cartório QUINZE

15° OFÍCIO DE NOTAS TABELIÃ FERNANDA DE FREITAS LEITÃO

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Código	POL-SIP
Versão vigente	2.0
Data da versão vigente	06/09/2024
Tipo de documento	Política
Autores/Revisores	Alex Pereira Paulo Camargo Rodrigo Lopes
Aprovador(es)	Fernanda Leitão
Classificação	Interna

Sumário

1. Introdução

Fundado em 1918, o **15º OFÍCIO DE NOTAS DA CAPITAL DO ESTADO DO RIO DE JANEIRO** (“CARTÓRIO 15”),sob a delegação da Tabeliã Titular Fernanda de Freitas Leitão desde 1998, tem como missão a prestação de Serviços Notariais com a máxima excelência, abrangendo entre suas atividades a elaboração de diversos documentos, tais como escrituras, procurações, atas notariais, testamentos, além da abertura e reconhecimento de firmas e autenticação de documentos. O CARTÓRIO 15 compreende ser de suma importância proteger as estratégias, metodologias, processos internos, ferramentas tecnológicas e conhecimentos específicos, bem como os dados pessoais de todos os clientes, colaboradores, parceiros, fornecedores e demais partes interessadas.

Assim, considera que a informação acumulada ao longo de mais de um século de funcionamento seja um ativo estratégico de inestimável valor, e sua correta gestão, assegurando que esteja sempre disponível para as pessoas certas e no momento adequado, é fundamental para a reputação do CARTÓRIO 15, para o seu crescimento e para a manutenção de sua boa percepção pelo mercado.

Desta forma, o CARTÓRIO 15 estabelece esta Política de Segurança da Informação e Privacidade (“Política”) para direcionar seu Sistema de Gestão de Segurança da Informação (SGSI), alinhado às melhores práticas de mercado e às normas internacionalmente aceitas, com o objetivo de determinar e manter níveis adequados de segurança capazes de assegurar a confidencialidade, integridade e disponibilidade de suas informações e daquelas tratadas sob sua responsabilidade.

2. Termos e Definições

Consulte o documento **Termos e Definições de Segurança da Informação e Privacidade.**

3. Objetivos

3.1. Esta Política estabelece as diretrizes e responsabilidades para o planejamento, implementação, operação, monitoramento e melhoria contínua do SGSI do CARTÓRIO 15, e define objetivos estratégicos de segurança da informação e privacidade alinhados aos objetivos de negócio, propósito, cultura e estratégia de mercado.

3.2. O CARTÓRIO 15 deve, através do SGSI, implementar controles aptos a assegurar a confidencialidade, integridade e disponibilidade de informações e ativos associados pertencentes ou tratados sob sua responsabilidade.

3.3. Estes controles devem ser planejados e implementados com base em um processo de gestão de riscos em segurança da informação e privacidade, através do qual decisões informadas sobre eliminar, transferir, mitigar ou aceitar riscos identificados, analisados e avaliados devem ser tomadas.

3.4. O SGSI do CARTÓRIO 15 deve ser mantido, monitorado e melhorado continuamente, no contexto de seu propósito, estratégia de mercado, obrigações legais, regulatórias e contratuais.

3.5. O SGSI do CARTÓRIO 15 deve contar com recursos humanos e financeiros adequados para sua implementação, operação, monitoramento e melhoria contínua.

3.6. O SGSI deve estar integrado por padrão *(by default)* e no desenho *(by design)* de todos os processos, sistemas, ferramentas tecnológicas, documentos e relações do CARTÓRIO 15. Segurança da informação e privacidade deve ser responsabilidade coletiva de todos os colaboradores, e questões pertinentes devem ser tratadas como prioridade.

4. Aplicação

4.1. Esta política deve ser aplicada a todo o corpo funcional do CARTÓRIO 15 - Tabeliã, Oficiais, funcionários e demais colaboradores que tenham vínculos empregatícios diretos ou indiretos, isso inclui pessoas que trabalhem em período integral, meio período ou em regime temporário, seja em atuação presencial ou remota. Todos são referidos nesta Política simplesmente como “colaboradores”.

4.2. A Política se aplica ao tratamento de informações pertencentes ou sob a responsabilidade do Cartório, abrangendo comunicações verbais, uso de qualquer plataforma tecnológica ou mídia física.

4.3. Diretrizes de segurança da informação e privacidade estabelecidas por esta Política devem ser aplicadas a instalações físicas, sistemas, *softwares*, ferramentas tecnológicas e recursos de tecnologia da informação e comunicação (TIC) contratados ou pertencentes ao CARTÓRIO 15.

5. Responsabilidades

5.1. O CARTÓRIO 15 deve assegurar que conte com pessoas com competência comprovada para planejar, implementar, gerenciar, medir e melhorar continuamente seu SGSI e todos os controles definidos para aplicação.

5.2. Todos os colaboradores o CARTÓRIO 15 devem:

a. considerar segurança da informação e privacidade como sua responsabilidade em conjunto com todos no Cartório;
b. conhecer integralmente e compreender o conteúdo, regras de diretrizes desta Política e outros documentos de segurança da informação e privacidade relevantes para sua função, atividades de trabalho e ativos aos quais possuem acesso;
c. conhecer e cumprir legislações que regulamentam aspectos como privacidade e proteção de dados pessoais e propriedade intelectual, e qualquer outra questão aplicável às suas atividades profissionais;
d. cumprir com os treinamentos de segurança da informação e privacidade promovidos pelo Cartório;
e. conhecer e aplicar em sua rotina de trabalho as regras para criação, coleta, inventário, classificação, rotulagem, manuseio, compartilhamento e descarte de informações e outros ativos associados, conforme diretrizes desta Política e outros documentos aplicáveis;
f. adotar senhas fortes em suas contas de acesso para e-mails, sistemas e estações de trabalho;
g. nunca compartilhar suas senhas em nenhuma hipótese;
h. habilitar autenticação multifatorial (MFA) sempre que este recurso estiver disponível;
i. ter ciência de que todas as contas de e-mail, sistemas, diretórios em nuvem etc. pertencentes ao CARTÓRIO 15 estão sujeitas a monitoramento contínuo e auditoria sem aviso prévio; portanto, é desaconselhada a utilização destes recursos para o armazenamento, compartilhamento ou comunicação de suas informações pessoais;
j. ser cauteloso quanto a "*phishing*" e outras práticas similares, por isso não abrir e-mails, SMS ou outro tipo de mensagem de procedência duvidosa e/ou com assuntos duvidosos;
k. tratar informações pertencentes ao CARTÓRIO 15 exclusivamente através de recursos de TIC fornecidos, homologados ou autorizados, em conformidade com esta Política e demais normas internas estabelecidas;
l. tratar dados pessoais de clientes em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), sempre em consonância com as Políticas e Protocolos instituídos internamente através do programa de *Compliance*, sem prejuízo de outras legislações e regulamentos aplicáveis, e consultar o DPO sempre que houver dúvidas sobre um determinado tratamento;
m. não utilizar sistemas, softwares ou soluções "*as a service*" sem que tenham sido previamente homologados;
n. armazenar arquivos, documentos, códigos fonte etc. pertencentes ao CARTÓRIO 15 em diretórios e locais pré-determinados, conforme regras estabelecidas para governança de informações do Cartório;

