15° Cartório Ofício de Notas
Tabeliã: *Fernanda de Freitas Leitão*
Substituta Legal: *Michelle Novaes*

CARTÓRIO 15
Política de Segurança da Informação e Privacidade

Nome do documento	**Tipo de documento**	**Classificação**
CARTÓRIO 15 – Política de Segurança da Informação e Privacidade	Política	Interna
Criada por	**Data de criação**	**Versão**
Rodrigo Lopes (rodrigo@fwdcomputers.com)	26/05/2022	1
Revisada por	**Data de revisão**	**Revisão**
Matheus de Alencar (matheusdealencar@gussemsaad.com) Sofia Martinelli (sofiabmartinelli@gussemsaad.com) Alex Pereira (alexpereira@cartorio15.com.br)	27/07/2022	2
Aprovada por	**Data de aprovação**	**Prazo para revisão**
Fernanda de Freitas Leitão	**27/07/22**	Anual
Revisão anual		
Matheus de Alencar (matheusdealencar@gussemsaad.com)	**Data da revisão** **28/07/23**	

ÍNDICE

1. Declaração

1.1 Fundado em 1918, o CARTÓRIO 15º OFÍCIO DE NOTAS ("CARTÓRIO 15") está sob a delegação da Tabeliã Titular Fernanda de Freitas Leitão desde 1998 e 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. A informação acumulada ao longo de mais de um século de funcionamento é um ativo estratégico para o CARTÓRIO 15, sendo de inestimável valor os dados pessoais de todos os clientes, colaboradores, parceiros e fornecedores tratados em suas atividades de negócio.

1.2 Assim, consideramos que a correta gestão da informação, assegurando que ela 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, bem como por seus colaboradores, fornecedores, clientes e pelo público em geral.

1.3 Desta forma, o CARTÓRIO 15 estabelece esta Política de Segurança da Informação e Privacidade (doravante apenas referida como "Política") como parte de seu Sistema de Gestão Organizacional, alinhado às melhores práticas do mercado e às normas internacionalmente aceitas, com o objetivo de manter níveis adequados de segurança, que possam assegurar confidencialidade, integridade e disponibilidade das informações tratadas e sob sua responsabilidade.

2. Glossário

2.1 Visando o melhor entendimento de todos aqueles que devem tomar conhecimento desta Política, ficam estabelecidas aqui as definições para alguns termos básicos:

Termo / Conceito	Definição / Exemplo
Segurança da Informação	Aplicação de controles para proteção da confidencialidade, da integridade e da disponibilidade da informação em qualquer formato (físico ou digital) de acordo com sua relevância para o cumprimento dos objetivos de negócio e das responsabilidades legais do CARTÓRIO 15. Os esforços de Segurança da Informação do CARTÓRIO 15 são orientados pelas Normas Técnicas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e pelo NIST Cybersecurity Framework; sem prejuízo de outros modelos, controles e melhores práticas que possam ser consultados e considerados.

Segurança Cibernética	Aplicação de medidas técnicas com objetivo de proteger a informação armazenada por meio digital, incluindo servidores, computadores, smartphones, sistemas, e-mails, bancos de dados, estando estes armazenados localmente ou em nuvem.
Privacidade e Proteção de Dados Pessoais ("Privacidade")	Consiste no compromisso da organização com o direito fundamental à privacidade do indivíduo, traduzido na aplicação de medidas técnicas e administrativas para proteção de dados pessoais e sensíveis, no Brasil, conforme requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD). Os esforços de Privacidade e Proteção de Dados do CARTÓRIO 15 são orientados pela Norma Técnicas ABNT NBR ISO/IEC 27701:2019, além da própria LGPD; sem prejuízo de outros regulamentos, modelos, controles e melhores práticas que possam ser consultados e considerados.
Lei Geral de Proteção de Dados Pessoais ("LGPD")	Refere-se à Lei nº 13.709/2018, é a legislação brasileira federal que estabelece regras para tratamento de dados pessoais.
Dado	Parte sem significado da informação.
Informação	Dado colocado em um contexto, com significado. Também referenciada nesta Política como **ativo de informação**.
Ativo	Qualquer coisa (tangível ou intangível) com valor para a organização. **Exemplos de ativos tangíveis**: pessoas e suas competências, equipamentos, softwares e informações. **Exemplos de ativos intangíveis**: reputação e imagem da organização.
Confidencialidade	Característica atribuída a uma informação de acesso restrito aos indivíduos para os quais tal acesso seja necessário à execução de suas atividades funcionais e de negócio.
Integridade	Característica que preza que Ativos de Informação devem ser mantidos íntegros, válidos, livres de adulteração e não corrompidos.
Disponibilidade	Característica que preza que as Informações devem estar disponíveis para indivíduos e sistemas que delas precisem para cumprir com suas atividades e tarefas em nome dos objetivos de negócio da organização.
Autenticidade	Princípio adotado para a confirmação da identidade dos usuários antes que seja liberado a eles o acesso a sistemas, e-mails e recursos computacionais, como forma de minimizar os riscos de acessos e utilizações não autorizados. A autenticidade requer que a autorização de usuários, dispositivos, serviços, conexões seja validada para acessar, transmitir e receber determinadas Informações. Os mecanismos básicos para a autenticação são **logins e senhas**, mas também podem ser utilizados recursos como a autenticação biométrica ou a autenticação por meio de tokens. A combinação de 2 ou mais fatores de autenticação, por exemplo, senha e confirmação de um token no smartphone do usuário, é chamada de

