Sumário

Revisão nº	Item	Natureza da Alteração	Data	Autorizado Por
1	Todos	Alteração de Layout e e-mails de dados, e adição do campo definições, englobando mais itens.	01/07/2025	Denis Almeida

Elaboração: Denis Almeida, Gustavo Malachias Silva

Responsável: Victor Augusto D'Alessandro Barros

Revisão: Alessandro Henrique Monteiro e Silva

Aprovação: Eloísa Afonso Rios

1.0 Objetivo

1.1 Estabelecer diretrizes para estruturar uma Política de Segurança da Informação, visando garantir a proteção e confidencialidade aos dados e recursos de informação do cartório, seus colaboradores, clientes, parceiros, fornecedores e demais agentes envolvidos direta ou indiretamente.

2.0 Definições

2.1 **DPO**: "Data Protection Officer", ou, Encarregado de Proteção de Dados. É um profissional designado por uma organização para garantir que a empresa cumpra as leis e regulamentos de proteção de dados pessoais, como a LGPD.

2.2 **LGPD**: “Lei Geral de Proteção de Dados”, lei brasileira que estabelece regras para o tratamento de dados pessoais, tanto online quanto offline, por empresas e órgãos públicos, visando proteger a privacidade e os direitos fundamentais dos cidadãos.

2.3 **Agentes de Segurança da Informação**: administradores, colaboradores, fornecedores, e quaisquer outros envolvidos direta ou indiretamente em processos internos do cartório.

2.4 **Informação**: é todo o conjunto de dados e elementos gerados ou desenvolvidos pelo e para o cartório de propriedade ou não deste, podendo estar presentes em sistemas de informação, arquivos digitais, equipamentos, conversas, diretórios de rede, bancos de dados internos ou externos, mídia impressa, magnética ou ótica, dispositivos eletrônicos móveis, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral que, independentemente da forma apresentada, compartilhada ou armazenada, devem ser adequadamente manuseadas e protegidas, e utilizadas apenas para a sua finalidade originária.

2.5 **Informação Confidencial**: Informação não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbal ou de outra forma emitidas, reveladas e obtidas pelo cartório.

2.6 **Segurança da Informação**: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger as informações do cartório. Segurança Cibernética: Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado.

2.7 **Canal de Ética**: Canal de comunicação do cartório para recebimento de denúncias relacionadas ao não atendimento desta Política.

2.8 **Cartório**: 1º Ofício de Registro de Imóveis, Títulos e Documentos e Civil das pessoas Jurídicas de Itapecerica-MG.

3.0 Abrangência

3.1 A presente Política aplica-se a todos os Agentes de Segurança da Informação, conforme definidos na seção 4.5 abaixo.

3.2 É missão e responsabilidade de cada Agente de Segurança da Informação, observar e seguir as políticas, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação, sendo imprescindível que cada Agente de Segurança da Informação tenha conhecimento dessa política e compreenda o papel da Segurança da Informação em suas atividades diárias e a importância desta para o cartório.

3.3 Essa política é aplicável tanto ao ambiente informatizado quanto aos meios convencionais de processamento, comunicação e armazenamento da informação. Abrange todos os equipamentos e recursos possuídos ou utilizados pelo cartório.

3.4 Os colaboradores e terceiros que tenham acesso aos recursos do cartório somente os utilizarão seguindo os princípios de segurança aqui estipulados e sem afetar ou causar prejuízo a outrem.

3.5 Quaisquer dos Agentes de Segurança da Informação que observarem desvios às diretrizes desta Política de Segurança da Informação ou ao Código de Conduta do cartório deverão comunicar tais fatos no email: lgpd@1ritdpjitapecerica.com.br

4.0 Diretrizes da Segurança da Informação

4.1 Informações, como definida no item 4.4, precisam ser preservadas observando três princípios básicos de Segurança da Informação:

4.1.1 Integridade — a Informação deve ter seu conteúdo original mantido, sendo protegida contra alterações indevidas, seja de forma intencional ou acidental;

4.1.2 Confidencialidade — somente pessoas devidamente autorizadas podem ter acesso às informações;

4.1.3 Disponibilidade — o acesso à Informação deve ser garantido às pessoas autorizadas sempre que for necessário.

4.2 É de propriedade exclusiva do cartório toda informação, ideias e métodos gerados utilizando-se integralmente ou parcialmente seus recursos.