o. zelar pelo uso apropriado de recursos de TIC fornecidos pelo CARTÓRIO 15 em conformidade com normas internas e procedimentos estabelecidos;

p. quando autorizado a utilizar recursos próprios de TIC, prática conhecida como "*bring your own device*" (BYOD), fazê-lo exclusivamente dentro das regras e diretrizes previstas pelas normas internas e procedimentos estabelecidos;

q. adotar práticas de mesa limpa e tela limpa, guardar documentos e mídias contendo informações confidenciais em gaveteiros e armários com chave, evitando que informações confidenciais sejam expostas no ambiente de trabalho;

r. adotar medidas cabíveis para proteger as informações do CARTÓRIO 15 – em formato digital ou físico – contra acesso, modificação, destruição ou divulgação não autorizados, mesmo quando fora do Cartório, por exemplo, em *home office* ou viagem;

s. reportar de imediato, através dos canais previamente aprovados e comunicados pelo CARTÓRIO 15, qualquer suspeita de incidentes relacionados à segurança da informação e privacidade;

t. considerar que as diretrizes estabelecidas nesta Política e demais documentos adotados pelo CARTÓRIO 15 não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, os exemplos de medidas, procedimentos e protocolos de segurança da informação utilizados não representam um rol taxativo, cabendo a cada colaborador adotar, além daquelas aqui previstas, outras medidas que considerar necessárias para proteger as informações do CARTÓRIO 15, mediante comunicação proativa sobre tais medidas.

5.3. A Tabeliã, sem prejuízo dos deveres de todos os colaboradores, deve:

a. liderar o tratamento da temática sobre segurança da informação e privacidade, assegurando que os objetivos e diretrizes estejam alinhados ao propósito, cultura, objetivos de negócios e estratégias de mercado do CARTÓRIO 15;

b. liderar a comunicação sobre a importância de segurança da informação e privacidade para o CARTÓRIO 15.

5.4. Colaboradores com função de liderança do CARTÓRIO 15, sem prejuízo dos deveres de todos os colaboradores, devem:

a. promover a comunicação sobre a importância de segurança da informação e privacidade para o CARTÓRIO 15;

b. tomar ciência e informar à Diretoria sobre questões, sobretudo legais e regulatórias, relativas à segurança da informação e privacidade que impactem processos e atividades de sua área de especialidade ou responsabilidade;

c. assegurar que nenhum colaborador sob sua liderança exerça suas funções e atividades sem o conhecimento desta Política e outros documentos de segurança da informação e privacidade aplicáveis;

d. formalizar a solicitação de acessos para seus liderados, observando que estes tenham sempre apenas o acesso necessário, pelo tempo necessário para o exercício de sua função;

e. salvo nos casos de dispensa não planejada e com efeito imediato, formalizar, ao Setor de Recursos Humanos, com antecedência não inferior a 48 horas sobre o desligamento de colaboradores, para que acessos aos recursos de TIC por eles utilizados sejam revogados e as contas bloqueadas;

f. responder, quando for de seu conhecimento, às dúvidas apresentadas por seus liderados, e encaminhá-las à Diretoria sempre que não puder responder;

g. respeitar as bases legais e princípios estabelecidos pela LGPD, políticas e protocolos internos para o tratamento de dados pessoais de todos os colaboradores do CARTÓRIO 15;

h. notificar o Chief Compliance Officer de imediato sobre qualquer comportamento suspeito relacionado à segurança da informação e privacidade por parte de seus liderados;

i. no caso de infração cometida por um liderado, notificar, imediatamente, o Chief Compliance Officer ou por meio da Ouvidoria. O processo de averiguação de irregularidade é realizado pelo Comite de Compliance por meio de uma investigação interna, sendo que somente ele é quem possui atribuição para a aplicação de punição disciplinar.

j. não contratar ou utilizar, nem permitir que sejam contratados ou utilizados em seu departamento, sistemas, softwares ou aplicações que não tenham sido previamente aprovados – prática conhecida como "*shadow IT*".

5.5. O **Responsável pelo TI** do CARTÓRIO 15, sem prejuízo dos deveres de todos os colaboradores e da liderança, deve:

a. assegurar que o CARTÓRIO 15 cumpra com os objetivos de segurança da informação e privacidade estabelecidos pelo SGSI e informar à Tabeliã ou ao Substituto Legal caso, por qualquer motivo, acredite que algum objetivo não está sendo ou será cumprido;

b. assegurar que o CARTÓRIO 15, através de colaboradores ou empresas prestadoras de serviços especializados, conte com todas as competências para implementar e manter recursos tecnológicos dentro dos critérios previstos para mitigação de riscos, conforme plano de tratamento de riscos aprovado, no cumprimento de seus objetivos de governar, identificar, proteger, detectar, responder e recuperar em segurança da informação e privacidade;

c. coordenar a elaboração, revisão quanto a segurança da informação e privacidade e aprovação de procedimentos operacionais de TIC e desenvolvimento seguro;

d. coordenar os esforços para que o CARTÓRIO 15 possua medidas de segurança cibernética aptas a proteger informações e outros ativos associados, inclusive dados pessoais, sobretudo quando classificados como confidenciais, restritos; de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação indevida ou qualquer outro tratamento inadequado ou ilícito;

e. coordenar a implementação, revisão e testes de *backups* para todos os sistemas e serviços de TIC e ativos de informação do CARTÓRIO 15;

f. coordenar os esforços de resposta a incidentes e continuidade de negócios em TIC do CARTÓRIO 15, com objetivo de assegurar a formação e treinamento de um time de resposta, a correta comunicação, deteção e resposta a incidentes e o cumprimento do objetivo do ponto de recuperação (RPO) e o objetivo de tempo de recuperação (RTO);

g. elaborar e manter um plano eficiente e eficaz de gestão de mudanças para os ativos de informação do CARTÓRIO 15 com objetivo de evitar que mudanças de tecnologia possam impactar o negócio e prevenir falhas advindas de *softwares* desatualizados ou equipamentos obsoletos;

h. supervisionar que sejam utilizados apenas *softwares* licenciados e suportados por seus fabricantes;

i. atender colaboradores, clientes e outras partes interessadas relacionadas ao CARTÓRIO 15 quanto às solicitações e questionamentos sobre segurança da informação e privacidade.

