cartório QUINZE

15º OFÍCIO DE NOTAS TABELIÃ FERNANDA DE FREITAS LEITÃO

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Código	POL-SIP
Versão vigente	3
Data da versão vigente	14/05/2025
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.

O CARTÓRIO 15 compreende que a informação acumulada ao longo de mais de um século de funcionamento constitui ativo estratégico de valor inestimável. Sua correta gestão, assegurando confidencialidade, integridade, disponibilidade, rastreabilidade e conformidade legal, é fundamental para a reputação e a continuidade operacional da serventia.

Esta **Política Geral de Segurança da Informação e Privacidade** ("**Política"**) estabelece as diretrizes estratégicas para os esforços de segurança da informação e privacidade do CARTÓRIO 15, alinhadas a normas e melhores práticas reconhecidas, em especial à ISO/IEC 27001:2022 e à ISO/IEC 27002:2022, e em integral observância ao Provimento CNJ nº 213/2026 ("Provimento 213**"**) e à Lei nº 13.709/2018 ("LGPD").

2. Termos e Definições

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

3. Objetivos

3.1. Esta Política deve estabelecer diretrizes e responsabilidades para o planejamento, a implementação, a operação, o monitoramento e a melhoria contínua dos esforços de segurança da informação e privacidade do CARTÓRIO 15, visando assegurar:

a. confidencialidade, integridade e disponibilidade de informações e ativos associados;
b. rastreabilidade e conformidade legal, incluindo o cumprimento integral do Provimento 213 e da LGPD;
c. gestão de riscos de segurança da informação e privacidade baseada em processo sistemático e documentável;
d. integração da segurança da informação e privacidade por padrão (*by default*) e no desenho (*by design*) dos processos e sistemas do CARTÓRIO 15.

3.2. Os esforços de segurança da informação e privacidade do CARTÓRIO 15 são regidos pelos seguintes **princípios**, conforme o Anexo III do Provimento 213:

a. **Confidencialidade**: as informações são acessadas apenas por pessoas autorizadas, conforme a necessidade funcional;
b. **Integridade**: as informações são preservadas em sua exatidão e completude, vedada modificação não autorizada;
c. **Disponibilidade**: as informações e os sistemas estão disponíveis e utilizáveis quando demandados pela operação da serventia;

d. **Rastreabilidade**: as operações sobre as informações são registradas e podem ser reconstituídas mediante trilha de auditoria;
e. **Conformidade legal**: o tratamento da informação observa integralmente as obrigações legais, regulatórias e contratuais aplicáveis ao CARTÓRIO 15.

4. Aplicação

4.1. Esta Política aplica-se à Tabeliã, ao Substituto Legal, aos colaboradores em regime integral, parcial ou temporário, presencial ou remoto, aos estagiários, prestadores de serviço e demais terceiros que tratem informações pertencentes ao CARTÓRIO 15 ou sob sua responsabilidade, abrangendo comunicações verbais, plataformas tecnológicas e mídias físicas.

4.2. As diretrizes desta Política aplicam-se às instalações físicas, sistemas, softwares, ferramentas e demais recursos de tecnologia da informação e comunicação (TIC) pertencentes ao CARTÓRIO 15 ou por ele contratados.

5. Responsabilidades

5.1. Todos os colaboradores, inclusive terceiros autorizados, devem:

a. conhecer e cumprir integralmente esta Política e as demais normas internas de segurança da informação e privacidade aplicáveis à sua função;
b. tratar informações do CARTÓRIO 15 exclusivamente por recursos de TIC homologados, abstendo-se de utilizar sistemas, softwares, recursos de inteligência artificial (IA) e demais serviços não aprovados (prática conhecida como “shadow IT”);
c. adotar senhas fortes e habilitar autenticação multifator (MFA) sempre que disponível, jamais compartilhando credenciais;
d. adotar práticas de mesa limpa e tela limpa;
e. tratar dados pessoais conforme a LGPD, as políticas internas e as orientações do DPO;
f. reportar imediatamente, pelos canais aprovados, qualquer suspeita de incidente de segurança cibernética;
g. cumprir os treinamentos de segurança da informação e privacidade promovidos pelo CARTÓRIO 15.

5.2. A Tabeliã, sem prejuízo dos deveres comuns a todos os colaboradores, lidera a temática de segurança da informação e privacidade, assegurando que objetivos e diretrizes estejam alinhados ao propósito e à estratégia do CARTÓRIO 15, e aprova esta Política e suas revisões.

5.3. Colaboradores com função de liderança e/ou coordenação, sem prejuízo dos deveres comuns, devem:

a. assegurar que nenhum liderado exerça funções sem conhecer esta Política e as normas internas de segurança da informação e privacidade aplicáveis;
b. comunicar à Diretoria questões legais ou regulatórias que impactem processos sob sua responsabilidade;
c. formalizar solicitações de acesso, observando o princípio do menor privilégio, salvo nas hipóteses de dispensa imediata documentadas;
d. notificar o Departamento de TI com antecedência mínima de 48 horas sobre desligamentos planejados;
e. não contratar, nem permitir que sejam contratados em seu departamento sistemas, aplicações, recursos de IA e serviços que não tenham sido previamente autorizados (shadow IT);
f. notificar a Diretoria imediatamente sobre qualquer comportamento suspeito relacionado à segurança da informação e privacidade.

5.4. O Responsável por Tecnologia da Informação e Comunicação (“Responsável TIC”), sem prejuízo dos demais deveres, deve:

a. assegurar que o CARTÓRIO 15 cumpra os objetivos de segurança da informação e privacidade, informando à Tabeliã caso qualquer objetivo não esteja sendo ou não possa ser cumprido;
b. coordenar a implementação, a manutenção e os testes de cópias de segurança e dos demais controles técnicos de segurança;
c. coordenar os esforços de resposta a incidentes e continuidade operacional, conforme o **Plano de Resposta a Incidentes e Continuidade de Negócios;**
d. elaborar e manter plano efetivo de gestão de mudanças aplicável aos ativos de informação;
e. supervisionar a utilização exclusiva de softwares licenciados e com suporte ativo de seus fabricantes.

