# PORTARIA INTERNA Nº 06/2022 DE 4 DE OUTUBRO DE 2022

***"Dispõe sobre a Política de Segurança de Informação – PSI do Tabelionato do Segundo Ofício de Notas de Ipatinga/MG"***

O TABELIÃO DO SEGUNDO OFÍCIO DE NOTAS DE IPATINGA/MG, Bel., M.Sc., LL.M., BERNARDO PRADO DA CAMARA, usando das atribuições legais que lhe são pertinentes:

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação – PSI no âmbito do Segundo Tabelionato de Notas de Ipatinga/MG - Cartório.

**CAPÍTULO I DO ESCOPO**

Art. 2º A PSI tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, sistemas, documentos, correspondências e publicações, bem como seus repositórios ou meios de armazenamento, reconhecidamente necessários à prestação dos serviços executados pelo Cartório, contra ameaças que possam comprometer seus ativos ou sua imagem institucional.

§1º As diretrizes estabelecidas nesta política devem estar alinhadas a eventual Planejamento Estratégico, ao Código de Ética do Cartório, à Política Interna de Proteção de Dados e em consonância com os valores institucionais.

§2º Os colaboradores, usuários, fornecedores, prestadores de serviço e agentes de fiscalização devem observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta PSI.

§3º Integram também a PSI as normas e os procedimentos complementares, inclusive aqueles previstos no Provimento 93/CGJ TJMG, Provimentos 50, 88 e 134 do CNJ, IN 1111 RFB, dentre outros, destinados à proteção da informação e à disciplina de sua utilização.

§4º A PSI trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos vitais do Cartório, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como os valores éticos e as melhores práticas de Segurança da Informação – SI.

**CAPÍTULO II DOS CONCEITOS E DEFINIÇÕES**

Art. 3º No âmbito da PSI, serão consideradas as definições apresentadas na legislação e arcabouço jurídico aplicável ao tema:

**CAPÍTULO III DOS PRINCÍPIOS**

Art. 4º As ações relacionadas à SI no Cartório são norteadas pelos seguintes princípios:

I - Legalidade: a PSI levará em consideração as leis, as normas, instruções, procedimentos e as políticas administrativas, organizacionais, técnicas e operacionais formalmente estabelecidas e emanadas do Cartório;

II - Impessoalidade: a PSI visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais;

III - Moralidade: a elaboração da PSI, bem como sua posterior aplicação, deverá observar os preceitos da boa administração pública, pautando-se pela atuação ética e nos ideais de honestidade e justiça;

IV - Publicidade: as diretrizes, normas e procedimentos da PSI definidos pelo Cartório devem ser publicados e amplamente divulgados para o balizamento dos agentes públicos no pleno desempenho de suas atribuições;

V - Responsabilidade: a PSI deverá ser seguida pelos agentes públicos no exercício de suas atividades, pautando-se por atitudes e comportamentos condizentes com as diretrizes, normas e procedimentos de SI;

VI - Proporcionalidade: a aplicação da PSI, no que abrange o nível, a complexidade e o custo das ações deverá ser adequada ao entendimento administrativo e aos valores dos ativos a serem protegidos; e

VII - Privacidade: os dados pessoais de pessoas naturais, quando tratados pelo Cartório no âmbito de suas atividades, devem estar consoantes com o interesse público ou com o consentimento do titular para assegurar-lhe a inviolabilidade da intimidade, da honra e da imagem.

**CAPÍTULO IV DA ESTRUTURA E GESTÃO DA SI**

Art. 5º A PSI é proposta pelo Tabelião Titular do Segundo Tabelionato de Notas de Ipatinga/MG.

§1º Por iniciativa do Tabelião, grupos de trabalho podem ser formados para conceber, planejar ou realizar atividades específicas de SI.