	autenticação multifatorial (Multifactor Authentication, ou MFA na sigla em inglês).
Não Repúdio	Princípio que busca assegurar que uma pessoa ou entidade **não possa negar** a autoria de seus atos. Por exemplo: negar a utilização de uma informação fornecida, transações realizadas em um sistema de informação ou computador, acessos e transações realizadas na Internet etc. Na Gestão de Segurança da Informação, isso significa ser **capaz de provar** o que foi feito, por quem e quando foi feito, impossibilitando a negação das ações por parte de seus respectivos executores.
Vulnerabilidade	Ponto fraco de um Ativo ou Controle de segurança que possa ser explorado por uma ameaça e desta forma causar danos aos objetivos de negócio da organização
Ameaça	Causa potencial de um incidente indesejado, que possa resultar em danos a um ativo, sistema ou a uma organização.
Ameaças humanas intencionais	Ameaças que sejam causadas por comportamento humano doloso, no sentido de produzir a ameaça direta ou indiretamente. Exemplos: extravio de informações, ataque hacker, roubo etc.
Ameaças humanas não intencionais	Ameaças que sejam causadas por comportamento humano decorrente de culpa, negligência, imprudência ou imperícia. Pen drive infectado, usuário clica em um link malicioso por acidente, perda de um laptop ou smartphone etc.
Ameaças não humanas	Ameaça não associada a um comportamento humano. Exemplos: incêndio, inundação, falha no ar-condicionado, queda de energia etc.
Risco	Potencial que uma Ameaça tem de explorar Vulnerabilidades de um Ativo ou grupo de Ativos e, desta forma, causar danos à organização. Os riscos devem ser analisados segundo sua probabilidade (ocorrência) X consequência (impacto).
Controle	Medida Administrativa, Técnica ou Física integrada aos processos da organização com objetivo de mitigar Riscos. Tais como políticas, processos, sistemas de segurança, práticas etc.
Incidente	Evento indesejável e/ou inesperado que pode comprometer os objetivos de negócio explorando um Risco à Confidencialidade, Integridade ou Disponibilidade das Informações.
Medidas físicas	Exemplos: crachás para identificação colaboradores de visitantes, geradores e sistemas para alimentação ininterrupta de energia (UPS), extintores de incêndio, câmeras de segurança, controle de acesso, trituradores de papel etc.
Medidas técnicas	Exemplos: controle de identidades, autenticação multifatorial (MFA), soluções antimalware, backup, criptografia, firewall, sistemas para detecção de intrusos, sistemas para recuperação de desastres, sistemas para

	prevenção contra extravio e perda de dados, atualização e correção de sistemas etc.
Medidas administrativas	Exemplos: Política de Segurança da Informação e Privacidade, inventário de ativos, programa de treinamento e capacitação de colaboradores, seguros de responsabilidade empresarial e contra danos cibernéticas, termos de confidencialidade etc.
Dado Confidencial	Qualquer Dado ou Informação sobre o qual recai Confidencialidade e, portanto, cuja revelação deva ser controlada e seu acesso restrito a pessoas prévia e explicitamente autorizadas, que precisem conhecê-lo para execução de suas funções.
Dado Pessoal	Informação relacionada à pessoa natural identificada ou identificável. **Exemplos:** nome, sobrenome, data de nascimento, CPF, RG, CNH, sexo, endereço, e-mail, telefone etc.
Dado Pessoal Sensível (“Dado Sensível”)	Informações de caráter íntimo, muito pessoal e que podem levar a discriminação do indivíduo. **Exemplos:** dados sobre a saúde (prontuários, exames, laudos cirúrgicos etc.) genéticos, biométricos, referentes a origem racial ou étnica, convicção religiosa ou política e referentes a vida sexual.
Dado Pseudo-anonimizado	Dados que estão aparentemente anonimizados, mas podem identificar o titular caso alguma informação seja complementada. **Exemplos:** informações que combinadas possam levar à identificação do indivíduo.
Pseudo-anonimização	Conjunto de técnicas empregadas para converter um Dado Pessoal em Dado Pseudo-anonimizado.
Dado Anonimizado	Qualquer dado relacionado a um indivíduo, mas que não possa identificá-lo. **Exemplo:** dados expostos genericamente em uma pesquisa.
Anonimização	Conjunto de técnicas empregadas para converter um Dado Pessoal em Dado Anonimizado.
Titular dos Dados (“Titular”)	Pessoa física (natural) a quem pertencem os Dados Pessoais.
Tratamento de Dados (“Tratamento”)	Toda e qualquer operação realizada com um Dado Pessoal, incluindo acesso, coleta, produção, recepção, classificação, utilização, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, modificação, comunicação, transferência etc.
Agentes de Tratamento	Pessoas físicas ou jurídicas, de direito público ou privado, que realizam Tratamento de Dados Pessoais.
Controlador	Agente de Tratamento que toma decisões referente ao Tratamento dos Dados Pessoais. O CARTÓRIO 15 é Controlador dos Dados Pessoais dos clientes atendidos pelo cartório (por exemplo, Dados Pessoais fornecidos para celebração de uma procuração), bem como de seus funcionários (por exemplo, Dados Pessoais coletados para realização de pagamentos e benefícios).