5.6. O **DPO** do CARTÓRIO 15, sem prejuízo dos deveres de todos os colaboradores e da liderança, deve:

a. manter conhecimento relevante e atualizado sobre: (i) a LGPD; (ii) outras legislações e regulamentos sobre privacidade e proteção de dados aplicáveis ao CARTÓRIO 15; (iii) melhores práticas para proteção à privacidade; (iv) aspectos nas operações do CARTÓRIO 15 que possam impactar direitos e liberdades dos titulares de dados;

b. elaborar e atualizar, ou assegurar que seja elaborada e atualizada a documentação relevante para privacidade e proteção de dados, sobretudo aquela obrigatória para o cumprimento da LGPD e outros regulamentos aplicáveis ao CARTÓRIO 15;

c. revisar, quando aplicável, os documentos do SGSI quanto à privacidade e proteção de dados;

d. agir com autonomia quanto à proteção dos interesses dos titulares de dados tratados pelo CARTÓRIO 15, e comunicar à Tabeliã caso perceba cerceada tal autonomia;

e. mensurar a eficácia e a efetividade das medidas para proteção à privacidade implementadas pelo CARTÓRIO 15;

f. monitorar as regras internas de privacidade e proteção de dados, obrigações previstas na LGPD e outros regulamentos aplicáveis quanto a sua observância por colaboradores e fornecedores do CARTÓRIO 15;

g. atuar como ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD), comprometendo-se em assegurar que o CARTÓRIO 15 responda às requisições ou medidas necessárias, também buscando orientações proativamente quando considerar apropriado;

h. atuar como ponto de contato entre o CARTÓRIO 15 e os titulares de dados, garantindo que requisições destes sejam atendidas dentro do prazo legal estabelecido e da melhor forma possível;

i. comunicar, dentro das determinações da LGPD, à ANPD e aos titulares de dados nos casos de um incidente ou violação que comprometa dados pessoais;

j. atuar como disseminador da cultura de privacidade e proteção de dados no CARTÓRIO 15, prestando aconselhamento sobre melhores práticas e avaliando a consequência de decisões e operações cotidianas quanto ao tratamento de dados pessoais;

k. prover aconselhamento aos membros da liderança sobre questões relacionadas à privacidade e proteção de dados;

l. informar à Diretoria sobre a necessidade de buscar aconselhamento externo sempre que considerar necessário, tendo em vista o propósito do Cartório, objetivos de negócio e objetivos do SGSI do CARTÓRIO 15.

6. Obrigações, requisitos e expectativas

6.1. O CARTÓRIO 15 deve identificar e manter conformidade com obrigações e requisitos de segurança da informação e privacidade, conforme previstos por legislações e regulamentos aplicáveis, sem prejuízo das obrigações contratuais firmadas.

6.2. Convém que o CARTÓRIO 15 identifique requisitos e expectativas quanto a segurança da informação e privacidade de partes interessadas internas e externas, e como eles serão endereçados pelo SGSI.

7. Privacidade e proteção de dados pessoais

7.1. O CARTÓRIO 15 compreende privacidade e proteção de dados como uma extensão de seus esforços de segurança da informação, e por isso promove sua integração ao SGSI.

7.2. Todo tratamento de dados pessoais deve respeitar as bases legais previstas na LGPD e no Provimento CNJ n° 134/2022, sem prejuízo do cumprimento das regras dispostas nesta Política e na **Política de Privacidade** instituída nesta serventia extrajudicial.

7.3. O tratamento de dados pessoais pelo CARTÓRIO 15 deve ser mapeado, para que possam ser identificados riscos para os titulares de dados e adotadas medidas apropriadas para mitigar estes riscos.

8. Gestão de riscos

8.1. O SGSI do CARTÓRIO 15 deve ser governado por um processo de gestão de riscos conforme estabelecido pelo **Plano para Gestão de Riscos de Segurança da Informação e Privacidade**, através do qual riscos são identificados, analisados quanto a sua probabilidade e consequência, avaliados quanto aos critérios estabelecidos e determinado um plano de tratamento, que deve ser executado conforme apropriado.

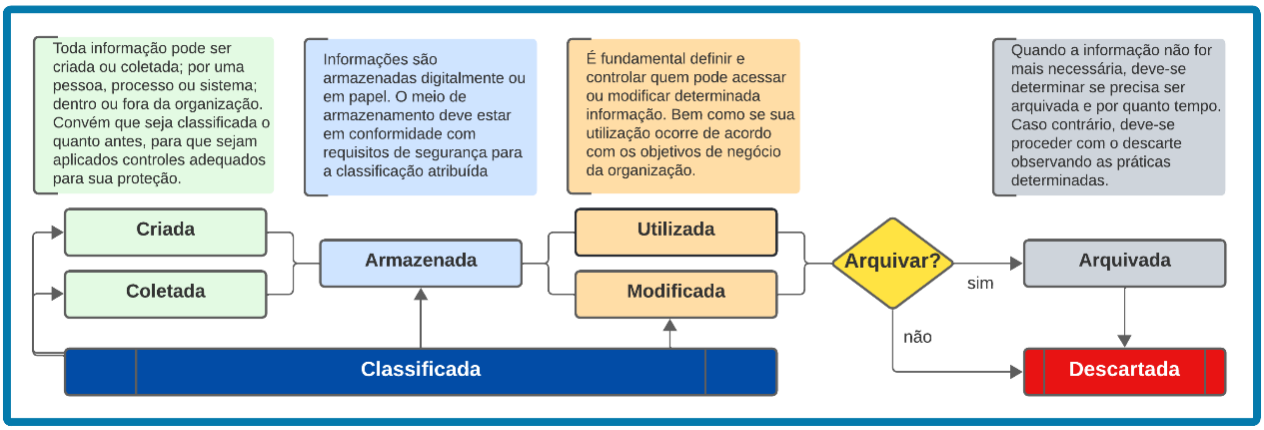
8.2. Avaliações de riscos de segurança da informação e privacidade devem ser repetidas a cada 12 meses, ou sempre que houver uma mudança significativa no ambiente de negócios, ou quando for deliberada como relevante pela Diretoria.

8.3. O plano de tratamento de riscos do CARTÓRIO 15 deve prever a implementação de controles de segurança da informação e privacidade aplicáveis ao Cartório, levando em conta recomendações da ISO/IEC 27002:2022 e de outros *frameworks* e melhores práticas reconhecidos de mercado.

8.4. O CARTÓRIO 15 deve assegurar a implementação e manutenção de ferramentas tecnológicas aptas a mitigar os riscos avaliados a um nível aceitável.