5.5. O CARTÓRIO 15 mantém a designação formal de um Responsável Técnico pela Implementação do Provimento 213 (“RT”), nominalmente identificado, com registro em ato formal e no dossiê técnico de conformidade. O RT é o interlocutor técnico da serventia perante a fiscalização correicional em matéria de segurança da informação e tecnologia.

5.6. O Encarregado de Dados Pessoais (“DPO”) deve:

a. manter conhecimento atualizado sobre a LGPD, o Provimento 213 e demais regulações aplicáveis à proteção de dados pessoais;
b. elaborar e manter a documentação obrigatória para o cumprimento da LGPD e do Provimento 213;
c. monitorar a observância das regras internas de privacidade e proteção de dados por colaboradores e fornecedores do CARTÓRIO 15;
d. agir com autonomia na proteção dos interesses dos titulares de dados, comunicando à Tabeliã caso perceba tal autonomia cerceada;
e. atuar como ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares de dados;

f. comunicar incidentes que comprometam dados pessoais à ANPD e aos titulares, conforme prazos e procedimentos previstos na LGPD e no **Plano de Resposta a Incidentes e Continuidade de Negócios**;

g. prover aconselhamento à liderança sobre questões de privacidade e proteção de dados;

h. disseminar a cultura de privacidade e proteção de dados no CARTÓRIO 15.

6. Obrigações, Requisitos e Conformidade Legal

6.1. O CARTÓRIO 15 deve identificar e manter conformidade com obrigações de segurança da informação e privacidade previstas em legislações, regulamentos e contratos aplicáveis, incluindo, entre outros, o Provimento 213, a LGPD, a Lei nº 8.935/1994 e as demais normas técnicas expedidas pelo Conselho Nacional de Justiça e pela Corregedoria competente.

6.2. O cumprimento das obrigações desta Política deve ser evidenciado em dossiê técnico de conformidade, mantido sob guarda da serventia, apto à fiscalização correicional, com retenção mínima de 5 (cinco) anos.

7. Gestão de Riscos

7.1. Os esforços de segurança da informação e privacidade do CARTÓRIO 15 devem ser governados por processo formal de gestão de riscos, conforme avaliações de riscos regulares, por meio das quais riscos são identificados, analisados, avaliados e tratados conforme plano de tratamento de riscos estabelecido.

7.2. As avaliações de riscos devem ser realizadas com frequência compatível com o perfil de risco da serventia, e obrigatoriamente sempre que houver mudança significativa no ambiente de negócios, na infraestrutura tecnológica ou no quadro normativo aplicável.

7.3. O plano de tratamento de riscos deve contemplar controles fundamentados na Legislação Vigente, nas exigências do Provimento 213 e nos controles detalhados conforme Norma Técnica ISO/IEC 27002:2022, sem prejuízo de outros *frameworks* e melhores práticas aplicáveis.

8. Gestão de Mudanças

8.1. Toda mudança que possa causar impacto às estratégias, objetivos ou operações do CARTÓRIO 15, incluindo mudanças de processos, infraestrutura, ferramentas, softwares, sistemas e serviços de TIC, deve ser planejada, avaliada, aprovada, implementada e monitorada de forma controlada, com o objetivo de minimizar consequências negativas para a serventia e para a continuidade dos serviços notariais.

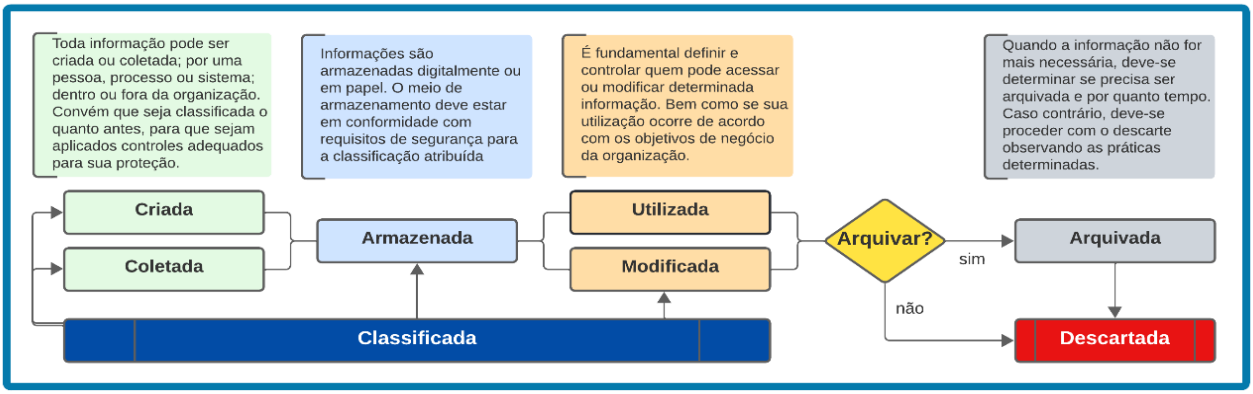
8.2. Sempre que viável, as mudanças devem ser planejadas de modo a mitigar riscos de interrupção ou degradação de serviços, considerando elementos como redundância de recursos e implementação em horários de menor atividade, tais como finais de semana e feriados prolongados.

8.3. A atualização e a substituição de sistemas operacionais, aplicações críticas e demais componentes tecnológicos devem observar o encerramento do suporte oficial pelo fabricante (End of Life, EOL), sendo vedada a utilização de componentes em EOL.

8.4. Convém que toda mudança esteja prevista em procedimento, plano ou projeto documentado e aprovado pela liderança responsável antes de sua implementação.

8.5. Mudanças não controladas devem ser mapeadas periodicamente e tratadas conforme procedimentos específicos, considerando os potenciais riscos para a operação e para a segurança da informação do CARTÓRIO 15.