Operador	Agente de Tratamento que efetivamente trata os Dados Pessoais, de acordo com a orientação do Controlador. **Exemplo:** O sistema MobiRio é operador de dados do CARTÓRIO 15.
Encarregado de Dados ou Data Protection Officer ("DPO")	Pessoa física ou jurídica pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, inclusive comunicando incidentes.
Autoridade Nacional de Proteção de Dados ("ANPD")	Autarquia federal, independente e autônoma, criada com o objetivo elaborar diretrizes nacionais para proteção de Dados Pessoais, bem como elaborar regulamentações e estudos complementares, fiscalizar o cumprimento da LGPD e punir infrações.
Plano de Comunicação, Conscientização e Treinamento em Segurança da Informação e Privacidade	Estabelece a estratégia do CARTÓRIO 15 para garantir que todos os colaboradores estejam conscientes de suas responsabilidades, bem como dos processos, tecnologias e ferramentas com os quais contam para que possam contribuir na missão do CARTÓRIO 15 em assegurar a Confidencialidade, Integridade e Disponibilidade dos Dados Confidenciais, Pessoais e Sensíveis tratados pelo ou em nome do CARTÓRIO 15.
Plano de Continuidade dos Negócios	Controle que tem como objetivo assegurar a continuidade dos serviços de TI e das linhas de atendimento aos clientes nos casos de incidentes de Segurança da Informação e Privacidade.

3. Escopo e objetivos

3.1. Todos os empregados, funcionários, colaboradores, gestores e administradores do CARTÓRIO 15 (referidos em conjunto como "Partes") tratam informações, seja de forma verbal, através de vários tipos de mídias físicas ou plataformas tecnológicas.

3.2. Assim, esta Política aplica-se a todas as Partes que exercem atividades junto ou em nome do CARTÓRIO 15, incluindo a tabeliã titular, tabeliões substitutos, escreventes, colaboradores, prestadores de serviço e parceiros de negócios em geral, assim como sistemas, softwares, comunicações e instalações contratadas ou pertencentes ao CARTÓRIO 15, e deve gerenciar o tratamento de Ativos de Informação durante todo o seu ciclo de vida.

3.3. Políticas de Segurança da Informação e Privacidade aqui incluem todos os processos, papéis, modelos, arquitetura da informação, políticas, termos, regras e regulamentos, os quais em conjunto com esta Política, possam ser considerados necessários para garantir que a informação seja tratada de forma a atender as necessidades e objetivos de negócio da organização.

3.4. Toda a Informação criada, coletada, armazenada, acessada, utilizada, modificada, compartilhada arquivada ou destruída por qualquer pessoa ou sistema em nome do CARTÓRIO 15 deve ser classificada, protegida e disponibilizada corretamente e com segurança.

3.5. Todos os Ativos – sejam eles pessoas, processos, tecnologias, sistemas ou informações – devem ser governados por um processo de gerenciamento de Riscos e estar sujeitos a implementação de controles que assegurem as melhores práticas de Segurança da Informação e Privacidade.

3.6. Todo Tratamento de Dados Pessoais pelo CARTÓRIO 15 deve respeitar as bases legais claramente previstas na Lei Geral de Proteção de Dados Pessoais, conforme os princípios de boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e prestação de contas.

3.7. Sempre que possível, o Tratamento de Dados Pessoais pelo CARTÓRIO 15 se norteará pelo emprego de técnicas de Anonimização e Pseudo-anonimização, com foco na prevenção de danos aos titulares.

3.8. Dessa forma, esta Política tem por objetivo proteger Dados Confidenciais ou Pessoais em qualquer forma, física ou digital. Para tal, Segurança da Informação e Privacidade devem estar integradas por padrão e no desenho de todos os processos, sistemas, documentos e relações, sendo assim vistas como estratégicas para o prestígio, relevância e crescimento do CARTÓRIO 15 no mercado em que atua.