9. Ciclo de vida da informação

9.1. Compreende-se que toda informação tratada pelo CARTÓRIO 15, independentemente dos meios utilizados, é criada ou coletada, armazenada em formato digital ou físico, ao longo de seu ciclo de vida é acessada, utilizada, e pode ser modificada e compartilhada. Quando não é mais necessária, esta informação deve ser arquivada e/ou descartada. Todas as etapas previstas no Ciclo de Vida da Informação devem ocorrer conforme regras dispostas nesta Política.



9.2. Conforme a ISO/IEC 27005:2022, informações, assim como os processos de negócio ligados diretamente a elas devem ser considerados ativos primários para o CARTÓRIO 15, enquanto ativos como colaboradores, fornecedores, infraestrutura, dispositivos, sistemas e serviços de TIC devem ser considerados ativos de suporte, referenciados nesta política também como ativos associados.

9.3. O proprietário da informação é o responsável direto por aquela informação. Por exemplo: o gestor de um determinado departamento é o proprietário das informações daquele departamento.

9.4. Convém que a classificação ocorra o quanto antes possível no ciclo de vida da informação, de forma que seja possível a aplicação de controles apropriados para sua proteção e de seus ativos associados.

10. Informação documentada

10.1. O CARTÓRIO 15 deve determinar, elaborar, revisar, aprovar e controlar políticas, normas internas, planos, procedimentos, inventários, modelos, imagens, fluxogramas, termos, regras, instruções, relatórios e outros documentos, que em conjunto com esta Política, sejam considerados necessários para atender aos objetivos do SGSI e seu suporte ao cumprimento dos objetivos de negócio.

10.2. Toda informação documentada deve respeitar regras para elaboração, formatação e controle estabelecidas pelo CARTÓRIO 15 e sempre que possível deve-se utilizar um modelo previamente aprovado.

10.3. Todas as informações tratadas pelo CARTÓRIO 15 devem ser inventariadas conforme seus ativos associados, usuários ou departamentos autorizados para acesso, regras para classificação, armazenamento, compartilhamento, arquivamento e descarte e controles de segurança no documento **Inventário de Informações e Processos de Negócio.**

10.4. Todos os dados pessoais tratados pelo CARTÓRIO 15 em suas atividades de negócio, assim como o processo para coleta, responsáveis pelo tratamento das informações, regras para armazenamento, compartilhamento, arquivamento e descarte, e bases legais mapeadas para cada atividade devem constar no documento **Inventário de Dados Pessoais**.

10.5. Todos os sistemas, serviços de TIC e softwares autorizados pelo CARTÓRIO 15 devem constar no **Inventário de Sistemas, Serviços de TIC e Softwares.**

10.6. Todos os inventários devem ser mantidos atualizados e relevantes para as atividades de negócio do CARTÓRIO 15.

11. Acesso à informação

11.1. O CARTÓRIO 15 deve adotar medidas adequadas para proteger e controlar o acesso às suas informações, de seus clientes e outras partes interessadas, sobretudo quando classificadas como informações confidenciais.

11.2. O acesso às informações pertencentes ao CARTÓRIO 15, ou tratadas sob sua responsabilidade, deve ocorrer exclusivamente através de identidades controladas ou homologadas pela serventia extrajudicial.

11.3. As atividades de criação, gestão, proteção, monitoramento, revogação, desativação e exclusão de identidades e acessos a informações, infraestrutura, sistemas e serviços de TIC mantidos pelo CARTÓRIO 15 devem ocorrer conforme autorizado pelo proprietário da informação, respeitando princípios e regras desta Política.

11.4. Convém que acessos atribuídos sejam baseados nos seguintes princípios de segurança:

- **a.** necessidade de conhecer (*need-to-know*): uma entidade só tem acesso às informações que requer para executar suas tarefas;
- **b.** menor privilégio ou necessidade de uso (*least privilege)*: todo acesso para uso de um recurso deve ser atribuído com o menor privilégio possível para execução da tarefa pretendida;
- **c.** acesso sob demanda (*just-in-time*): acessos devem ser liberado apenas pelo tempo necessário para execução das tarefas pretendidas.

11.5. Convém que acessos privilegiados sejam devidamente justificados, autorizados pelo proprietário da informação, atribuídos, sempre que possível, seguindo os princípios de segurança anteriormente mencionados e documentados no **Inventário de Sistemas, Serviços de TIC e Softwares,** incluindo a descrição dos privilégios concedidos.

11.6. Convém que sejam mantidas um mínimo de duas e um máximo de quatro contas de usuário com privilégios administrativos máximos (geralmente referenciados como "system admin", "global admin", "superusuário" ou "root user") para todos os sistemas e serviços de TIC em uso pelo CARTÓRIO 15.

11.7. Recursos de complexidade de senhas e autenticação multifatorial (MFA) devem ser habilitados para todas as identidades e acessos do CARTÓRIO 15 sempre que estiverem disponíveis.

11.8. Convém que sistemas e serviços de TIC que não suportem MFA não sejam contratados ou sejam substituídos por soluções que suportem este recurso.

11.9. Registros ("*logs*") de acessos bem-sucedidos e tentativas malsucedidas devem ser mantidos por um período mínimo de 30 dias, conforme recursos disponíveis de cada sistema.

12. Classificação e rotulagem das informações

12.1. O esquema de classificação de confidencialidade de informações foi determinado levando em conta o valor estratégico da informação para o CARTÓRIO 15, requisitos legais, regulatórios, contratuais e de partes interessadas ligadas ao Cartório e dano potencial financeiro, operacional e reputacional caso a informação seja divulgada.

12.2. Os rótulos para classificação de ativos de informação pertencentes ao CARTÓRIO 15 são:

Rótulo	Definição / Exemplo
Pública	Informação cuja revelação causa danos aos negócios da Cartório, desde que observada sua integridade. Dados de domínio público e que podem ser divulgados livremente. **Exemplo:** informações disponíveis no site.
Interna / Uso Interno	Informação que pode ser divulgada para todos os colaboradores e prestadores de serviços. Entende-se que divulgar estas informações publicamente pode causar dano de menor potencial aos interesses e objetivos de negócio do Cartório. **Exemplo:** políticas e procedimentos internos.
Confidencial	Informação de caráter sigiloso, que deve ser conhecida apenas por determinados indivíduos ou departamentos dentro do Cartório, que necessitem do acesso a esta informação para o exercício de suas atividades ("*need-to-know*"). Entende-se que a divulgação indevida destas informações causará impacto significativo de curto ou

	médio prazo aos objetivos de negócio, interesses ou operações do Cartório. **Exemplos:** informações estratégicas departamentais.
Secreta	Informação de caráter altamente sigiloso, que deve ter seu acesso controlado, podendo ser acessada apenas por indivíduos especificamente relacionados. Sempre deve ser avaliado criticamente quem pode ter acesso, através de quais meios ela será acessada e quais controles existem para proteger sua confidencialidade e integridade. Entende-se que a divulgação indevida de informações classificadas como secretas tem um sério impacto aos objetivos e interesses de longo prazo do Cartório, podendo colocar a existência do negócio em risco. **Exemplo:** informações sobre o planejamento estratégico de longo prazo.

