

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONTROLE DE FLUXO DE DADOS.

Sumário

1. INTRODUÇÃO	2
2. OBJETIVOS.....	2
3. APLICAÇÃO	2
4. PRINCÍPIOS.....	2
5. DIRETRIZES GERAIS.....	3
6. PENALIDADES.....	6
7. PAPÉIS E RESPONSABILIDADES	6
7.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (CSI)	6
7.2. TECNOLOGIA DA INFORMAÇÃO (TI)	7
7.3. ENCARREGADO NOMEADO.....	7
7.4. USUÁRIOS	7
7.5. RECURSOS HUMANOS	8
8. GESTÃO DA POLÍTICA.....	8

1. INTRODUÇÃO

O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ entende que a informação é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus clientes.

O cartório compreende que a manipulação da informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas e privacidade de dados pessoais, seja de clientes ou funcionários.

Dessa forma, o RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações do cartório ou sob sua responsabilidade.

2. OBJETIVOS

Declarar formalmente, as diretrizes que visam à proteção dos ativos de informação e privacidade dos dados pessoais com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade. Assim como dos Ativos de Tecnologia de Informação e Comunicação que as sustentam, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio.

Estabelecer as competências, responsabilidades e limites de atuação dos colaboradores do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, em relação à segurança da informação e privacidade, reforçando a cultura de segurança e priorizando as ações necessárias conforme o negócio.

3. APLICAÇÃO

Esta Política de Segurança da Informação é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela é aplicada a todos os empregados, estagiários, menores aprendizes, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores, clientes, ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as Informações e os Ativos do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

4. PRINCÍPIOS

Preservar e proteger a informação em todo o seu ciclo de vida, contida em qualquer meio, suporte ou formato, por qualquer ativo de propriedade ou responsabilidade do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, dos diversos tipos de ameaça.

Prevenir e reduzir impactos gerados por incidentes de segurança, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais.

Estabelecer e definir as atribuições e responsabilidades do Comitê de Segurança da informação e privacidade visando alcançar os objetivos e estabelecer os controles definidos pelo RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

Assegurar que a Tecnologia da Informação realize a gestão e a segurança dos Ativos de propriedade do cartório ou dos que estão sob sua responsabilidade.

Estabelecer um plano anual de capacitação e conscientização direcionado ao desenvolvimento e manutenção das habilidades e aperfeiçoamento dos colaboradores sobre tecnologia e segurança da informação.

Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades profissionais no que diz respeito à segurança da informação e aos objetivos institucionais, morais e éticos.

5. DIRETRIZES GERAIS

Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

Publicidade: Esta PSI e seus documentos complementares serão divulgados aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com o RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, ou que, direta ou indiretamente, são impactados.

Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ e devem ser empregados unicamente para fins profissionais.

Propriedade Intelectual: É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto.

Classificação da Informação: Os colaboradores devem utilizar apenas os recursos disponibilizados pelo RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte.

Sigilo: É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, por seus colaboradores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja classificada como “pública”.

Uso dos Ativos: Os Ativos de propriedade do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

O colaborador deve utilizar apenas Ativos previamente homologados e autorizados pela TI, sejam eles onerosos, gratuitos, livres ou licenciados.

Manutenção dos Ativos: Todos os Ativos em uso no ambiente corporativo do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ devem atender as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.

Mobilidade: Os Ativos que permitem mais mobilidade ao colaborador devem ser utilizados somente quando fornecidos ou autorizados pelo RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições do colaborador.

Ativos Particulares: O uso de Ativos Particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve ocorrer somente após solicitação formal e fundamentada do colaborador solicitante e autorização expressa do seu gerente e da TI.

Repositórios digitais: É vedado aos colaboradores o uso de repositórios digitais não homologados pela TI para armazenar ou publicar informações de propriedade ou sob a responsabilidade do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, salvo casos em que a informação esteja classificada como “pública”.

Softwares de comunicação instantânea: É vedado aos colaboradores a instalação e o uso de softwares de comunicação instantânea não homologados pela TI nos Ativos do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

Mídias Sociais: A participação do colaborador nas mídias sociais por meio dos Ativos do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve ser realizada de acordo com controles estabelecidos em documento específico e estar relacionada às atividades profissionais.

O colaborador é responsável por sua conduta no uso das mídias sociais. Por isso, cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade, etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.

Controle de acesso: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ controla o acesso físico e lógico às suas dependências e aos seus Ativos. Desse modo, cada colaborador deve possuir um login e senha de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

O colaborador é responsável pelo uso e sigilo de suas credenciais de acesso, não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de logins e senha de terceiros. Sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

Ambientes Lógicos: Os sistemas e processos que suportam os Ativos do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

Ambientes Físicos: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve estabelecer perímetros de segurança para proteção de suas propriedades, bem como implementar controles de identificação e registro de acesso em suas dependências para assegurar o acesso somente de colaboradores autorizados e Ativos homologados.

Áudio, Vídeos e Fotos: É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ por seus colaboradores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico ou uso nas mídias sociais.

Contratação, Terceirização ou Prestação de Serviços: Os relacionamentos e contratações, inclusive de colaboradores, em que ocorra o compartilhamento de informações do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ ou a concessão de qualquer tipo de acesso aos seus ambientes e Ativos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da informação e privacidade.