4. Diretrizes e responsabilidades

Responsabilidades gerais

4.1 Em linha com seus objetivos, o CARTÓRIO 15 reitera seu compromisso com o cumprimento de suas obrigações legais e contratuais, uma responsabilidade aplicável ao CARTÓRIO 15 em sua coletividade e que deve ser compartilhada por todos aqueles direta ou indiretamente ligados a ele, ou que, por atuar em nome, também estejam sujeitos a essas obrigações na execução de suas tarefas e atividades profissionais.

4.2 Com objetivo de promover o alinhamento estratégico dos interesses do CARTÓRIO 15 com as melhores práticas de Segurança da Informação e Privacidade necessárias ao cumprimento dos objetivos e responsabilidades, fica decidida a formação do “Comitê Estratégico de Tecnologia e Segurança da Informação” (CETSI) com participação da Tabeliã Titular, da Substituta Legal, do Encarregado de Dados Pessoais, de um representante da Consultoria em Segurança da Informação, de um representante da Consultoria Jurídica, de um funcionário de Tecnologia da Informação vinculado ao CARTÓRIO 15 e de um consultor externo indicado pela Tabeliã Titular.

4.3 A comunicação sobre esta Política deve ocorrer de imediatamente após sua aprovação ou atualização, e nenhuma Parte deve ser considerada apta a exercer suas atividades em nome do CARTÓRIO 15 sem conhecimento e ciência formal de seu teor.

4.4 A comunicação deve ser feita de acordo com o Plano de Comunicação, Conscientização e Treinamento em Segurança da Informação e Privacidade e é de responsabilidade de todos os gestores junto a suas respectivas equipes. Questionamentos e dúvidas devem ser prontamente endereçados ao CETSI.

4.5 A contratação de prestadores de serviços e fornecedores pelo CARTÓRIO 15 deverá ser feita mediante a celebração, pelo respectivo contratado, de um Termo de Confidencialidade compatível com os serviços que a serem realizados. Para fins de seleção de prestadores de serviços e fornecedores, todo e qualquer contratado deverá demonstrar que adota melhores práticas e medidas de segurança cabíveis no tratamento de Dados Confidenciais. No caso em que os prestadores de serviços e fornecedores contratados pelo CARTÓRIO 15 tenham acesso a Dados Pessoais, deverão demonstrar sua conformidade com a LGPD, permitindo, inclusive, ao CARTÓRIO 15 conduzir auditorias específicas, seja diretamente ou por empresa terceirizada contratada para esta finalidade.

4.6 Todos os prestadores de serviços e fornecedores contratados pelo CARTÓRIO 15 serão cientificados quanto à existência dessa Política, cabendo ao CETSI avaliar a necessidade de que recebam treinamento específico sobre esta Política como requisito para o exercício de suas atividades junto ao CARTÓRIO 15.

4.7 Todas as Partes do CARTÓRIO 15, independente de cargo ou função, além dos prestadores de serviços, parceiros de negócios e demais terceiros que tratam informações pertencentes ao CARTÓRIO 15 ou em seu nome, devem tomar ciência e assinar um Termo de Confidencialidade compatível com as informações às quais terão acesso, formalizando suas responsabilidades, inclusive após o encerramento do vínculo contratual com o CARTÓRIO 15.

4.8 Todos os colaboradores tratam Dados Confidenciais e/ou Pessoais em nome da CARTÓRIO 15 e lhes são concedidos recursos tecnológicos para o exercício das suas atividades, por exemplo: contas de e-mail, acesso a sistemas, computadores e smartphones, dentre outros (“Recursos”). Esta política estabelece regras gerais de uso dos Recursos e é complementada pelo Regulamento dos Meios de Tecnologia da Informação e Comunicação do CARTÓRIO 15, que contém a listagem de todos os Recursos concedidos e o detalhamento das condições associadas ao seu adequado manuseio.

4.9 Todos os Recursos disponibilizados pelo CARTÓRIO 15 devem ser utilizados com exclusividade para a execução de atividades funcionais, sendo expressamente proibida sua utilização para qualquer propósito impróprio ou ilegal, como armazenamento e transmissão de conteúdos de caráter discriminatório, ofensivo, difamatório, pornográfico e/ou de associado a pedofilia.

4.10 Todos os Recursos estão sujeitos a monitoramento contínuo e auditoria, na forma estipulada pelo Regulamento dos Meios de Tecnologia da Informação e Comunicação do CARTÓRIO 15. Portanto, desaconselhamos a utilização dos Recursos para manuseio, armazenamento ou comunicação de informações de caráter pessoal do próprio colaborador.