9. Ciclo de Vida da Informação



9.1. Toda informação tratada pelo CARTÓRIO 15 percorre as etapas de criação ou coleta, armazenamento, acesso, utilização, modificação, compartilhamento, arquivamento e descarte. Todas essas etapas devem ocorrer conforme as diretrizes desta Política e dos documentos complementares aplicáveis.

9.2. Informações e processos a elas associados constituem ativos primários do CARTÓRIO 15. Colaboradores, fornecedores, infraestrutura e sistemas de TIC constituem ativos de suporte.

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.

10. Classificação e Rotulagem das Informações

10.1. Os rótulos de classificação de informações do CARTÓRIO 15 são:

Rótulo	Definição / Exemplo
Pública	Informação de domínio público que pode ser divulgada livremente. Exemplo: informações disponíveis no *site* institucional.
Interna / Uso Interno	Informação acessível a todos os colaboradores e prestadores de serviços. Divulgação pública pode causar dano de menor potencial. Exemplo: Políticas e procedimentos internos.
Confidencial	Informação sigilosa, acessível apenas a indivíduos ou departamentos que dela necessitem (need-to-know). A divulgação indevida causa impacto significativo. Todo documento que contenha dados pessoais sensíveis é classificado como confidencial por padrão.
Secreta	Informação altamente sigilosa, com acesso restrito a indivíduos especificamente relacionados. A divulgação indevida tem impacto severo, podendo colocar a continuidade do negócio em risco. A alteração desse rótulo é restrita à Diretoria. Exemplo: planejamento estratégico de longo prazo.

10.2. A classificação deve ser realizada pelo proprietário da informação o mais cedo possível em seu ciclo de vida, mediante rótulos em cabeçalhos ou rodapés de documentos e rótulos de confidencialidade configurados no Microsoft 365. Essa atividade pode ser delegada, mas o proprietário da informação mantém a responsabilidade pela classificação e rotulagem.

10.3. Informações classificadas como confidenciais e secretas podem ser referidas coletivamente como informações confidenciais. Quando um controle for aplicável apenas a informações secretas, estas devem ser referenciadas de forma específica.

11. Gestão de Identidades e Acessos

11.1. O acesso às informações e aos sistemas do CARTÓRIO 15 deve ocorrer exclusivamente por identidades nominais, controladas e mantidas pela serventia, observando os princípios de:

a. **necessidade de conhecimento (need-to-know)**: acesso somente às informações necessárias ao exercício da função;
b. **menor privilégio (least privilege)**: toda concessão de acesso é atribuída com o menor privilégio possível;
c. **acesso sob demanda (just-in-time)**: liberação restrita ao tempo necessário à execução da tarefa.

11.2. O ciclo de vida das identidades deve observar as seguintes etapas formais, com registro auditável:

a. **Provisionamento**: criação de identidade nominal mediante solicitação formal aprovada pelo gestor responsável, com atribuição de perfil compatível com a função;
b. **Alteração**: revisão e ajuste de privilégios sempre que houver mudança de função, transferência interna, alteração de escopo de atribuições ou afastamento prolongado;
c. **Revogação**: desativação imediata da identidade no desligamento, encerramento do contrato ou perda do vínculo, e exclusão definitiva quando expirados os prazos de retenção legal aplicáveis, observada a LGPD.

11.3. Identidades inativas por período superior a 45 (quarenta e cinco) dias devem ser preventivamente bloqueadas ou desativadas. As identidades de colaboradores desligados devem ser desativadas imediatamente; quando determinada sua exclusão definitiva, esta deve ser realizada de forma irrecuperável, com eliminação dos dados pessoais de cadastro associados, conforme orientação do DPO.

11.4. A autenticação deve observar as seguintes regras:

a. uso obrigatório de autenticação multifator (MFA) para todos os acessos administrativos, de gestão de sistemas, bancos de dados e funcionalidades críticas, conforme exigência do Anexo II do Provimento 213;
b. uso de MFA para todos os acessos a partir de redes externas, dispositivos não corporativos ou em situações de risco identificadas;
c. vedação expressa ao uso de contas genéricas, contas compartilhadas ou credenciais reutilizadas por mais de uma pessoa;
d. preferência por autenticação centralizada e federada (SSO) sempre que tecnicamente viável, com integração ao provedor corporativo de identidade;
e. políticas de senhas fortes, vedação ao reuso de senhas e proteção de credenciais em cofre corporativo homologado.

11.5. As contas privilegiadas (contas com privilégios administrativos sobre sistemas, bancos de dados, dispositivos de rede ou serviços de nuvem) devem observar controles adicionais:

a. manutenção de número limitado de contas, entre 2 (duas) e 4 (quatro) por sistema crítico, suficientes para assegurar continuidade administrativa sem ampliar a superfície de risco;
b. segregação entre conta administrativa e conta de uso cotidiano do mesmo colaborador;
c. registro auditável de toda atividade administrativa relevante;
d. revisão mínima trimestral da lista de contas privilegiadas pelo Responsável TIC.

11.6. As contas de serviço (utilizadas por sistemas, integrações ou automações) devem ser identificadas como tal, mantidas em inventário próprio, com proprietário formalmente designado, escopo de uso documentado e credenciais protegidas em cofre corporativo, vedada sua utilização interativa por pessoas físicas.

11.7. A revisão periódica de acessos deve ser realizada com periodicidade mínima semestral, sob coordenação do Responsável TIC em conjunto com os gestores de área, com o objetivo de confirmar a aderência dos privilégios atribuídos às funções vigentes.

11.8. Os registros de auditoria (*logs*) de acessos bem-sucedidos, tentativas malsucedidas e atividades administrativas devem ser preservados por prazo mínimo de 5 (cinco) anos, em repositório com mecanismos de imutabilidade (*WORM* ou equivalente), segregação de acesso e monitoramento de integridade.