§ 2º A recepção, a análise e o tratamento de eventos de SI será realizada pelos profissionais indicados pelo Tabelião e responsáveis pelo Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

**CAPÍTULO V DAS DIRETRIZES**

**Seção I - Das Diretrizes Gerais**

Art. 6º As informações criadas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas, realizadas no âmbito do Cartório, são patrimônio do mesmo, classificadas e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o seu ciclo de vida.

Parágrafo único. O uso das informações deverá ser feito apenas para o desempenho das atividades profissionais.

Art. 7º Todos os contratos celebrados pelo Cartório com prestadores de serviços ou fornecedores devem conter cláusulas que determinem a observância da PSI e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.

Art. 8º. Os prestadores de serviços sob contrato com o Cartório serão obrigados a assinar Termo de Aceitação, em obediência ao estabelecido na PSI.

**Seção II - Do uso de recursos de TI**

Art. 9º. Os recursos de tecnologia da informação vinculados ao Cartório, colocados à disposição para uso como ferramenta de trabalho, devem ser utilizados em atividades primordialmente relacionadas às funções institucionais desempenhadas pela serventia.

Parágrafo único. É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

Art. 10. É vedada a utilização dos recursos de tecnologia da informação com o objetivo de praticar ações prejudiciais ao funcionamento e à utilização de quaisquer recursos da rede de computadores do Cartório ou redes externas.

Parágrafo único. O Tabelião ou pessoa indicada por ele pode autorizar terceiros ou efetuar testes controlados de sistemas e de infraestrutura com o objetivo de identificar vulnerabilidades e mensurar riscos, adotando as medidas preventivas cabíveis a fim de evitar quaisquer efeitos danosos ou impactos indesejáveis ao ambiente computacional e ao trabalho dos usuários.

Art. 11. O uso dos recursos computacionais pelos colaboradores do Cartório está sujeito à monitoração, respeitando-se os princípios constitucionais e legais aplicáveis.

Art. 12. É vedado aos colaboradores, prestadores de serviço e fornecedores alterar, física ou logicamente, as estações de trabalho disponibilizadas pelo Cartório.

Art. 13. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento das informações, de acordo com a sua classificação.

**Seção III - Da gestão de ativos de informação**

Art. 14. As informações e dados produzidos ou recebidos pelo Cartório, em decorrência da prestação dos seus serviços, serão considerados públicos, ressalvadas as exceções previstas na legislação aplicável e considerando que a sua administração e gerenciamento é exercido em caráter privado (art. 236 da Constituição da República).

Art. 15. Os ativos de informação devem:

I. ser inventariados e protegidos;

II - ter identificados os seus titulares, nos termos da LGPD e do Provimento 134 do CNJ e demais normas jurídicas aplicáveis;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a sua entrada e saída nas dependências do Cartório autorizadas e registradas por autoridade competente;

V - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - ser regulamentados por norma específica quanto a sua utilização; e

VII - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 16. Cada ativo de informação do Cartório será de responsabilidade do colaborador responsável por sua inclusão no sistema, sob a supervisão do Tabelião.

Art. 17. Na eventualidade de impossibilidade de se identificar o colaborador responsável pelo ativo de informação, o Tabelião adotará as providências necessárias para a devida apuração e identificação, podendo nomear uma Comissão específica para isso.

Parágrafo único. A ausência desta identificação imediata não exclui a responsabilidade civil e penal do gestor identificado *a posteriori*, que será passível das punições descritas no Código de Ética do Cartório.

Art. 18. O Tabelião deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 19. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 20. Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pelo Cartório.

Art. 21. O acesso dos colaboradores, prestadores de serviço e fornecedores aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

**Seção IV - Do tratamento de incidentes de segurança**

Art. 22. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de SI por parte do prestador.

Parágrafo único. Em relação aos contratos mencionados no caput, cabe ao Tabelião ou pessoa indicada por ele supervisionar o tratamento de incidentes de SI para o fiel cumprimento das suas atribuições.