4.11 **TODOS OS COLABORADORES** são responsáveis por e assumem o dever de:

a. Conhecer integralmente o conteúdo desta Política e conduzir suas atividades de trabalho segundo as regras nela estabelecidas, bem como atuar em conformidade com outros documentos, políticas e termos específicos sobre segurança da informação que lhe venham a ser apresentados no contexto de suas atividades ou que sejam particulares de Ativos aos quais possuam acesso.

b. Assumir a Segurança da Informação e Privacidade como uma responsabilidade de todos na organização e, por isso, manter-se atento ao utilizar Ativos e tratar Informações pertencentes ao CARTÓRIO 15 ou ao fazê-los em nome do CARTÓRIO 15, observando as regras da organização estabelecidas nesta Política, bem como em outras políticas, termos específicos e boas práticas disseminadas.

c. Conhecer e cumprir, no exercício de suas atividades profissionais em nome do CARTÓRIO 15leis, as normas que regulamentam aspectos como Privacidade e Proteção de Dados Pessoais e Propriedade Intelectual.

d. Conhecer e aplicar em sua rotina de trabalho as regras para classificação, rotulagem, manuseio e descarte de Ativos de Informação, conforme estabelecido na Política de Ciclo de Vida e Classificação da Informação.

e. Tratar informações pertencentes a, ou em nome do CARTÓRIO 15 preferencialmente através de dispositivos, e-mails e sistemas fornecidos para esta finalidade, exceto quando autorizados formal e explicitamente a proceder de maneira diferente, na forma do Regulamento dos Meios de Tecnologia da Informação e Comunicação do CARTÓRIO 15.

f. Adotar senhas fortes para que suas contas de acesso para e-mails, sistemas e estações de trabalho sejam mantidas seguras, não compartilhar suas senhas em nenhuma hipótese, e utilizar autenticação multifatorial (MFA) sempre que este recurso estiver disponível.

g. Cumprir com os treinamentos de conscientização em Segurança da Informação e Privacidade promovidos pelo CARTÓRIO 15 (por exemplo, treinamento sobre LGPD e treinamento sobre defesa cibernética pessoal) e seguir recomendações estabelecidas sobre o tratamento de Dados Pessoais ou Sensíveis de clientes, colaboradores, parceiros e fornecedores

h. Zelar pelo uso apropriado de equipamentos e recursos tecnológicos fornecidos pelo CARTÓRIO 15 (por exemplo, não abrir e-mails, SMS ou outro tipo de mensagem de procedência ou com assuntos duvidosos, tais como: solicitações cadastrais por parte de bancos, Receita Federal, Tribunal de Justiça e Serasa) e reportar, de imediato, através dos canais previamente aprovados pelo CARTÓRIO 15, qualquer problema, suspeita ou solicitação relacionados à Segurança da Informação e Privacidade, por exemplo, suspeitas de ataques

cibernéticos, vazamento de dados ou comportamento suspeito em seus computadores, smartphones, sistemas, e-mails e arquivos, ou de outro colaborador.

i. Consultar o Encarregado de Dados (DPO) sempre que houver dúvidas sobre riscos advindos de um determinado tratamento de Dados Pessoais ou Sensíveis.

j. Armazenar seus documentos em diretórios pré-determinados, conforme as regras de governança de dados da organização para que sejam realizados os devidos backups e procedimentos de alta disponibilidade.

k. Adotar medidas cabíveis para proteger as informações do CARTÓRIO 15 - em formato físico ou digital - contra acesso, modificação, destruição ou divulgação não autorizados.

Responsabilidades da Tabeliã Titular

4.12 A **TABELIÃ TITULAR,** sem prejuízo dos deveres impostos a todos os colaboradores, é responsável por:

a. Liderar o tratamento da temática de Segurança da Informação e Privacidade como um todo no CARTÓRIO 15, alinhando-a aos objetivos e às atividades de negócio da organização.

b. Assegurar que o CARTÓRIO 15 conte com recursos humanos e financeiros para endereçar assuntos relacionados à Segurança da Informação e Privacidade.

c. Liderar a comunicação sobre a importância da temática de Segurança da Informação e Privacidade para o CARTÓRIO 15.

Responsabilidades do CETSI

4.13 O **CETSI,** sem prejuízo dos deveres impostos a todos os colaboradores, é responsável por:

a. Conduzir o tratamento da temática de Segurança da Informação e Privacidade no CARTÓRIO 15.

b. Elaborar, revisar e aprovar orçamentos compatíveis com as necessidades do CARTÓRIO 15 nas questões de Segurança da Informação e Privacidade.

c. Zelar pelo alinhamento desta Política de Segurança da Informação e Privacidade aos objetivos de negócio estratégicos do CARTÓRIO 15.

d. Coordenar o Sistema de Gestão de Riscos em Segurança da Informação e Privacidade do CARTÓRIO 15, responsabilizando-se pela definição de critérios para classificação e aceitação de riscos.

e. Coordenar a realização periódica anual de avaliações de Riscos em Segurança da Informação e Privacidade e a aplicação de controles cabíveis para mitigar a probabilidade e o impacto dos Riscos encontrados, como parte do plano de tratamento de Riscos estabelecido e atualizado com base nos critérios para classificação e aceitação de riscos do CARTÓRIO 15. A periodicidade das avaliações poderá ser inferior se houver alguma mudança regulamentar de alto impacto para a atividade da instituição ou se algum novo Risco antes desconhecido for descoberto.