11.9. O acesso remoto à infraestrutura de TIC do CARTÓRIO 15 deve ocorrer exclusivamente por meios seguros e controlados, com MFA obrigatório.

12. Armazenamento, Utilização e Criptografia

12.1. Informações confidenciais devem ser armazenadas exclusivamente em infraestrutura, diretórios, sistemas e mídias previamente homologados pelo CARTÓRIO 15.

12.2. Toda informação pertencente ao CARTÓRIO 15 deve estar sujeita à rotina de cópias de segurança compatível com sua relevância, conforme definido no **Plano de Resposta a Incidentes e Continuidade de Negócios**.

12.3. A criptografia deve ser aplicada a dados em trânsito, em repouso e em *backups*, com algoritmos e protocolos que possuam reconhecimento público, atualização ativa e suporte vigente pelo fabricante. São proibidos algoritmos, protocolos e versões sem suporte ativo (*End of Life*), depreciados ou tecnicamente inseguros.

12.4. Em **trânsito**, todas as comunicações de dados críticos devem utilizar TLS 1.2 ou superior, ou padrão tecnicamente equivalente com suporte ativo. São expressamente proibidas as versões SSL 3.0, TLS 1.0 e TLS 1.1. Os certificados digitais devem ser emitidos por Autoridade Certificadora reconhecida e renovados preventivamente.

12.5. Em **repouso**, os dados críticos armazenados em dispositivos físicos ou virtuais devem ser protegidos por criptografia equivalente, no mínimo, a AES-256, ou padrão tecnicamente equivalente ou superior. A obrigação abrange *backups*. É vedado o armazenamento de dados críticos em dispositivos removíveis sem criptografia previamente aplicada.

12.6. Os mecanismos por ambiente são:

Ambiente	Mecanismo
Microsoft Azure	TLS 1.2+ por padrão; SSE com AES-256 nas contas de armazenamento; TDE com AES-256 nos bancos de dados; chaves gerenciadas via PMK (Platform Managed Keys)

Microsoft 365	TLS 1.2+ e AES-256 aplicados pela Microsoft por padrão, com evidência via Microsoft Trust Center.
Estações e servidores locais	BitLocker com AES-256 em todos os dispositivos Windows.
Backups em mídia local ou removível	Criptografia equivalente a AES-256 aplicada antes do armazenamento, com chave sob custódia exclusiva da serventia

12.7. Para os ambientes Microsoft (Azure e Microsoft 365), onde é adotado o modelo PMK – no qual as chaves são geradas, armazenadas e rotacionadas integralmente pela Microsoft, sem acesso direto pela serventia. A equivalência funcional é demonstrada pelo relatório SOC 2 Type II ou documentação equivalente, publicamente disponibilizada no Microsoft Service Trust Portal.

12.8. Para certificados TLS externos, tokens de assinatura digital e demais chaves fora do ambiente Azure, a custódia é atribuída ao Responsável TIC. Custódia de contingência deve ser designada e registrada em inventário, com acesso restrito auditável, conforme aplicável.

12.9. A rotação e renovação de chaves criptográficas deve seguir critérios técnicos documentados em procedimento interno, observadas as melhores práticas reconhecidas. Em caso de suspeita de comprometimento, a rotação deve ser imediata.

12.10. As operações de geração, renovação e revogação devem ser registradas com data, tipo, identificador do item e responsável pela execução. Em ambiente Microsoft, os Activity Logs registram automaticamente as operações sobre recursos criptografados.

12.11. Os padrões criptográficos adotados devem ser revisados, no mínimo, anualmente, com registro formal das decisões e atualizações decorrentes.

12.12. O CARTÓRIO 15 deve manter em seu **Inventário de Sistemas, Serviços de TIC e Fornecedores** o registro de certificados digitais e chaves criptográficas, contendo, para cada item: identificação, finalidade, validade, emissor ou autoridade certificadora, responsável pela gestão/custódia e data da última alteração. Este inventário deve ser atualizado a cada emissão, renovação ou revogação e, no mínimo, anualmente.

13. Compartilhamento de Informações

13.1. O compartilhamento de informações deve ser gerenciado conforme o rótulo de classificação aplicável:

a. informações públicas podem ser compartilhadas livremente;
b. informações internas podem ser compartilhadas com qualquer colaborador do CARTÓRIO 15;

c. informações confidenciais podem ser compartilhadas internamente com base na função e na necessidade do colaborador (need-to-know);
d. informações secretas só podem ser compartilhadas mediante autorização expressa da Diretoria;
e. nenhuma informação confidencial deve ser compartilhada com partes externas sem assinatura prévia de um termo de confidencialidade ou instrumento equivalente.

14. Arquivamento de Informações

14.1. O arquivamento de informações observa prazos de retenção compatíveis com obrigações legais, regulatórias e contratuais do CARTÓRIO 15. O arquivo digital é mantido em diretório homologado, com acesso controlado. O arquivamento físico é evitado e, quando necessário, ocorre em local seguro e trancado.

15. Descarte de Informações e Ativos Associados

15.1. Toda informação que não seja mais necessária para as atividades operacionais ou para o cumprimento de obrigações legais, regulatórias ou contratuais do CARTÓRIO 15 deve ser descartada de forma irrecuperável. O descarte abrange explicitamente dados pessoais, eliminados de forma definitiva após o encerramento da finalidade que justificou seu tratamento, conforme a LGPD e as orientações do DPO.

Método	Descrição	Aplicabilidade
Excluir documentos ou pastas	Excluir arquivos do diretório, incluindo dados pessoais armazenados.	Qualquer documento ou pasta digital.
Excluir informações de sistemas	Eliminar registros de sistemas, incluindo dados pessoais, após encerramento da finalidade de tratamento.	Sistemas mantidos pelo CARTÓRIO 15.
Excluir e-mails e mensagens (Microsoft Teams e 365)	Excluir e-mails ou mensagens corporativas.	Contas corporativas Microsoft 365.
Triturar papel	Trituração por trituradores homologados.	Documentos impressos internos, confidenciais ou restritos.
Sobregravar ou expurgar mídia	Expurgo por *software* homologado pelo TI.	HDs, SSDs e *pen drives* a reaproveitar.
Remover disco	Remover e destruir fisicamente o disco (HD ou SSD).	Computadores *desktops* e *laptops* a reaproveitar.