**Seção V - Da gestão de risco**

Art. 23. A gestão de riscos em SI constitui um processo contínuo de planejamento, execução, verificação e revisão das ações que visem manter em níveis aceitáveis os riscos de SI a que estão sujeitos os ativos de informação do Cartório.

Art. 24. Deverá ser definida, em normatização complementar, a metodologia de análise e avaliação de riscos, que será realizada periodicamente no levantamento de risco nos ativos de informação do Cartório, visando à proteção destes ativos.

Art. 25. A normatização mencionada no art. 24 deverá assegurar que as atividades de análise e avaliação produzam resultados comparáveis e reproduzíveis, de modo a permitir a priorização no tratamento dos maiores riscos.

§1º A normatização de que trata o caput deverá contemplar a definição de níveis aceitáveis de riscos, de acordo com requisitos legais, regulatórios ou internos do Cartório.

§2º Todos os riscos identificados, mesmo os que forem considerados aceitáveis, deverão ter sua evolução acompanhada para permitir a detecção de possíveis mudanças no seu impacto ou probabilidade de ocorrência.

**Seção VI - Da gestão de continuidade de negócios**

Art. 26. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento contínuo ou recuperação antecipada do Cartório quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

Art. 27. O Plano de Continuidade de Negócios do Cartório, baseado em metodologias e boas práticas e aprovado pelo Tabelião, deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

**Seção VII - Da auditoria e conformidade**

Art. 28. O Cartório manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

Art. 29. Os processos de negócio, em todas as áreas do Cartório, deverão ser auditados na conformidade com as normas de SI e a pertinente legislação em vigor.

Art. 30. É vedada ao prestador de serviços a responsabilidade de executar a verificação da conformidade dos próprios serviços prestados.

Art. 31. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações apresentadas pelo Tabelião.

Parágrafo único. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, e será montado um plano de ação para a tomada das ações cabíveis.

**Seção VIII - Dos controles de acesso**

Art. 32. As instalações, equipamentos, redes e sistemas de computadores, exceto os sistemas destinados a atendimento ao público, deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, que possibilitem a identificação das pessoas.

Art. 33. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa.

Art. 34. Para utilização dos recursos de TI do Cartório será sempre necessária a autenticação do colaborador, mediante credencial de acesso, senha ou identificação biométrica.

§1º As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimento sobre o Cartório.

§2º As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função.

Art. 35. Os equipamentos e softwares utilizados na administração dos recursos de TI deverão ser protegidos por senha, que será de conhecimento exclusivo dos técnicos da STI e/ou terceiros responsáveis pela administração destes recursos.

Parágrafo único. Os administradores dos recursos de TI do Cartório são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Art. 36. Na ocorrência de afastamento, mudança de responsabilidades ou atribuições dentro do Cartório, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos.

Parágrafo único. Na efetivação do desligamento do colaborador, deverão ser extintos todos os direitos de acesso e uso dos ativos de informação a ele atribuídos.

Art. 37. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio colaborador, a qualquer tempo, ou por determinação do Tabelião, especialmente quando houver suspeita de sua violação.

Parágrafo único. Qualquer utilização dos sistemas e demais recursos de informática do Cartório é de responsabilidade do colaborador ao qual estejam associadas as credenciais de acesso utilizadas.

Art. 38. A senha de rede valerá por prazo determinado, em normatização complementar estabelecida pelo Tabelião, ressalvado o caso da certificação digital, regida por regra específica.

Parágrafo único. O Tabelião divulgará as regras a serem seguidas na definição da senha de rede dos agentes públicos, além de recomendações que visem assegurar a maior privacidade possível da senha.

Art. 39. Poderão ser implementados controles de acesso físico para o acesso a algumas dependências do Cartório (tais como arquivos, salas e ambientes internos), com a disponibilização de credenciais que permitam o acesso dos colaboradores a estes locais.