12.3. Convém que a classificação de informações ocorra através da aplicação dos rótulos relacionados:

- **a.** aos cabeçalhos ou rodapés de todos os documentos pertencentes ao CARTÓRIO 15,
- **b.** conforme modelo aprovado para elaboração do documento;
- **c.** através de rótulos de confidencialidade configurados para o Microsoft 365;
- **d.** através de marcas d'água aplicada a informações classificadas como secretas.

12.4. A classificação da informação deve ser realizada pelo proprietário da informação. Esta atividade pode ser delegada, mas o proprietário da informação continua sendo o responsável pela classificação e rotulagem.

12.5. Todo documento que contenha dados pessoais sensíveis deve ser classificado por padrão como confidencial.

12.6. Informações classificadas como confidenciais e secretas podem ser referenciadas coletivamente como informações confidenciais. Quando um controle ou característica for aplicável apenas a informações secretas ou requerer este nível de confidencialidade, esta deve ser referenciada especificamente.

12.7. Apenas membros da Diretoria do CARTÓRIO 15 podem alterar o rótulo de informações classificadas como secretas.

13. Armazenamento, utilização e modificação de informações

13.1. Informações confidenciais devem ser armazenadas exclusivamente em infraestrutura, diretórios, sistemas, serviços de TIC, dispositivos e mídias previamente homologados pelo CARTÓRIO 15.

13.2. Convém que toda informação mantida em qualquer meio digital de armazenamento controlado pela CARTÓRIO 15 receba criptografia em repouso e em trânsito.

13.3. Toda informação pertencente ou tratada sob a reponsabilidade ou de propriedade do CARTÓRIO 15 deve estar sujeita a uma rotina de backup compatível com sua relevância para o Cartório, conforme determinado pelo **Plano de Resposta a Incidentes e Continuidade de Negócios** alinhado ao **Inventário de Informações e Processos de Negócio**.

13.4. Convém que sempre que houver modificação em uma informação ou ativo associado, seja avaliado se a classificação atribuída permanece adequada.

14. Compartilhamento de informações

14.1. O compartilhamento, sobretudo externo, de informações deve ser gerenciado e controlado conforme rótulos de classificação aplicados.

14.2. Informações classificadas como públicas podem ser compartilhadas livremente.

14.3. Informações classificadas como internas podem ser compartilhadas com qualquer colaborador do CARTÓRIO 15.

14.4. O compartilhamento interno de informações confidenciais deve ser realizado baseado na função do colaborador conforme sua necessidade de acesso (*"need-to-know"*) a esta informação.

14.5. O compartilhamento interno ou externo de qualquer informação classificada como secreta deve ser explicitamente autorizado pela Diretoria do CARTÓRIO 15.

14.6. Convém que seja evitado o compartilhamento de informações confidenciais como anexo de e-mails, e seja priorizado o compartilhamento via um link seguro para acesso ao documento ou à sua pasta.

14.7. Convém que nenhuma informação confidencial seja compartilhada com partes externas, como prestadores de serviços e parceiros comerciais, sem a assinatura de um Termo de Confidencialidade.

15. Arquivamento de informações

15.1 Convém que o arquivamento de informações esteja sujeito à análise prévia quanto a sua necessidade e conformidade com os objetivos de negócio do CARTÓRIO 15 e requisitos legais, regulatórios e/ou contratuais aos quais a organização esteja sujeita.

15.2 O arquivo morto deve ser mantido através de um diretório previamente homologado, com acesso controlado, prazo para retenção e recuperação conforme documentado no **Inventário de Informações e Processos de Negócio**.

15.3 Convém que o arquivamento físico de informações impressas seja evitado e, caso necessário, ocorra em local seguro, trancado, com acesso controlado, monitorado por câmeras de segurança e respeitando o mesmo prazo para retenção de informações em formato digital.

16. Descarte de informações e outros ativos associados

16.1. Toda informação que não for mais necessária para as atividades operacionais, para os objetivos do negócio ou cumprimento de obrigações legais, regulatórias ou contratuais do CARTÓRIO 15 deve ser descartada e destruída de forma irrecuperável por seu proprietário, ou custodiante autorizado, através dos métodos descritos a seguir conforme aplicável:

Método	Descrição	Aplicabilidade
Excluir documentos ou pastas do diretório	Excluir documentos ou pastas que não sejam mais necessários.	Qualquer documento ou pasta em qualquer formato.
Excluir informações do sistema	Excluir informações do sistema.	Informações dos sistemas mantidos pelo Cartório, listados nos inventários correspondentes.
Excluir e-mails ou mensagens do Microsoft Teams	Excluir e-mail/mensagem.	E-mails e mensagens do Microsoft 365 acessadas por contas corporativas.
Triturar de papel	Triturar documentos utilizando os trituradores de papel disponibilizados pelo Cartório	Documentos impressos classificados como internos, confidenciais ou restritos.
Sobregravar / Expurgar mídia	Expurgar dados utilizando software específico homologado pelo Departamento de Tecnologia da Informação.	HDs, SSDs, pen drives, CDs e DVDs que serão reaproveitados.

Remover disco	Remover e destruir disco (HD ou SSD) de computador que será reaproveitado.	Computadores em geral, tanto desktops quanto laptops.
Aplicar criptografia de caminho único.	Uso de um hash para criptografia tipo "*one-way*" (por exemplo: SHA256) homologado previamente pelo Departamento de Tecnologia da Informação para criptografar uma informação de forma irrecuperável.	HDs, SSDs, pen drivers, CDs e DVDs que serão descartados.
Acionar remoção por empresa especializada	Remoção de ativo por empresa especializada em descarte seguro homologada.	Computadores, smartphones, servidores etc.
Destruir ativo fisicamente	Destruição física do ativo de forma irrecuperável, como através do uso de incineradores, ácido ou pulverizadores previamente homologados.	Qualquer ativo que não seja reaproveitado.

16.2. O descarte efetivo das informações, documentos e mensagens apenas será considerado após o prazo de retenção, conforme regras de backup previstas.

16.3. A necessidade de exclusão imediata de informações e documentos do backup está sujeita a análise de viabilidade técnica, e deve ser comunicada ao Responsável pelo TI.