Aplicar criptografia de caminho único	*Hash one-way* (ex.: SHA-256) homologado pelo TI para tornar a informação irrecuperável.	Mídias (HD, SSD, *pen drive*, CD/DVD) a descartar.
Acionar empresa especializada	Descarte seguro por empresa homologada.	Computadores, *smartphones*, servidores e equipamentos similares.
Destruição física	Destruição física irrecuperável por método homologado.	Qualquer ativo não reaproveitado.

15.2. O descarte só deve ser considerado efetivo após o decurso do prazo de retenção aplicável.

15.3. A necessidade de exclusão imediata de dados em cópias de segurança está sujeita à análise de viabilidade técnica pelo Responsável TIC.

15.4. O descarte físico de ativos de TIC deve observar as melhores práticas de sustentabilidade e responsabilidade ambiental.

16. Confidencialidade e Não Divulgação

16.1. Todos os colaboradores e fornecedores devem estar cientes de seu compromisso com a confidencialidade das informações do CARTÓRIO 15 e de terceiros tratadas sob sua responsabilidade, incluindo informações de clientes, colaboradores, parceiros e demais partes interessadas.

16.2. Para fins desta Política, todo colaborador e fornecedor deve tratar como confidencial toda informação do CARTÓRIO 15 que não seja de domínio público, independentemente do meio em que se encontre, abrangendo:

- **a.** informações em meios digitais, como plataformas tecnológicas, sistemas, diretórios e documentos digitais;
- **b.** informações em meios físicos, como documentos impressos, manuscritos e mídias removíveis;
- **c.** informações expressas oralmente em reuniões, conversas ou negociações, presencialmente ou por meios eletrônicos.

16.3. Todos os colaboradores e fornecedores com acesso a informações confidenciais devem assinar instrumento formal de confidencialidade e não divulgação, que estabelece que o compromisso com o sigilo é permanente e não se extingue com o encerramento do contrato ou vínculo.

16.4. Deve ser claro para colaboradores e fornecedores, que a violação de obrigações de confidencialidade pode resultar em processo disciplinar interno, rescisão contratual, ações indenizatórias por perdas e danos materiais, morais ou lucros cessantes, e responsabilização civil e criminal, conforme aplicabilidade ao contexto e legislação vigente.

17. Segurança de Recursos de TIC

17.1. O CARTÓRIO 15 deve implementar e manter controles técnicos de segurança cibernética proporcionais ao seu porte, perfil de risco e às exigências do Provimento 213, abrangendo:

a. **Proteção de *endpoint*:** todos os dispositivos utilizados para tratamento de informações do CARTÓRIO 15 devem contar com ferramentas para proteção contra *malware*, com recursos avançados para análise comportamento capacidade de detecção em tempo real, além de atualizações automáticas de softwares instalados.
b. ***Firewall* e segmentação de rede:** o CARTÓRIO 15 deve implementar *firewall de próxima geração* (NGFW) ou solução equivalente com capacidades de IPS/IDS e adotar segmentação lógica de redes compatível com a criticidade da serventia, isolando redes de acesso público das redes internas e dos sistemas críticos;
c. **Wi-Fi para visitantes:** redes sem fio de acesso a visitantes e público externo devem ser segregadas das redes internas em todas as unidades;
d. **Proteção de e-mail:** o serviço de e-mail corporativo deve contar com mecanismos de autenticação de domínio (SPF, DKIM e DMARC), filtragem de mensagens maliciosas e *phishing*, além de recursos para criptografia de comunicações em trânsito;
e. **Filtro de conteúdo e acesso à *web*:** convém que sejam implementados recursos para bloqueio de domínios e *sites* maliciosos ou indesejados, com monitoramento de atividades suspeitas e prevenção de envio não autorizado de informações a destinos externos;
f. **Acesso remoto seguro:** o acesso externo à infraestrutura de TIC do CARTÓRIO 15 deve ocorrer exclusivamente por meios seguros e controlados, com MFA obrigatório;
g. **Inventários:** o CARTÓRIO 15 deve manter inventários atualizados de seus dispositivos, sistemas, serviços de TIC e softwares, incluindo histórico de atualizações e vigência de suporte dos fabricantes.

18. Segurança Física e de Ambiente

18.1. O CARTÓRIO 15 deve implementar controles de segurança física para o ambiente de trabalho, abrangendo instalações, equipamentos, estações de trabalho, mídias removíveis, impressoras e demais periféricos.

18.2. Os controles de segurança física devem ser revistos atualizados, considerando, conforme aplicável, os seguintes elementos:

a. controle de acesso físico a escritórios e instalações restritas;
b. recursos para identificação de colaboradores e visitantes;
c. controle e supervisão do acesso de visitantes;

d. recursos para prevenção e mitigação de incêndios, inundações, variações térmicas e outras ameaças ambientais;
e. sistemas de circuito fechado de TV (CFTV);
f. sistemas para prevenção e detecção de intrusos.

18.3. O acesso físico às instalações restritas do CARTÓRIO 15 deve ser autorizado aos colaboradores apenas durante o horário de suas atividades funcionais. Qualquer acesso fora desse horário deve ser explicitamente autorizado pelo gestor responsável.