f. Coordenar os esforços de comunicação e conscientização sobre Segurança da Informação e Privacidade, assegurando ao Marketing os recursos necessários para comunicar não apenas esta Política, mas também processos, papéis, modelos, arquitetura da informação, políticas, termos, guias, regras e regulamentos relacionados ao tema da segurança da informação.

g. Monitorar, medir a eficácia e revisar controles, avaliações e planos implementados referentes ao tratamento de Riscos do CARTÓRIO 15, com objetivo de eliminar não-conformidades e continuamente melhorar a pertinência, adequação e eficácia do Sistema de Gestão de Segurança da Informação e Privacidade da organização.

h. Atribuir os papéis e responsabilidades relacionados à Segurança da Informação e Privacidade.

i. Apontar o Encarregado de Dados (DPO) do CARTÓRIO 15 e assegurar que ele possua autonomia e recursos tecnológicos e humanos para o exercício de suas funções.

j. Analisar criticamente as medidas aqui estabelecidas para que estas sejam mantidas de forma proporcional e relevante aos objetivos de negócio da CARTÓRIO 15 e aos requisitos legais e contratuais impostos à organização.

k. Coordenar a revisão anual desta Política, envolvendo equipes e colaboradores e fazendo uso de aconselhamento especializado sempre que considerá-lo necessário.

l. Coordenar a elaboração e revisão do Plano de Continuidade de Negócios do CARTÓRIO 15, controle necessário para assegurar a máxima resiliência da organização em caso incidentes de Segurança da Informação e Privacidade, como um ataque cibernético ou vazamento de dados pessoais.

Responsabilidades de Gestores e Líderes de Departamentos

4.14 Os **GESTORES/LÍDERES DE DEPARTAMENTOS,** sem prejuízo dos deveres impostos a todos os colaboradores, são responsáveis por:

a. Estar cientes e informar ao CETSI sobre questões relativas à Segurança da Informação e Privacidade que impactem as atividades e processos de seu respectivo departamento.

b. Assegurar que nenhum colaborador em seu departamento exerça suas funções e atividades sem o conhecimento quanto à existência e conteúdo desta Política.

c. Responder, quando for de seu conhecimento, às dúvidas apresentadas por colaboradores de seus respectivos departamentos ou encaminhá-las ao CETSI nos casos em que não se considerarem aptos a respondê-las.

d. Notificar o CETSI de imediato sobre qualquer comportamento suspeito relacionado à Segurança da Informação e Privacidade por parte de um colaborador de seu departamento.

e. Seguir as instruções do CETSI e do Gestor de Recursos Humanos sobre processos disciplinares que devam ser aplicados aos colaboradores de seu departamento.

f. Não contratar ou utilizar, nem permitir que sejam contratados ou utilizados, sistemas, softwares ou aplicações que não tenham sido previamente aprovados pelo Departamento de TI do CARTÓRIO 15, prática classificada popularmente como “Shadow IT”.

Responsabilidades do Responsável por Tecnologia da Informação (TI)

4.15 A **TI**, sem prejuízo dos deveres impostos a todos os colaboradores, é responsável por:

- **a.** Coordenar os esforços para que o CARTÓRIO 15 possua medidas de segurança cibernéticas – Medidas Técnicas de Segurança da Informação e Privacidade - capazes de proteger os Dados Confidenciais e Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação indevida ou qualquer outro tratamento inadequado ou ilícito.
- **b.** Aconselhar o CETSI e o DPO sobre questões pertinentes a Tecnologia da Informação e Segurança Cibernética que possam impactar os esforços de Segurança da Informação e Privacidade do CARTÓRIO 15 no contexto de seus objetivos de negócio, fornecendo, sempre que necessário, apoio técnico ao cumprimento de obrigações regulatórias, por exemplo, o atendimento a solicitações da ANPD ou de Titulares.
- **c.** Elaborar e manter atualizados políticas e termos de uso de recursos tecnológicos da organização, tais como sistemas, e-mails e equipamentos.
- **d.** Assegurar que o CARTÓRIO 15 conte, através de colaboradores ou prestadores de serviços especializados, com todas as competências para implementar e manter os recursos tecnológicos dentro dos critérios previstos para aceitação de Riscos, conforme definido critérios estabelecidos para riscos em Segurança da Informação e Privacidade.
- **e.** Recomendar tecnologias e ferramentas que possam ser relevantes para os esforços de Segurança da Informação e Privacidade do CARTÓRIO 15, observando os requisitos do negócio, tendências de mercado e recomendações de especialistas externos.
- **f.** Observar as regras estabelecidas nesta Política, bem como as melhores práticas de mercado para gestão de Ativos de Tecnologia da Informação, com objetivo de assegurar a proteção da Informação conforme as regras de classificação enumeradas na Política de Ciclo de Vida e Classificação da Informação, em todo o seu ciclo de vida.
- **g.** Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos dos usuários.
- **h.** Manter registro e controle atualizados de todas as liberações de acesso concedidas, procedendo, sempre que necessário, com a pronta suspensão ou alteração de tais liberações.
- **i.** Elaborar e manter um plano eficiente e eficaz de gestão de mudanças para os Ativos de informação do CARTÓRIO 15 com objetivo de evitar falhas advindas de softwares desatualizados ou equipamentos obsoletos.