Art. 40. O acesso de usuários, clientes, prestadores de serviço e fornecedores do Cartório às suas dependências internas só serão possíveis mediante autorização do colaborador responsável e sob sua supervisão.

§1º Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores do Cartório, mas poderão ter acesso à internet (wi-fi) quando solicitado e após autorização do colaborador responsável.

§2º Nos casos de invalidação temporária ou definitiva das credenciais de acesso dos colaboradores, o acesso aos ativos de informação do Cartório dar-se-á mediante as condições estabelecidas para os visitantes.

**Seção IX - Do desenvolvimento de sistemas**

Art. 41. O Tabelião deverá estabelecer critérios de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 42. Os desenvolvimentos e aquisições de sistemas e aplicações corporativas devem atender a requisitos de segurança previstos em norma específica.

**CAPÍTULO VI DAS PENALIDADES**

Art. 43. Ações que violem a PSI ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas e aos responsáveis poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

**CAPÍTULO VII DAS COMPETÊNCIAS E RESPONSABILIDADES**

Art. 44. Compete ao Tabelião:

I - implantar ações técnicas para os controles de segurança dos ativos de informação, de acordo com a sua classificação;

II - encaminhar solicitação dos recursos necessários para implantação da PSI, no limite de suas atribuições, à Autoridade competente para as providências cabíveis;

III - prestar assessoria técnica aos gestores de ativos nos temas relacionadas a TI;

IV – identificar e estabelecer um plano pra solução das situações que eventualmente comprometam a SI;

V - operacionalizar PSI no âmbito de suas atribuições;

VI - monitorar o uso dos recursos computacionais; e

VII - promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de SI.

Art. 45. Compete ainda ao Tabelião ou a pessoa por ele indicada:

I – manter atualizados os arquivos de seus colaboradores, principalmente relativos a alteração de cargo, função ou responsabilidades dos colaboradores do Cartório, bem como sobre afastamentos destes por períodos superiores a 30 (trinta) dias;

e II - promover a capacitação dos colaboradores nas normas de SI adotadas pela Cartório.

Art. 46. Compete aos colaboradores do Cartório:

I - indicar as necessidades de treinamento sobre eventuais assuntos relativos à PSI;

II - indicar as necessidades de concessão/revogação de credenciais de acesso para os colaboradores nos ativos de informação de sua responsabilidade, de acordo com sua classificação.

III - classificar os ativos de informação sob sua responsabilidade;

IV - determinar o nível de acesso frente aos ativos de informação sob sua responsabilidade; e

V - solicitar o credenciamento e descredenciamento de pessoas associadas a contratações de fornecedores e prestadores de serviços sob sua responsabilidade.

Art. 47. Compete ainda aos colaboradores:

I - conhecer e disseminar institucionalmente a PSI e as normas complementares de SI, propondo, inclusive, sugestões de melhoria;

II - cumprir e fazer cumprir as normas e procedimentos relativos à segurança da informação e das comunicações do Cartório;

III - informar imediatamente ao Tabelião qualquer evento relacionado à SI.

IV - zelar pelo sigilo das suas credenciais de acesso aos ativos de informação do Cartório;

V - comunicar a perda ou o comprometimento das suas credenciais de acesso;

VI - responder pela quebra de segurança ocorrida com a utilização da sua credencial de acesso; e

VII - manter o nível de proteção da informação a que tem acesso.

**CAPÍTULO VIII DISPOSIÇÕES FINAIS E TRANSITÓRIAS E VIOLAÇÕES**

Art. 48. A PSI será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 49. As propostas de alteração ou criação de normas internas sobre SI deverão ser encaminhadas ao Tabelião.

Art. 50. Após sua publicação, o Tabelião deverá dar ampla divulgação da PSI a todos os colaboradores.

Art. 51. A PSI deverá ser revisada e atualizada sempre que eventos ou mudanças significativas relativas ao tema assim o exigirem ou a cada período de 3 (três) anos.