18.4. Os Centros de Processamento de Dados (CPDs) do CARTÓRIO 15 devem:

a. ser localizados em salas ou instalações dedicadas a essa finalidade;
b. estar protegidos contra intempéries naturais, problemas estruturais e ameaças humanas;
c. ser mantidos trancados, com acesso controlado e autorizado apenas a colaboradores do Departamento de TI, membros da Diretoria e fornecedores autorizados;
d. possuir controle de acesso físico adequado;
e. possuir recursos de tolerância a falhas provocadas pela interrupção de serviços essenciais como energia elétrica ou conectividade;
f. contar com recursos de climatização e controle de umidade apropriados conforme padrões de mercado;
g. contar com câmeras de segurança cobrindo acessos e área interna, com ponto e contraponto, conforme o necessário.

18.5. Documentos e mídias contendo informações confidenciais devem ser armazenados em cofres, armários ou gaveteiros trancados.

18.6. A impressão de informações confidenciais deve ser evitada e, quando necessária, os documentos impressos não devem ser deixados em impressoras, multifuncionais ou scanners sem supervisão.

19. Gestão de Vulnerabilidades

19.1. O CARTÓRIO 15 deve manter processo formal de gestão de vulnerabilidades que assegure:

a. identificação contínua de vulnerabilidades por meio de varreduras automatizadas, monitoramento de boletins de fornecedores e fontes de inteligência reconhecidas;
b. priorização baseada em criticidade técnica e em exposição efetiva dos ativos afetados;
c. atualização periódica de sistemas, aplicações e dispositivos, com aplicação tempestiva de correções de segurança;
d. registro formal, auditável e cronologicamente organizado de todas as providências adotadas, com indicação de responsável e data de conclusão.

19.2. Os prazos máximos e os critérios técnicos de tratamento de vulnerabilidades devem observar integralmente o disposto no Anexo II do Provimento 213, em especial o tratamento de vulnerabilidades críticas em prazo máximo regulatório, com adoção de medidas imediatas de contenção e correção emergencial, preferencialmente em até 72 (setenta e duas) horas, quando houver exploração ativa, risco iminente ou comprometimento relevante já identificado.

19.3. O CARTÓRIO 15 deve providenciar que sejam realizados testes de intrusão (*pentest*) ou metodologia tecnicamente equivalente ao menos a cada 2 (dois) anos e sempre que houver alteração relevante de infraestrutura, observado o Anexo II do Provimento 213, inclusive quanto às hipóteses de validação coletiva e dispensa condicionada para serventias que operem integralmente em ambiente SaaS de fornecedor cuja segurança seja demonstrada por relatório técnico coletivo equivalente.

19.4. Os registros de gestão de vulnerabilidades, incluindo varreduras, pentests, achados, planos de correção e evidências de encerramento, devem ser arquivados pelo prazo mínimo de 5 (cinco) anos.

20. Uso Seguro de Inteligência Artificial

20.1. O desenvolvimento, a implementação, a utilização e o monitoramento de sistemas, serviços, ferramentas e demais recursos de Inteligência Artificial (recursos de IA) pelo CARTÓRIO 15 deve ocorrer em conformidade com as diretrizes desta Política e dos documentos complementares aplicáveis, observando os objetivos da serventia, o processo de gestão de riscos e a classificação das informações tratadas.

20.2. Recursos de IA devem ser previamente homologados pelo Responsável TIC antes de serem implementados ou utilizados por qualquer colaborador.

20.3. A utilização de recursos de IA para tomada de decisão automatizada com efeitos sobre titulares de dados deve ser previamente autorizada pela Tabeliã, com avaliação prévia do DPO.

20.4. Os colaboradores que utilizem recursos de IA devem:

- **a.** revisar os conteúdos gerados (textos, análises, imagens e demais elementos) antes de utilizá-los em operações, sistemas, serviços, documentos ou apresentações do CARTÓRIO 15;
- **b.** assegurar que os conteúdos gerados por recursos de IA contenham aviso claro e visível de que foram produzidos parcialmente por Inteligência Artificial.

20.5. Em razão da rápida evolução das tecnologias de IA, as diretrizes desta Política não esgotam todas as salvaguardas necessárias. Cada colaborador deve adotar medidas adicionais que considerar pertinentes para proteger as informações do CARTÓRIO 15 e assegurar o uso responsável e ético de IA – comunicando-as proativamente à Diretoria.

21. Resposta a Incidentes, Recuperação e Continuidade de Negócios

21.1. Esta Política estabelece as diretrizes estratégicas que fundamentam a elaboração e a manutenção do **Plano de Resposta a Incidentes e Continuidade de Negócios**, que contempla o tratamento tático-operacional integral dos esforços para resposta a incidentes, recuperação de desastres e continuidade de negócios, como documento complementar obrigatório que consolida as funções de Plano de Resposta a Incidentes, Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD). Consolidação esta admitida pelo Provimento 213 e pela ISO/IEC 27031:2025.

21.2. São processos críticos do CARTÓRIO 15, para fins de continuidade operacional, aqueles cuja interrupção comprometa diretamente a prestação dos serviços notariais, a integridade do acervo digital ou a observância de prazos legais. A identificação e a priorização desses processos são detalhadas no **Plano de Resposta a Incidentes e Continuidade de Negócios**, com base em análise de impacto no negócio.

21.3. O **Plano de Resposta a Incidentes e Continuidade de Negócios** deve definir os parâmetros de **Objetivo de Tempo de Recuperação (RTO)** e de **Objetivo de Ponto de Recuperação (RPO)** para os processos críticos, observando os requisitos mínimos aplicáveis à Classe 3 do Provimento 213. Estes parâmetros devem ser revistos a cada simulação anual de desastre e sempre que houver mudança relevante na arquitetura tecnológica, nos fornecedores críticos, na determinação regulatória ou no perfil de risco da serventia.