Responsabilidades do Gestor de Recursos Humanos (RH)

4.16 O **RH**, sem prejuízo das reponsabilidades gerais que recaem sobre todos os colaboradores e daquelas atribuídas a gestores de departamento, é responsável por:

- **a.** Realizar a devida diligência com objetivo de assegurar que os responsáveis por funções ligadas a Segurança da Informação e Privacidade possuam competência – baseada em educação, treinamento e experiência - compatível com o exercício de suas atividades.

b. Realizar, na condução de qualquer processo seletivo, uma verificação de antecedentes dos candidatos ("background check") proporcional às atividades que vão desempenhar, com objetivo de mitigar riscos relacionados aos acessos que estes terão a informações confidenciais e pessoais tratadas pelo CARTÓRIO 15.

c. Assegurar que colaboradores não exerçam suas funções sem o devido conhecimento desta Política e demais instrumentos relacionados ao tema da segurança da informação, coletando por escrito sua ciência, quando cabível.

d. Formalizar ao Departamento de Tecnologia da Informação a realização de contratações, promoções, mudanças de atividade em toda a organização, com objetivo de assegurar que cada colaborador possua sempre apenas o acesso necessário pelo tempo necessário para o exercício de suas funções.

e. Salvo nos casos de dispensa com efeitos imediatos, formalizar ao Departamento de Tecnologia da Informação, com antecedência não inferior a 24 horas, sobre o desligamento de colaboradores, para que acessos aos sistemas e recursos tecnológicos por eles utilizados sejam desativados/excluídos.

f. Respeitar as bases legais mapeadas pela assessoria jurídica especializada para o tratamento de dados pessoais de colaboradores contratados, conforme estabelecido pela LGPD.

Responsabilidades do Encarregado de Dados (DPO)

4.17 O **DPO**, sem prejuízo dos deveres impostos a todos os colaboradores, é responsável por:

a. Manter seus conhecimentos relevantes e atualizados sobre: (i) a LGPD, (ii) melhores práticas e modelos de Segurança da Informação e Privacidade, (iii) Legislações que impactem a regulação sobre Proteção de Dados Pessoais nos negócios operados pelo CARTÓRIO 15, (iv) aspectos que possam impactar direitos e liberdades dos Titulares de dados na operação do CARTÓRIO 15.

b. Agir com autonomia quanto à proteção dos interesses dos titulares de dados tratados pelo CARTÓRIO 15 e comunicar de maneira formal ao CETSI sempre que, por qualquer razão, perceber cerceada tal autonomia.

c. Monitorar se as regras internas de Privacidade e Proteção de Dados e as obrigações previstas na LGPD estão sendo observadas por colaboradores, gestores e terceiros e demais partes interessadas, durante o Tratamento de Dados Pessoais pelo ou em nome do CARTÓRIO 15.

d. Mensurar o esforço e a efetividade do Programa de Privacidade do CARTÓRIO 15, com o auxílio da equipe multidisciplinar de apoio ao Encarregado e por meio de indicadores próprios, avaliações periódicas e acompanhamento de canais de denúncia estabelecidos para atender às requisições dos titulares de dados.

e. Atuar como ponto de contato entre o CARTÓRIO 15 e a ANPD, comprometendo-se a assegurar que o CARTÓRIO 15 responda às requisições ou medidas necessárias, também buscando orientações proativamente sempre que considerar pertinente.

f. Atuar como ponto de contato entre o CARTÓRIO 15 e Titulares de Dados, assegurando que as requisições destes sejam atendidas dentro do prazo legal e da melhor forma possível.

g. Atuar como disseminador da cultura de Privacidade e Proteção de Dados no CARTÓRIO 15, prestando aconselhamento sobre melhores práticas e avaliando o impacto de decisões e operações cotidianas quanto ao Tratamento de Dados Pessoais.

h. Avaliar e aconselhar sobre a necessidade de realizar ou atualizar um relatório de impacto a Proteção de Dados em relação a alguma atividade desempenhada pelo CARTÓRIO 15.

i. Prover aconselhamento ao CETSI e aos Gestores de Departamento sobre questões relacionadas à Privacidade e Proteção de Dados e sobre a LGPD como um todo.

j. Informar o CETSI sobre a necessidade de buscar aconselhamento jurídico ou em segurança da informação e cibernética sempre que considerar necessário para a realização de suas atividades, tendo em vista os interesses e objetivos de negócio do CARTÓRIO 15.