16.4. Convém que todos os documentos contendo informações confidenciais sejam triturados antes do descarte.

16.5. Dispositivos como computadores, laptops, smartphones, tablets, mídias removíveis etc. contendo informações do CARTÓRIO 15 devem passar por um procedimento conforme homologado antes de sua efetiva reutilização ou doação.

16.6. Dispositivos como computadores, laptops, smartphones, tablets, mídias removíveis etc. contendo informações do CARTÓRIO 15 devem ser descartados de forma segura conforme regras desta Política.

16.7. O descarte e destruição físico de qualquer ativo de TIC deve ocorrer respeitando as melhores práticas de sustentabilidade e responsabilidade ambiental.

17. Relações com colaboradores

17.1. O CARTÓRIO 15 deve gerenciar riscos na seleção, contratação, relações, mudança ou encerramento de contrato com colaboradores conforme regras desta Política**.**

17.2. O CARTÓRIO 15 de respeitar as bases legais e princípios estabelecidas pela LGPD e outras legislações e regulamentos aplicáveis para proteção da privacidade aplicáveis para o tratamento de dados pessoais de todos os colaboradores.

17.3. Convém que o processo de seleção para novos colaboradores inclua as seguintes etapas:

- **a.** verificação da identidade do colaborador através de documento original apresentado;
- **b.** verificação das informações do curriculum vitae e do LinkedIn, incluindo a verificação das qualificações profissionais e acadêmicas alegadas;
- **c.** verificação das redes sociais publicamente disponíveis;
- **d.** verificação do histórico funcional mantido no TJRJ, quando aplicável;
- **e.** solicitação de referências profissionais de empresas onde o colaborador tenha trabalhado ou prestado serviços anteriormente.

17.4. Todo colaborador contratado pelo CARTÓRIO 15 deve assinar, no ato de sua contratação, um contrato onde constem:

- **a.** declaração de sua responsabilidade para com segurança da informação e privacidade;
- **b.** declaração de seu compromisso e ciência sobre está Política, Código de Ética e os demais documentos implementados pelo programa de compliance do Cartório e demais documentos relevantes de segurança da informação e privacidade;
- **c.** declaração de seu compromisso em cumprir treinamentos sobre segurança da informação e privacidade;
- **d.** cláusulas de confidencialidade e não revelação compatíveis com as informações às quais terá acesso;
- **e.** cláusulas relacionadas ao tratamento de dados pessoais, relevantes para LGPD e outras legislações e regulamentos aplicáveis;
- **f.** cláusulas sobre regras de propriedade intelectual.
- **g.** declaração de sua concordância com regras estabelecidas para a mudança ou encerramento da contratação.

17.5. Deve ficar estabelecido que o compromisso com a confidencialidade não se extingue com o encerramento do contrato celebrado e que o colaborador permanece obrigado a manter este compromisso com o sigilo sobre informações recebidas por tempo indeterminado, inclusive abstendo-se de utilizar tais informações reveladas pelo CARTÓRIO 15.

17.6. O CARTÓRIO 15 deve conscientizar seus colaboradores sobre questões de segurança da informação e privacidade, e fornecer treinamentos conforme apropriado.

17.7. O CARTÓRIO 15 deve assegurar que para cada colaborador sempre seja concedido apenas os acessos necessários pelo tempo necessário para o exercício de suas funções. Estes acessos devem ser monitorados e revisados regularmente.

17.8. Contas de e-mail e sistemas, computadores, smartphones e outros recursos de TIC concedidos pelo CARTÓRIO 15 para o exercício de atividades em nome do Cartório devem ser utilizados de forma adequada conforme regras estabelecidas, sendo expressamente proibida sua utilização para qualquer propósito impróprio ou ilegal.

17.9. O CARTÓRIO 15 pode permitir a utilização de dispositivos do próprio colaborador para acesso a informações e/ou exercício de atividades funcionais, prática conhecida como "Bring Your Own Device" (BYOD). Dispositivos BYOD devem ser homologados através de um procedimento interno aprovado pelo Responsável pelo TI.

17.10. Convém que o desligamento de qualquer colaborador seja informado com antecedência cabível ou imediatamente, em caso de dispensa não planejada, ao Departamento de TI para que os que acessos aos sistemas e recursos tecnológicos sejam revogados.

18. Relações com fornecedores

18.1. A seleção, contratação, relações, mudança ou encerramento de contratação de fornecedores e prestadores de serviços pelo CARTÓRIO 15 deve ocorrer conforme regras desta Política.

18.2. Convém que O CARTÓRIO 15 promova a análise de riscos referente aos serviços contratados conforme o **Procedimento para Avaliação de Riscos na Contratação de Fornecedores** para determinar para determinar a contratação ou renovação de contratos com seus fornecedores, sobretudo com aqueles que acessam informações confidenciais ou fornecem serviços críticos para a organização.

18.3. Para fornecedores já contratados na data de emissão desta Política, convém que seja realizada uma avaliação de riscos conforme o **Procedimento para Avaliação e Riscos na Contratação de Fornecedores** para a renovação do contrato, priorizando fornecedores conforme criticidade e nível de acesso à infraestrutura de TIC crítica e informações confidenciais do CARTÓRIO 15.

18.4. Convém que sejam considerados para os contratos com fornecedores que tratem informações confidenciais ou forneçam serviços de TIC críticos para o CARTÓRIO 15 seções e/ou cláusulas que abordem os seguintes tópicos conforme aplicável:

a. requisitos legais, regulatórios ou contratuais, como, por exemplo, referentes à privacidade e proteção de dados, ou propriedade intelectual, que possam estar relacionados ao contrato firmado;
b. cláusulas de **confidencialidade e não-revelação** adequadas à sensibilidade das informações tratadas;
c. adequação do fornecedor à LGPD e outras legislações e regulamentos aplicáveis para proteção da privacidade aplicáveis;
d. métodos e regras para compartilhamento e acesso de informações confidenciais;
e. Acordo de Nível de Serviço (*Service Level Agreement*, SLA na sigla em inglês) que estabeleça requisitos para os serviços prestados compatíveis com as obrigações legais ou contratuais do CARTÓRIO 15;
f. requisitos de treinamento e conscientização de prepostos do fornecedor que tenham acesso a informações do CARTÓRIO 15;
g. regras relacionadas a subcontratação, incluindo processo de devida diligência e controles que precisem ser implementados;
h. requisitos e procedimentos para gestão de incidentes de segurança da informação e privacidade, incluindo obrigações e prazo para notificação por parte do fornecedor em caso de incidente;
i. regras para a mudança ou encerramento da contratação, abordando inclusive a retenção, transferência ou exclusão de informações pertencentes ao CARTÓRIO 15.
j. obrigação do fornecedor em apresentar políticas, normas, planos, procedimentos, relatórios de auditoria, relatórios de vulnerabilidades, testes de invasão ou outros documentos que evidenciem a implementação de controles para assegurar um nível adequado de segurança da informação e privacidade;
k. direito de auditar processos e controles do fornecedor relacionados ao escopo do contrato;
l. regras para retenção e descarte de informações pertencentes ao CARTÓRIO 15 durante e após o encerramento da contratação;
m. obrigação de o fornecedor colaborar com o CARTÓRIO 15, fornecendo suporte necessário no caso de mudança ou encerramento da contratação.