21.4. Adicionalmente, o **Plano de Resposta a Incidentes e Continuidade de Negócios** deve contemplar, no mínimo:

- **a.** procedimentos, papéis e prazos para detecção, classificação, contenção, erradicação e recuperação de incidentes de segurança cibernética;
- **b.** obrigações de comunicação à Corregedoria competente em até 72 (setenta e duas) horas nos casos críticos e de notificação à ANPD nos casos que envolvam dados pessoais;
- **c.** rotinas de cópias de segurança, incluindo frequência, retenção, meios de armazenamento, proteção das cópias e procedimentos periódicos de teste e verificação de integridade;
- **d.** planos de continuidade operacional para garantir a prestação dos serviços notariais essenciais durante e após eventos disruptivos;
- **e.** registro formal de análise de causa raiz e de lições aprendidas para todos os incidentes;
- **f.** a comunicação sobre incidentes (interna, à Corregedoria, à ANPD, aos titulares e a demais partes interessadas).

22. Privacidade e Proteção de Dados Pessoais

22.1. O CARTÓRIO 15 reconhece a Tabeliã como controladora de dados pessoais tratados pela serventia, nos termos da LGPD e do Provimento 213.

22.2. Todo tratamento de dados pessoais deve respeitar as bases legais previstas na LGPD, observando os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

22.3. O tratamento detalhado de todas as questões de privacidade e proteção de dados pessoais é definido na **Política de Privacidade** do CARTÓRIO 15, documento complementar obrigatório, mantido em razão da extensão e da criticidade do tema e da necessidade de publicização aos titulares.

23. Relações Internas

23.1. O CARTÓRIO 15 deve gerenciar riscos na seleção, contratação, manutenção e encerramento de vínculos com colaboradores.

23.2. O processo de seleção deve incluir verificação de identidade, qualificações, histórico funcional e referências profissionais.

23.3. Todo colaborador contratado deve assinar instrumento que contenha declarações de responsabilidade em segurança da informação, comprometimento com esta Política e demais normas internas, cláusulas de confidencialidade, de tratamento de dados pessoais e de propriedade intelectual.

23.4. Contas e recursos de TIC fornecidos pelo CARTÓRIO 15 devem ser utilizadas exclusivamente para fins funcionais, sendo expressamente vedada sua utilização para fins impróprios ou ilegais.

23.5. O CARTÓRIO 15 pode autorizar o uso de dispositivos próprios do colaborador (*BYOD – Bring Your Own Device*), desde que homologados pelo Departamento de TI conforme procedimento interno aprovado.

23.6. 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.

24. Relações com Fornecedores

24.1. A gestão de fornecedores deve observar os quatro subelementos do Anexo III, item 4.10, do Provimento 213:

- **a.** avaliação prévia de segurança;
- **b.** cláusulas contratuais de confidencialidade e segurança;
- **c.** definição clara de responsabilidades em caso de incidentes; e
- **d.** monitoramento contínuo do cumprimento contratual.

24.2. A avaliação prévia de segurança deve preceder toda contratação que envolva tratamento, armazenamento ou processamento de informações do CARTÓRIO 15, conforme procedimento interno aprovado.

24.3. Sempre que possível, deve ser evitada a dependência de fornecedores exclusivos.

24.4. Os contratos com fornecedores que envolvam tratamento, armazenamento ou processamento de informações do CARTÓRIO 15 devem conter cláusulas expressas e exequíveis que assegurem, no mínimo:

a. confidencialidade e não revelação de informações;
b. requisitos de segurança da informação e conformidade com a LGPD;
c. definição clara de responsabilidades em caso de incidentes, incluindo prazos de notificação ao CARTÓRIO 15;
d. acordo de nível de serviço (SLA) compatível com as obrigações da serventia;
e. reversibilidade integral da solução contratada;
f. portabilidade integral do acervo em formato interoperável e não proprietário, sem dependência de anuência discricionária do fornecedor para migração;
g. disponibilização de documentação técnica necessária à migração e cooperação ativa em caso de transição de fornecedor;
h. regras para retenção e descarte de informações durante e após o encerramento da contratação;
i. monitoramento contínuo do cumprimento das obrigações contratuais.

24.4. Para fornecedores que atuem como operadores ou corresponsáveis pelo tratamento de dados pessoais, os contratos devem contemplar adicionalmente:

a. registro de operações de tratamento de dados pessoais (ROPA) compartilhável;
b. acordo de processamento de dados (DPA);
c. relatório de impacto à proteção de dados (RIPD), quando aplicável.

24.5. A definição de responsabilidades em incidentes que envolvam fornecedores deve observar o **Plano de Resposta a Incidentes e Continuidade de Negócios**, em especial os fluxos de notificação recíproca, prazos e cooperação para contenção, erradicação, recuperação e comunicação às autoridades competentes.

24.6. O monitoramento contínuo do cumprimento contratual deve ser exercido e registrado no **Inventário de Sistemas, Serviços de TIC e Fornecedores**, com o nível de risco mapeado para cada fornecedor de TIC ativo.

24.7. Fornecedores críticos devem ser avaliados regularmente quanto à aderência aos acordos firmados, com registro formal das constatações e dos planos de ação aplicáveis.

24.8. Considera-se mitigada a dependência estrutural em relação a fornecedor quando houver, cumulativamente:

a. cláusula contratual que assegure reversibilidade e portabilidade em formato interoperável e não proprietário;
b. comprovação documental de teste de extração integral do acervo;
c. inexistência de restrição técnica ou contratual que impeça a migração sem anuência discricionária do fornecedor, conforme Art. 15 do Provimento 213.

24.9. Caso ocorra a utilização pelo CARTÓRIO 15 de soluções tecnológicas em ambiente compartilhado com outras serventias ou clientes do mesmo fornecedor, deve ser assegurada segregação lógica inequívoca de dados, bases, trilhas de auditoria, cópias de segurança e controles de acesso, por mecanismos técnicos que impeçam acesso, visualização, alteração ou extração indevida por terceiros.

25. Conscientização, Treinamentos e Comunicação Interna

25.1. O CARTÓRIO 15 deve assegurar a comunicação interna, a disponibilidade digital e os treinamentos sobre esta Política e as demais normas internas de segurança da informação e privacidade. A presente seção trata exclusivamente da comunicação interna da Política a colaboradores e terceiros, não se confundindo com a comunicação sobre incidentes (interna ou externa), regida integralmente pelo **Plano de Resposta a Incidentes e Continuidade de Negócios**.