4.18 As violações, mesmo que por mera omissão ou tentativa não consumada, desta Política, bem como demais normas e procedimentos de Segurança da Informação e Privacidade, serão passíveis de penalidades previstas no Código de Ética e Políticas de Conduta 15º Ofício de Notas do Rio de Janeiro, disponível no link http://cartorio15.com.br/, são elas: advertência, recomendação de suspensão, rescisão contratual, demissões, desligamento, sem prejuízo das sanções cíveis e criminais cabíveis a serem apuradas em processo judicial.

4.19 A aplicação das sanções será feita de maneira proporcional à gravidade e ao efeito da infração, sua recorrência, de acordo com as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, e seguirá o Protocolo de Processamento Interno e Mecanismos Sancionatórios previsto pelo Código de Ética e Políticas de Conduta.

4.20 No caso de terceiros contratados ou prestadores de serviço, as sanções previstas pelo Código de Ética e Políticas de Conduta poderão ser cumuladas com sanções e punições previstas em contrato, bem como sobre ações judiciais cabíveis.

4.21 Em 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 pertinentes, e sem prejuízo das demais sanções previstas nesta Política.

4.22 As diretrizes estabelecidas nesta Política e demais normas e procedimentos adotados pelo CARTÓRIO 15 não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Assim, os exemplos de medidas, procedimentos e protocolos de segurança da informação ora utilizados não representam um rol taxativo, cabendo ao usuário da Informação adotar, além daquelas aqui previstas, outras medidas que considerar necessárias para proteger as informações do CARTÓRIO 15, mediante comunicação proativa sobre tais medidas ao CETSI.

5. Políticas, normas, termos e procedimentos internos complementares

5.1 Esta Política não esgota em si todos os instrumentos que direcionam e regulamentam o tratamento de informações no CARTÓRIO 15, embora seja o principal documento de referência para questões de Segurança da Informação e Privacidade na organização.

5.2 Documentos que compõem os esforços de Segurança da Informação e Privacidade do CARTÓRIO 15, sem prejuízo de outras políticas, termos e normas não especificadas aqui, são:

- **a.** Relatório de Avaliação e Plano de Tratamento de Riscos em Segurança da Informação e Privacidade
- **b.** Política de Ciclo de Vida e Classificação da Informação
- **c.** Política de Privacidade
- **d.** Regulamento dos Meios de Tecnologia da Informação e Comunicação
- **e.** Termos de Confidencialidade e Não Divulgação
- **f.** Plano de Resposta a Incidentes
- **g.** Plano para Recuperação de Desastres
- **h.** Plano para Continuidade de Negócios

5.3 Caso haja conflito entre diretrizes estabelecidas nesta Política e qualquer outra política interna, termo ou documento, deve prevalecer o que está determinado nesta Política.

6. Melhoria contínua

6.1 O conteúdo desta Política apenas poderá ser modificado por deliberação do CETSI do CARTÓRIO 15 e deverá ser revisado anualmente ou em menor prazo, sempre que necessário. O CETSI deve monitorar, medir, analisar e avaliar o desempenho quanto a segurança da informação como um todo e a eficácia do Sistema de Gestão de Segurança da Informação e Privacidade especificamente, levando em conta o que precisa ser monitorado, método que deve ser aplicado para o monitoramento, quando os resultados devem ser analisados e quem deve analisar e avaliar estes resultados. Mantendo toda a documentação relativa ao processo de monitoramento.

6.2 O CETSI deve coordenar a revisão e atualização desta Política, bem como demais políticas, normas, termos, procedimentos e processos pertinentes à Segurança da Informação e Privacidade do CARTÓRIO 15 sempre que considerar necessário, não excedendo a periodicidade máxima de 12 (doze) meses.

6.3 O CETSI deve planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos e resultados de auditorias anteriores.

6.4 O CETSI deve analisar criticamente e buscar melhorar continuamente a pertinência das regras estabelecidas pelo Sistema de Gestão de Segurança da Informação e Privacidade, bem como seu alinhamento contínuo aos objetivos de negócio do CARTÓRIO 15, 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 da organização.
d. Mudanças em legislações vigentes aplicáveis a organização.
e. Resultados da avaliação de riscos e situação plano de tratamento de riscos.
f. Resultados de auditorias e seus comentários.
g. Não conformidades e ações corretivas aplicadas.
h. Técnicas, produtos ou processos que possam melhorar o desempenho do Sistema de Gestão de Segurança da Informação e Privacidade da organização.

7. Controle de Versões e Revisões

Versão/Revisão	Data	Responsáveis	Ações
1.0 (versão 1)	26/05/2022	Rodrigo Lopes	○ Criação da Política de Segurança da Informação e Privacidade (PSIP).
1.1 (versão 1, revisão 1)	22/06/2022	Matheus de Alencar Sofia Martinelli Rodrigo Lopes	○ Ajustes gerais em toda a PSIP quanto a especificidades do Cartório 15. ○ Definições sobre o CETSI ○ Ajustes de responsabilidades ○ Melhorias de redação em geral
1.2 (versão 1, revisão 2)	27/07/2022	Alex Pereira	○ Inclusão do Link