18.5. Convém que em contratos com fornecedores, que sejam operadores ou co-controladores de dados pessoais de clientes, sócios, colaboradores e outras partes interessadas do CARTÓRIO 15, sejam consideradas também, além dos itens da cláusula anterior, seções e/ou cláusulas que abordem:

a. registro de operações de tratamento de dados pessoais (Record of Processing Activities, ROPA na sigla em inglês) de dados pessoais tratados conforme requisitos da LGPD e outras legislações e regulamentos aplicáveis;
b. acordo de processamento de dados (data process agreement, DPA na sigla em inglês);
c. dados para contato do encarregado de dados (DPO) do fornecedor;

d. relatório de impacto a proteção de dados pessoais (RIPD).

18.6. Os contratos de serviços em nuvem são geralmente predefinidos e por adesão. Por este motivo, na contratação de serviços em nuvem deve-se verificar se o provedor de serviços indica em seu termo de adesão e políticas publicadas atender às questões de segurança da informação e privacidade relevantes para os serviços contratados.

18.7. Para serviços em nuvem que armazenem informações confidenciais, provisionem infraestrutura ou sistemas e serviços de TIC críticos para a CARTÓRIO 15, convém que sejam contratados apenas fornecedores certificados ISO/IEC 27001:2022 e com relatórios SOC 2 tipo 2 atualizados.

18.8. O CARTÓRIO 15 deve determinar se o armazenamento de dados disponibilizado pelo fornecedor de serviços em nuvem ocorre em locais aprovados (país ou região) em conformidade com a LGPD e outras legislações e regulamentos aplicáveis.

18.9. Convém que o CARTÓRIO 15 mantenha um **Inventário de Fornecedores** com fornecedores de TIC ativos, incluindo informações mapeadas sobre o risco de cada fornecedor.

18.10. Convém que fornecedores, sobretudo de importância crítica para o CARTÓRIO 15, sejam monitorados e avaliados regularmente sobre aderência aos acordos firmados.

18.11. Antes de comunicar ao fornecedor a mudança ou encerramento da contratação, deve ser determinado o impacto de tal medida para o CARTÓRIO 15, levando em conta fatores como:

a. acessos mantidos pelo fornecedor a informações, infraestrutura ou sistemas e serviços de TIC do CARTÓRIO 15;
b. questões de propriedade intelectual;
c. equipamentos do fornecedor alocados nas premissas do CARTÓRIO 15;
d. portabilidade de informações em caso de alteração do fornecedor ou internalização.

18.12. Caso trate-se de uma mudança de fornecedor, a transferência de informações e/ou serviços utilizados pelo CARTÓRIO 15 deve ser supervisionada e documentada pelo responsável direto pelo contrato com o fornecedor.

18.13. Convém que o CARTÓRIO 15 documente uma estratégia para alterar ou interromper o uso de serviços em nuvem, incluindo estratégias para troca de fornecedores e soluções alternativas.

18.14. Convém que, após o encerramento da contratação, seja avaliada a necessidade de se obter declaração formal do fornecedor quanto à exclusão de informações do CARTÓRIO 15, conforme requisitos do contrato firmado.

19. Segurança física e de ambiente

19.1. O acesso físico às instalações e escritórios restritos (sem acesso ao público) do CARTÓRIO 15 está autorizado aos colaboradores apenas durante o horário previsto para realização de suas atividades funcionais. Qualquer acesso fora deste horário deve ser explicitamente autorizado pelo gestor responsável.

19.2. Convém que instalações e escritórios do CARTÓRIO 15 sejam monitoradas por circuito fechado de TV (CFTV).

19.3. Convém que os CPDs do CARTÓRIO 15:

- **a.** sejam localizados em salas ou instalações dedicadas para esta finalidade;
- **b.** estejam protegidos contra intempéries naturais, problemas estruturais e ameaças humanas;
- **c.** sejam mantidos trancados e tenham seu acesso controlado e autorizado apenas a colaboradores do Departamento de TI, membros da diretoria e fornecedores autorizados;
- **d.** possuam controle de acesso digital por biometria;
- **e.** possuam recursos de tolerância a falhas provocadas pela interrupção de serviços essenciais como energia elétrica ou internet;
- **f.** contem com recursos para de climatização e controle de umidade apropriados conforme padrões aceitos de mercado;
- **g.** contem com câmeras de segurança cobrindo acessos e área interna com ponto e contraponto, conforme o necessário.

19.4. Convém que a impressão de informações confidenciais seja evitada.

19.5. Os colaboradores devem atentar para não deixar documentos contendo informações confidenciais em impressoras, multifuncionais ou scanners.

19.6. Qualquer informação confidencial em formato físico, como impressa ou gravada em mídias como HD externo, pen drive, CD ou DVD, deve ser armazenada em cofres, armários ou gavetas trancadas.

20. Gestão de mudanças

20.1. Toda mudança que possa impactar os objetivos e diretrizes do SGSI, tais como mudanças de estratégias, processos ou ferramentas tecnológicas, devem ser avaliadas quanto ao seu impacto, planejadas, autorizadas pela Diretoria e comunicadas às partes interessadas com antecedência conforme apropriado.

20.2. Mudanças emergenciais, nas quais não seja possível seguir as regras e procedimentos existentes, devem ser documentadas e, posteriormente, avaliadas pelo Diretoria.

21. Resposta a incidentes e continuidade de negócios

21.1. O CARTÓRIO 15 deve estabelecer um **Plano de Resposta a Incidentes e Continuidade de Negócios** com objetivo de implementar controles aptos a detectar e responder a incidentes de segurança cibernética, assim como estar pronto para recuperar informações, infraestrutura, sistemas e serviços de TIC dentro dos objetivos de tempo de recuperação (RTO) e de ponto de recuperação (RPO) estabelecidos.

21.2. Convém que o CARTÓRIO 15 estabeleça e treine um time de resposta a incidentes de segurança cibernética com colaboradores da organização, que devem receber orientação, treinamento e realizar exercícios, conforme apropriado.

21.3. Convém que sejam estabelecidos planos de contingência para assegurar a continuidade operacional no caso de falhas e disrupções potenciais mapeadas para mudanças críticas para o CARTÓRIO 15.