Art. 52. O descumprimento de qualquer dispositivo desta PSI e demais normas e procedimentos estabelecidos relativos à SI configura descumprimento do dever inserido na legislação aplicável.

§1º Caso se verifique o descumprimento previsto no caput por funcionários de prestadores de serviços terceirizados, eventuais colaboradores ou estagiários, o Cartório poderá determinar a respectiva substituição ou o desligamento, sem prejuízo das eventuais sanções penais e civis previstas na legislação aplicável.

§2º Os colaboradores registrarão em Termo de Responsabilidade o conhecimento de todas as normas e procedimentos de SI, bem como das penalidades a que estarão sujeitos em caso de descumprimento ou violação da PSI.

Art. 53. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo Tabelião.

Art. 54. Será estabelecido, no futuro, um Comitê Gestor de Segurança da Informação multidisciplinar (CGSI) que será responsável por promover a cultura de Segurança da Informação, bem como pela revisão da Política de Segurança da Informação e aprovação das Normas de Segurança da Informação e de Procedimentos de Segurança da Informação, dele fazendo parte representantes de todos os setores do Cartório que tratam com ativos críticos para o negócio.

§1º O CGSI deve, ainda:

I – Apoiar as ações estratégicas para a implantação dos processos mínimos especificados para o Modelo de Gestão;

II – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação, avaliando, inclusive, a possibilidade de criação de área específica para Gestão da Segurança da Informação.

III – Propor alterações na Política de Segurança da Informação;

IV – Propor normas relativas à Segurança da Informação.

Art. 55. Constituem exemplos de violação da PSI, que devem ser imediatamente informadas ao Tabelião ou pessoa indicada por ele, passíveis de investigação para apuração das origens e medidas aplicáveis, no intuito de corrigi-las ou reestruturar os processos:

I – Uso ilegal de software;

II – Introdução (intencional ou não) de vírus de informática;

III – Tentativas de acesso não autorizado a dados e sistemas;

IV – Compartilhamento de informações sensíveis do negócio;

V – Divulgação de informações de clientes e das operações contratadas;

§1º. Os princípios de segurança estabelecidos na presente política possuem total aderência da Tabelião e devem ser observados por todos na execução de suas funções.

Art. 56. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os colaboradores e/ou fornecedores e prestadores de serviços às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

§1º. Caso tenha algumas dúvidas quanto aos princípios e responsabilidades descritas nesta norma, deve-se entrar em contato com o Tabelião.

Art. 57. Esta Portaria entra em vigor na data de sua publicação.

**BERNARDO PRADO DA CAMARA**

**Tabelião Titular do Segundo Ofício de Notas de Ipatinga/MG**

**Anexo 1 – DEFINIÇÕES**

Para melhor compreensão dos termos utilizados neste documento é importante disseminar os seguintes conceitos:

Colaboradores: São todos os colaboradores que geram e manipulam informações no âmbito do cartório e de seus parceiros.

Ativo: Qualquer coisa que tenha valor para a organização.

Ativo Critico: Aquele que gera, armazena, processa, transmite e descarta informações de valor e criticidade altos para o negócio.

Autenticidade: Propriedade que permite a validação de identidade de usuários e sistemas.

Avaliação de Riscos: processo global da análise de risco e da valoração do risco.

Comitê Gestor de Segurança da Informação (CGSI): grupo de pessoas com a responsabilidade de promover a implementação das ações de Segurança da Informação do cartório e de seus parceiros. – AINDA NÃO CRIADO.

Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos que não possuam autorização.

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem objetivos estabelecidos nas políticas.

Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

Evento de Segurança da Informação: ocorrência identificada de um dispositivo portátil, equipamento, sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação, ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.

Gestão de Riscos: atividades coordenadas para dirigir e controlar as ações inerentes aos negócios da organização, no que se refere aos riscos. Normalmente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco.

Incidente de Segurança da Informação: um simples ou por uma série de eventos de Segurança da Informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação.