25.2. A publicação e a divulgação interna desta Política deve observar:

a. comunicação formal a todos os colaboradores, estagiários e terceiros sob a forma de e-mail circular com aviso de leitura, ata de reunião de divulgação ou termo individual de ciência assinado;
b. disponibilização permanente em repositório interno acessível a todos os colaboradores;
c. reapresentação formal a cada nova versão aprovada e a cada novo colaborador, durante o processo de integração.

25.3. A conscientização e capacitação deve observar:

a. programa periódico de treinamentos, com frequência mínima anual, abrangendo segurança da informação, proteção de dados pessoais, defesa cibernética e procedimentos em caso de incidente;
b. uso de treinamentos ao vivo e gravados, testes de *phishing* simulados e demais iniciativas julgadas pertinentes;
c. registro formal de cada ação realizada, contendo data, tema, instrutor, lista de participantes e carga horária;
d. retenção dos registros de capacitação pelo prazo mínimo de 5 (cinco) anos.

26. Tratamento de Exceções e Processo Disciplinar

26.1. Exceções às diretrizes desta Política devem ser aprovadas pela Tabeliã, mediante registro formal das motivações, dos riscos residuais e das medidas compensatórias adotadas.

26.2. Toda não conformidade deve ser avaliada e tratada e todo desvio deve ser analisado para verificar se caracteriza incidente de segurança, conforme o **Plano de Resposta a Incidentes e Continuidade de Negócios**.

26.3. Violações desta Política, ainda que por omissão ou tentativa não consumada, são passíveis de penalidades conforme a **Política de Conduta** do CARTÓRIO 15.

26.4. Para terceiros, as sanções contratuais aplicáveis podem ser cumuladas.

26.5. Violações que configurem atividades ilegais sujeitam o infrator às medidas judiciais e indenizatórias pertinentes, sem prejuízo de processo criminal quando aplicável.

27. Melhoria Contínua

27.1. Esta Política deve ser objeto de revisão periódica documentada, com periodicidade mínima anual, e de revisão extraordinária obrigatória nas seguintes hipóteses:

- **a.** alteração legislativa ou regulatória relevante, em especial em matéria de proteção de dados pessoais ou de normas expedidas pelo Conselho Nacional de Justiça e pela Corregedoria competente;
- **b.** ocorrência de incidente de segurança significativo;
- **c.** mudança relevante na arquitetura tecnológica, em fornecedores críticos ou no perfil de risco da serventia;
- **d.** recomendação fundamentada decorrente de auditoria interna, fiscalização correicional ou avaliação independente.

27.2. Toda revisão deve ser registrada com indicação da versão, da data, do responsável pela revisão, síntese das alterações realizadas.

27.3. Todas as alterações e revisões devem ser formalmente aprovadas pela Tabeliã.

27.4. O desempenho dos controles de segurança da informação e privacidade deve ser medido, monitorado, analisado e avaliado periodicamente, com resultados documentados. A revisão crítica considera, entre outros fatores:

- **a.** resultados de avaliações de riscos e situação dos planos de tratamento;
- **b.** não conformidades identificadas e ações corretivas adotadas;
- **c.** mudanças no contexto interno, externo, legal ou regulatório aplicável ao CARTÓRIO 15;
- **d.** oportunidades de melhoria em estratégias, processos ou tecnologias de segurança.

27.5. Os registros auditáveis produzidos no âmbito desta Política devem ser mantidos pelo prazo mínimo de 5 (cinco) anos.

28. Documentos Complementares

28.1. Esta Política não esgota em si todos os instrumentos que direcionam e regulamentam os esforços de Segurança da Informação e Privacidade do CARTÓRIO 15 e pode ser complementada por outros documentos relacionados a temas específicos, sendo diretamente referenciados em seu texto os seguintes instrumentos:

a. Inventário de Sistemas, Serviços de TIC e Fornecedores;
b. Plano de Resposta a Incidentes e Continuidade de Negócios;
c. Política de Privacidade;
d. Política de Conduta;
e. Termos e Definições de Segurança da Informação e Privacidade.

28.2. Em caso de conflito entre as diretrizes desta Política e qualquer outro documento interno de segurança da informação e privacidade do CARTÓRIO 15, prevalece o estabelecido nesta Política, ressalvada disposição expressa em contrário aprovada pela Tabeliã.

29. Histórico de Alterações

Versão	Data	Responsáveis	Ações
1	26/05/2022	Rodrigo Lopes	▪ Elaboração inicial
1	22/06/2022	Matheus Alencar Sofia Martinelli	▪ Revisão de Privacidade e Proteção de Dados Pessoais ▪ Inclusão de questões específicas sobre o Cartório 15
1	27/07/2022	Alex Pereira	▪ Revisão geral
2	08/05/2024	Rodrigo Lopes	▪ Atualização e melhorias em relação à ISO/IEC 27001:2022; ▪ Inclusão de seções sobre ciclo de vida e classificação da informação, identidades e acessos, relações com fornecedores, entre outras.
2	02/08/2024	Paulo Camargo	▪ Revisão de *Compliance* e privacidade e proteção de dados.
2	02/09/2024	Alex Pereira	▪ Revisão geral
2	06/09/2024	Fernanda Leitão	▪ Revisão e Aprovação
3	15/05/2026	Paulo Camargo Rodrigo Lopes Alexa Pereira	▪ Adequação ao Provimento CNJ nº 213/2026. ▪ Simplificação e melhoria geral do texto.
3	22/05/2026	Fernanda Leitão	▪ Revisão e Aprovação

FERNANDA DE FREITAS LEITAO:96106441715
Assinado de forma digital por FERNANDA DE FREITAS LEITAO:96106441715 Dados: 2026.05.23 09:14:16 -03'00'