4.3 O cartório, como custodiante de dados e informações, os considera sigilosos, logo serão tratados assim pelos seus colaboradores e todos que tenham acesso a estes.

4.4 As Informações, independentemente da forma apresentada, compartilhada ou armazenada, são de responsabilidade de quem as gerou, recebeu ou armazenou e, devem ser utilizadas apenas para sua finalidade original, estando sujeitos a monitoramento e auditoria.

4.5 É proibida a modificação, divulgação e destruição não autorizadas das Informações, quer oriundas de erros, ou mesmo fraudes, vandalismo, espionagem ou sabotagem.

4.6 Igualmente, as Informações Confidenciais, como definida na seção 5 abaixo, deverão ser mantidas em caráter sigiloso, com acesso restrito, sendo controladas suas cópias, dados e reproduções, não podendo ser repassadas para terceiros sem consentimento.

4.7 É também objetivo desta Política, a Segurança Cibernética que visa prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente virtual.

4.8 O cartório adotará ferramentas, procedimentos e controles para reduzir sua vulnerabilidade a incidentes e atender aos objetivos de Segurança Cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

4.9 Equipamentos particulares/privados como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes do cartório, ressalvadas as hipóteses devidamente autorizadas pelo gestor da área, que, em caso necessário, entrará em contato com o setor de Tecnologia.

4.10 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.

4.11 Os Agentes de Segurança da Informação não devem discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto.

4.12 Com relação aos prestadores de serviços e terceiros que tenham acesso às instalações, informações e dados do cartório, os instrumentos legais que regulamentam a relação entre as partes devem conter cláusulas que contemplem a responsabilidade destes no cumprimento desta Política de Segurança da Informação, suas normas e procedimentos.

5.0 Processo de Segurança da Informação

5.1 Fica a cargo da administração:

5.1.1 Dar anuência ao Plano de Segurança da Informação, proposto pela Administração do cartório quanto à Informação e os testes periódicos de análise de vulnerabilidade, realizados pelo cartório ou por empresas externas.

5.1.2 Aprovar os investimentos necessários a serem aplicados para a garantia dos níveis adequados da Segurança da Informação.

5.1.3 Gerenciar, conjuntamente, os riscos às informações consideradas críticas e importantes para o negócio da empresa e que tenham que ser acompanhados no nível máximo da empresa.

5.1.4 Aprovar proposta de procedimentos e controles em níveis de complexidade, abrangência e precisão voltados à prevenção e ao tratamento dos incidentes a serem adotados pelo cartório e por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do cartório.

5.2 Fica a cargo da administração e setor de tecnologia da informação:

5.2.1 Gerenciar a Segurança de Tecnologia da Informação no mais alto nível organizacional da empresa, de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio do cartório.

5.2.2 Elaborar e revisar anualmente um procedimento operacional de Segurança da Informação contendo: objetivo, escopo, definição de funções e responsabilidades, investimentos necessários e riscos envolvidos.

5.2.3 Assegurar atendimento em tempo integral, eficiente e autônomo para atender e orientar nos casos de incidentes que possam colocar em risco a Segurança da Informação do Cartório, bem como de seu patrimônio.

5.2.4 Assegurar que os Agentes de Segurança da Informação estejam cientes das ameaças e das preocupações que possam intervir na segurança e que sejam orientados para apoiar esta Política.

5.2.5 Alertar aos Agentes de Segurança da Informação que qualquer Informação ou sistema de Informação é passível de monitoramento, desde que, seja feito através de um processo formal e sistemático.

5.2.6 Definir os parâmetros a serem utilizados na avaliação de relevância dos incidentes, registrar a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes.

5.2.7 Estabelecer procedimentos e controles em níveis de complexidade, abrangência e precisão voltados à prevenção e ao tratamento dos incidentes a serem adotados pela Serventia e por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Serventia.

5.2.8 Informar como a confidencialidade e integridade serão mantidas, e como a disponibilidade dos serviços será assegurada em caso de incidente ou desastre;

5.2.9 Manter a segurança quanto aos aspectos dessa norma, quanto a responsabilidade pelo processo, auditando-os periodicamente, buscando a certificação do cumprimento dos requisitos de segurança.

