abaixo alguma delas:

- Firewall é um sistema de segurança que atua como uma barreira entre uma rede confiável (sua rede local) e uma rede não confiável (a Internet), com ele podemos monitorar e controlar o tráfego de dados com base em regras de segurança predefinidas.
- IDS/IPS o IDS é um sistema de detecção de intrusões, ele consegue monitorizar o tráfego de rede ou atividades do sistema e detecta comportamento suspeitos ou maliciosos gerando alertas para os administradores. Já o IPS é um sistema de prevenção de intrusões ele faz o que o IDS faz mas ele pode bloquear ou prevenir automaticamente atividades maliciosas.
- VPN trata-se de uma tecnologia que cria uma conexão segura e criptografada entre seu dispositivo e a internet. Ela permite que você navegue com mais privacidade ou acesse redes privadas em grande distância.
- Antivírus é um software de segurança projetado para detectar, bloquear e remover malwares como vírus worms, trojans, spyware, ransomware entre outros. O antivírus pode ser usado em computadores celulares e servidores.



5. Treinamento e Conscientização

5.1 Objetivo

Com o objetivo de capacitar os colaboradores para identificar, evitar e responder a riscos relacionados à segurança da informações, reduzindo erros humanos que não maioria dos grandes ataques teve seu início com uma falha humana.

O programa de treinamento e consciencialização em segurança da informação visa fortalecer a cultura de segurança e lidar com ameaças reais.