21.4. Convém que o CARTÓRIO 15 assegure que recursos de TIC sejam planejados, implementados, testados e monitorados para assegurar a continuidade de negócios em caso de incidente, violação ou qualquer disrupção.

21.5. O CARTÓRIO 15 deve estabelecer uma rotina cópias de segurança ("*backups*") de documentos, sistemas, serviços de TIC e bancos de dados importantes para a organização.

21.6. Convém que os *backups* sejam testados regularmente quanto a sua integridade e a capacidade de atender ao RTO e RPO estabelecidos.

21.7. O CARTÓRIO 15 deve manter redundância de toda infraestrutura considerada crítica.

22. Conscientização, treinamentos e comunicação

22.1 O CARTÓRIO 15 deve assegurar a comunicação, disponibilidade digital e treinamentos sobre esta Política e outros documentos do SGSI para os colaboradores conforme necessidade.

22.2 Convém que o CARTÓRIO 15 avalie requisitos para comunicação, disponibilidade digital e treinamentos sobre esta Política e outros documentos do SGSI com partes externas conforme legislações, regulamentos e contratos aplicáveis à organização.

22.3 O CARTÓRIO 15 deve promover a conscientização sobre segurança da informação e privacidade.

22.4 Convém que a conscientização sobre segurança da informação e privacidade faça uso de treinamentos ao vivo e gravados, mídias diversas distribuídas pelos canais de comunicação homologados pela CARTÓRIO 15, testes de *phishing* promovidos para todos os usuários, entre outras iniciativas conforme apropriado.

23. Tratamento de exceções

23.1. Exceções para diretrizes e regras estabelecidas nesta e outras políticas estabelecidas pelo CARTÓRIO 15 devem ser aprovadas pela Diretoria.

23.2. Toda não-conformidade com regras estabelecidas por esta Política deve ser avaliada e tratada, observando seu impacto para os objetivos de segurança da informação e privacidade do CARTÓRIO 15.

23.3. Todo desvio de regras estabelecidas por esta Política deve ser avaliado para identificar se trata de um incidente de segurança, conforme regras previstas pelo **Plano de Resposta a Incidentes e Continuidade de Negócios**.

24. Processo de Sancionamento Interno

24.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta Política, bem como das demais políticas, planos, normas e procedimentos de segurança da informação e privacidade, são passíveis de penalidades conforme previsto pela **Política de Processamento e Sancionamento Interno.**

24.2. No caso de terceiros contratados ou prestadores de serviço, as sanções aplicáveis poderão ser acumuladas com aquelas previstas pelo contrato estabelecido.

24.3. No caso de violações que infrinjam a legislação vigente, constituam atividades ilegais, incorram ou possam incorrer em dano ao CARTÓRIO 15, o infrator será responsabilizado pelos prejuízos causados, cabendo aplicação das medidas judiciais e indenizatórias pertinentes, sem prejuízo de processo criminal quando aplicável.

25. Melhoria contínua

25.1. O conteúdo desta e demais políticas de segurança da informação e privacidade deve ser revisado sempre que for considerado necessário, e apenas pode ser modificado mediante aprovação pela Diretoria do CARTÓRIO 15.

25.2. O desempenho do SGSI, incluindo dos controles implementados, deve ser medido, monitorado, analisado e avaliado; levando em conta o que precisa ser mensurado, método que deve ser aplicado, quando os resultados devem ser analisados e quem deve analisar e avaliar estes resultados; mantendo todo o processo documentado.

25.3. O CARTÓRIO 15 deve analisar criticamente e buscar melhorar continuamente a pertinência dos objetivos, diretrizes e controles estabelecidos pelo SGSI, bem como seu alinhamento contínuo ao seu propósito, objetivos de negócio e estratégia de mercado, levando em conta fatores como:

a. situação das análises críticas anteriores;
b. mudanças nas questões internas e externas;
c. mudanças no contexto do mercado de atuação do Cartório
d. mudanças em legislações vigentes aplicáveis ao Cartório;
e. resultados de avaliações de riscos;
f. situação de planos de tratamento de riscos;
g. não conformidades e ações corretivas aplicadas;
h. estratégias, processos, tecnologias ou técnicas que possam melhorar o desempenho do SGSI do Cartório.

26. Documentos complementares

26.1. Esta Política não esgota em si todos os instrumentos que direcionam e regulamentam os esforços para assegurar a confidencialidade, integridade e disponibilidade de informações e outros ativos associados pertencentes ao CARTÓRIO 15, ou tratados sob sua responsabilidade.

26.2. O CARTÓRIO 15 deve manter um inventário dos documentos do SGSI na **Lista Mestre de Documentos de Segurança da Informação e Privacidade**.

26.3. Esta política é diretamente complementada por outras políticas e planos relacionados a temas específicos, que podem ser complementados por normas internas, planos, procedimentos, inventários, modelos e outros documentos.

26.4. Os documentos mencionados ao longo desta Política, que a complementam diretamente são:

a. Inventário de Informações e Processos de Negócio
b. Inventário de Sistemas, Serviços de TIC e Softwares
c. Inventário de Dados Pessoais
d. Inventário de Endpoints
e. Inventário de Fornecedores
f. Inventário de Redes e Comunicações
g. Lista Mestre de Documentos de Segurança da Informação e Privacidade

h. Plano de Resposta a Incidentes e Continuidade de Negócios
i. Plano para Gestão de Riscos de Segurança da Informação e Privacidade
j. Política de Conduta
k. Política de Privacidade
l. Procedimento para Avaliação de Riscos na Contratação de Fornecedores
m. Termos e Definições de Segurança da Informação e Privacidade

26.5. No caso de conflito entre diretrizes estabelecidas por esta Política e qualquer outro documento do SGSI deve prevalecer o que está nesta Política.

27. Histórico de alterações

Versão	Data	Responsáveis	Ações
1.0	26/05/2022	Rodrigo Lopes	▪ Elaboração inicial
1.1	22/06/2022	Matheus Alencar Sofia Martinelli	▪ Revisão Privacidade e Proteção de Dados pessoais ▪ Inclusão de questões específicas sobre o Cartório 15
1.2	27/07/2022	Alex Pereira	▪ Revisão geral
2.0	08/05/2024	Rodrigo Lopes	▪ Atualização e melhorias em relação a ISO/IEC 27001:2022; ▪ Inclusão seções sobre ciclo de vida e classificação da informação, identidades e acessos, relações com fornecedores, entre outras.
2.0	02/08/2024	Paulo Camargo	▪ Revisão de Compliance e privacidade e proteção de dados.
2.0	02/09/2024	Alex Pereira	▪ Revisão geral
2.0	06/09/2024	Fernanda Leitão	▪ Revisão e Aprovação