Integridade: propriedade de proteção à precisão e perfeição da informação e dos meios e dos recursos necessários para manuseá-la ou obtê-la.

Política de Segurança da Informação: documento que declara o comprometimento da direção e estabelece o enfoque da organização para gerenciar a Segurança da Informação. Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários, colaboradores, prestadores de serviço, clientes e partes externas relevantes.

Salvaguarda de Processo Crítico: ações vitais para a empresa e seus clientes que devem ser conduzidas adequadamente, a fim de evitar falhas que possam gerar, entre outros, prejuízos, comprometimento de imagem e, até a inviabilização do negócio.

Proprietário da Informação: colaborador que define quem tem acesso à informação ou aos meios de processá-la ou obtê-la e que tipo de privilégio de acesso.

Regras Operacionais: conjunto de instruções que orientam os usuários sobre a utilização de algum recurso de tecnologia da informação e comunicação.

Recurso de Tecnologia da Informação e Comunicação: dispositivos portáteis, equipamentos servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de TI ou que a eles possam ser conectados para leitura e/ou gravação de dados, imagens ou informações.

Segurança da Informação: preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação ou dos meios de acessá-la ou obtê-la; adicionalmente, outras propriedades, tais como responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.

Tratamento de Riscos: processo de seleção e implantação de medidas de controle para modificar um risco.

Usuário: pessoa que utiliza sistemas e/ou demais recursos de tecnologia da informação e comunicação.

**Anexo 2 – DIRETRIZES ESPECÍFICAS**

A. Tratamento da Informação

Para o conjunto de informações utilizadas no Cartório, o Tabelião ou eventual Comitê Diretivo de Segurança e Contingência deve designar o proprietário. São atribuições dos proprietários das informações:

i. Nomear eventual gestor das informações, a quem cabe propor as regras de acesso às mesmas, e administrá-las operacionalmente; e

ii. Aprovar as regras de acesso às informações, conforme proposta.

Deverão ser configurados sistemas para atender às normas abaixo descritas para tratamento da informação, bem como a concessão de acessos a colaboradores.

Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo do Cartório. Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda. Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização. É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade do Cartório, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização do Tabelião ou CGSI, e das quais os funcionários venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

Os usuários devem adotar a prática de classificação da informação com o objetivo de fornecer o tratamento adequado à informação no aspecto de sua confidencialidade, nos termos da LGPD e Provimento 134 do CNJ.

Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco. As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo do Cartório. Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento que não deva ser armazenada nos termos do Provimento 50 do CNJ e demais normas aplicáveis deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do funcionário que necessita do suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento.

Os colaboradores poderão determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

a. Riscos inerentes às informações:

- Acesso por pessoas não autorizadas;

- Divulgação indevida;

- Indisponibilidade; e

- Alteração indevida.

b. Consequências: -

Fraudes: Possibilidades de lesão ao Cartório ou terceiros (clientes, fornecedores, etc.);

- Problemas legais: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços aos colaboradores, usuários, clientes, prestadores de serviço ou fornecedores, a outras pessoas físicas ou jurídicas;

- Perda de negócio: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;

- Prejuízo de imagem do Cartório: Possibilidades de prejudicar a imagem do Cartório ou de seus colaboradores;

- Problemas de recuperação: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

B. Segurança quanto às Pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos do Cartório.

i. Identificação das pessoas. Todas as pessoas com acesso aos sistemas e informações, pertencentes ou em posse do Cartório, deverão ter uma única identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pelo Tabelião ou CGSI.

ii. Declaração de Responsabilidade É um compromisso de responsabilidade direta do colaborador para com as informações, equipamentos e outras propriedades do Cartório a ele confiadas, devendo ser lida e assinada quando de sua admissão (Anexo 3). Este conceito deve ser utilizado também para prestadores de serviço e clientes:

- Prestadores de Serviço: a declaração de responsabilidade deve ser uma das cláusulas do contrato (Anexo 4).