5.2.10 Assegurar que os recursos de tecnologia colocados à disposição dos Agentes de Segurança da Informação sejam utilizados apenas para as finalidades aprovadas pelo Cartório.

5.2.11 Analisar periodicamente os ativos da Informação, de forma que estejam devidamente inventariados, protegidos, tenham um responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

5.2.12 Garantir que a aquisição de novos produtos, a seleção de mecanismos de segurança e a aquisição de bens e/ou serviços de tecnologia que levem em consideração o balanceamento de risco, tecnologia, custo, qualidade, velocidade e impacto nas atividades.

5.2.13 Assegurar que se evite quaisquer ações ou situações que possam expor o cartório a riscos de perda financeira, material ou humana, direta ou indiretamente, potenciais ou reais, comprometendo suas atividades.

5.2.14 Assegurar que medidas preventivas sejam tomadas para diminuir risco de ocorrência de fraudes internas ou externas, mantendo um forte processo de avaliação de riscos de Segurança da Informação e implementação de respectivos requisitos, utilizando-se de tecnologia de ponta e de um serviço de inteligência apropriado, bem como, uma equipe competente e preparada para dar tratamento a casos deste tipo, com agilidade e eficiência.

5.2.15 Adotar mecanismos para disseminação da cultura de segurança cibernética (programas de capacitação/rotinas de Informação a usuários finais/novos usuários sobre esta Política/precauções na utilização de ferramentas eletrônicas/ comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética), bem como, para verificação do cumprimento desta Política.

5.2.16 Garantir a observância, pelos terceiros contratados, desta Política e dos requisitos legais e regulamentos internos; Adotar providências de forma a reduzir as possibilidades de erro humano, falhas de equipamentos e dispositivos, ou qualquer outro tipo de incidente que possa causar a perda da integridade das informações.

5.2.17 Controlar os acessos aos ambientes tecnológicos e de informação através de um processo formal, físico e lógico ao ambiente ou serviços disponíveis em servidores, devendo as autorizações de acesso ser revistas, auditadas, confirmadas e continuadamente registradas.

5.2.18 Monitorar o tráfego efetuado em ambientes, recursos de Tecnologia de Informação e acordos de níveis de serviço rastreando eventos críticos e evidenciando possíveis ocorrências, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em casos de incidentes.

5.2.19 Prever no orçamento anual do Planejamento Estratégico, os recursos necessários para atendimento a esta Política, bem como, manter os níveis adequados em Segurança da Informação.

5.3 Fica a cargo dos colaboradores:

5.3.1 Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.

5.3.2 Cumprir as determinações desta Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

5.3.3 Utilizar recursos e sistemas de informações somente para os fins profissionais.

5.3.4 Responder, por todo e qualquer acesso, aos recursos bem como pelos efeitos desses acessos efetivados através de suas credenciais, ou outro atributo para esse fim utilizado.

5.4 Fica a cargo dos gestores:

5.4.1 Gerenciar o cumprimento desta Política, por parte de seus supervisionados. Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

5.4.2 Zelar, em nível físico e lógico, pelos ativos de informação e de processamento do cartório, relacionados com sua área de atuação.

5.4.3 Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações.

5.4.4 Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI (Tecnologia da Informação), que acessos e permissões devem ter os colaboradores, sob sua supervisão, as informações e sistemas.

5.4.5 Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI (Tecnologia da Informação), quais os colaboradores demitidos ou transferidos, para exclusão de permissões no cadastro dos usuários.

6.0 Disposições gerais

6.1 No que se refere a Informações, confidenciais ou não, em custódia ou não, é proibido tudo aquilo que não esteja previamente autorizado por esta política e demais documentos normativos.

6.2 É competência da Administração, alterar esta Política sempre que se fizer necessário.

7.0 Anexos

7.1 MAN-RCH-001-Manual-de-Conduta – Manual de Conduta;

7.2 POL-GER-002-Senhas – Política de Senhas;

7.3 POL-GER-003-Uso-do-email-corporativo - Política de uso do e-mail corporativo;

7.4 POL-GER-004-Acesso_Internet - Política de acesso à Internet;

7.5 POL-GER-005-Uso-estacao-trabalho - Política de uso da estação de trabalho;

7.6 POL-GER-006-Controle-Acesso – Política de Controle de Acessos;

7.7 POL-GER-007-Backup - Política de Backup.