Auditoria junto aos prestadores de serviço: Cláusulas contratuais que dispõem sobre a realização de auditorias eventuais ou periódicas para certificar a conformidade

com a PSI e seus documentos complementares devem ser estabelecidas junto aos prestadores de serviço do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

Desenvolvimento e aquisição de software: O desenvolvimento interno e/ou externo de softwares, assim como a aquisição de softwares e produtos no mercado, devem possuir requisitos de segurança para garantir informações confiáveis, íntegras, autênticas e oportunas.

Documentação: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus Ativos.

Salvaguarda (*backup*): O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve definir e manter um processo de salvaguarda e restauração das informações e de seus Ativos críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

Análise dos processos e Ativos: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve analisar, em intervalos regulares, seus processos e Ativos, visando assegurar que estes estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

Monitoramento: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, Ativos e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.

Inspeção dos Ativos: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, sempre que considerar necessário, pode auditar ou inspecionar os Ativos que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os Ativos de propriedade de terceiros, quando autorizada a entrada em suas dependências, independentemente da interação com seus ambientes e informações.

Gestão de Configuração e Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ devem preservar os controles relacionados à disponibilidade, integridade, sigilo e autenticidade das informações.

Continuidade do Negócio: No escopo das ações de Segurança da informação e privacidade, os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação e privacidade estabelecidos para proteção dos Ativos críticos.

Conformidade: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

Capacitação: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve possuir pessoas capacitadas para exercer a Conscientização em Segurança da informação e privacidade para capacitação e disseminação da cultura de Segurança da Informação, proteção de dados e privacidade junto aos seus colaboradores.

Investimentos: Os investimentos em Segurança da informação e privacidade no RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ devem ser estudados e

deliberados conjuntamente com o CSI, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

Comitê de Segurança da informação e privacidade (CSI): O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve manter um Comitê de Segurança da informação e privacidade (CSI), cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da informação e privacidade, além de avaliar os controles, violação de dados pessoais e incidentes relacionados.

Equipe de Resposta a Incidentes: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve manter uma Equipe de Resposta a Incidentes em Segurança da informação e privacidade, com composição fixa ou variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação.

Comunicação de Incidentes: O RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ deve possuir um canal de comunicação divulgado aos seus colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação e privacidade.

Alterações: As alterações desta PSI e de seus documentos complementares devem ser devidamente comunicadas aos seus colaboradores pelo RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

Exceções: As exceções que ocorram de forma exclusiva e excepcional a essa PSI, devem ser formalizadas e fundamentadas pelo colaborador solicitante, e podem ser revogadas a qualquer tempo, por mera liberalidade do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ.

As medidas alternativas às previstas nesta PSI, realizadas de modo excepcional para mitigar riscos em ocasiões específicas e justificáveis, inclusive em situações emergenciais, devem ser formalizadas e fundamentadas pelo colaborador de forma imediata ou assim que possível ao CSI.

Dúvidas: Qualquer dúvida relativa a esta PSI deve ser encaminhada ao CSI por meio do e-mail cartoriojardimprimavera@gmail.com.

6. PENALIDADES

Violações: Os incidentes de segurança da informação devem ser avaliados pelo Comitê de Segurança da Informação e Privacidade. Ao constatar uma violação, o CSI deverá avaliar o caso, podendo instaurar e apurar as responsabilidades dos envolvidos em procedimento administrativo disciplinar, visando aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, regimento pessoal e outros documentos normativos do RCPN e Tabelionato do 2º Distrito de Duque de Caxias - RJ, além da legislação vigente.

6.1.2. Verificada a ocorrência de incidente com dados pessoais, o CSI comunicará ao encarregado para que promova a comunicação ao controlador.

Tentativa de Burla: A tentativa de burlar às diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

7. PAPÉIS E RESPONSABILIDADES

Comitê de Segurança da Informação e Privacidade (CSI)

Analisar, revisar e propor políticas e normas relacionadas à segurança da informação, privacidade e proteção de dados;

Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação e privacidade;

Garantir que as atividades de segurança da informação, privacidade e proteção de dados, sejam executadas em conformidade com a PSI;

Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do cartório.

Tecnologia da Informação (TI)

Conduzir a Gestão e Operação da segurança da informação, privacidade e proteção de dados, tendo como base esta política e demais resoluções do CSI;

Apoiar o CSI em suas deliberações;

Elaborar e propor ao CSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PSI;

Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

Tomar as ações cabíveis para se fazer cumprir os termos desta política;

Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

Encarregado nomeado.

Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo cartório;

Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo cartório;

Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo cartório.

Adotar as medidas cabíveis nos casos de incidência e segurança.

Receber reclamações e sugestões e prestar informações aos usuários.

Atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Usuários

Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos a TI ou, quando pertinente, ao CSI;

Comunicar à TI qualquer evento que viole esta Política, coloque ou possa vir a colocar em risco a segurança das informações e privacidade do cartório;

Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

Recursos Humanos

Apoiar o CSI na elaboração de campanhas de conscientização e materiais de divulgação e alerta em segurança da informação e privacidade;

Estipular controles de segurança e proteção de dados especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões);

Comunicar à TI o desligamento dos colaboradores e término de contratações, para que os acessos destes sejam desativados;

Realizar a guardar o documento na pasta funcional do colaborador;

Disponibilizar e realizar a gestão das credenciais individuais de acesso ao ambiente físico do cartório;

8. Gestão da Política

A Política de Segurança da Informação é aprovada pelo Comitê de Segurança da Informação, em conjunto com o Notário e Registrador do cartório.