- Clientes: a declaração de responsabilidade deve ser uma das cláusulas do termo de adesão ao produto - ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

A declaração de responsabilidade deve ser lida e assinada por todos os funcionários antes de ser arquivada na respectiva pasta funcional. Poderá ser utilizado um Termo de Responsabilidade eletrônico, mediante aprovação do Tabelião ou CGSI.

C. Segurança Lógica de Computadores, Redes e Sistemas Aplicativos

Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse do Cartório. Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão, liberação etc. Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação. Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários. As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

i. Normas para segurança lógica de computadores e redes: Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles. Cada colaborador deve definir e manter atualizada uma política de acesso aos seus aplicativos.

ii. Administração do acesso aos sistemas aplicativos: As informações devem ser analisadas pelos respectivos colaboradores, de forma a permitir que sejam definidas as regras de acesso, através de perfis. Os sistemas aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

iii. Administração do acesso de usuários: Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

iv. Controle de acesso a computadores e redes: Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto. O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados. Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

v. Normas para controle de acesso a computadores, redes e sistemas aplicativos: Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;

- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);

- Os sistemas devem ser programados para nunca exibir a senha na tela;

- As senhas devem ser individuais e intransferíveis. A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;

- As senhas não devem ser triviais e previsíveis;

- Os tipos de caracteres utilizados para a formação da senha devem ser:

1. Letras maiúsculas;

2. Letras minúsculas;

3. Números; e 4

. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !).

- As senhas deverão ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;

- Os sistemas devem prever um prazo para a expiração de senhas de no máximo 30 (trinta) dias; - Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterála no primeiro acesso;

- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de vinte e quatro senhas);

- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito; -

Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário;

- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

vi. Monitoramento de uso e acesso aos sistemas aplicativos:

Todos os sistemas aplicativos deverão:

- Detectar tentativas de acesso não autorizado;

- Registrar eventos de entrada no sistema (login);

- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas;

- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

D. Segurança no Acesso de Prestadores de Serviço

Este tópico visa estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos. Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado deve ser explicitado no contrato assinado. É proibida a utilização de equipamentos próprios do prestador conectados à rede da organização sem a devida autorização escrita pela área de segurança da informação que deverá avaliar a necessidade através de justificativa técnica. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um "firewall" para controlar os acessos. Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

E. Segurança Física de Computadores

Este tópico destina-se aos usuários e administradores de computadores conectados ou não a uma rede. O objetivo é garantir que as Instituições estabeleçam, administrem e utilizem computadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

i. Normas para segurança física de computadores: Os meios de armazenamento considerados como mídias removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas. Os computadores não ligados a uma rede, e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados. Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

ii. Responsabilidade na segurança física de computadores: Poderá ser indicado um profissional ou pessoa jurídica responsável por elaborar e manter atualizado o inventário de hardware e software no Cartório, responsável por garantir o controle sobre o acesso físico aos equipamentos.

F. Padrões para Instalação de Computadores O padrão de instalação para os computadores deve atender a todas as normas estipuladas pelo Cartório. A estrutura para manter a segurança física deve obedecer aos padrões de segurança geral do Cartório e adequar-se às seguintes especificações:

i. Sala: - As dimensões do local devem ser suficientes para a instalação dos equipamentos;

- A disposição dos cabos lógicos e de energia deve ser adequada de forma que as pessoas possam transitar livremente;

- As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas; e

- Os equipamentos devem estar em locais firmes que evitem trepidações.

ii. Refrigeração e qualidade do ar:

- Climatização deve ser conforme especificado pelo fabricante; e

- O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou falhas de processamento.

iii. Rede elétrica:

- É recomendável que exista aterramento exclusivo para os equipamentos e que os pontos de energia sejam estabilizados;

- Para os equipamentos considerados críticos recomenda-se a instalação de UPS (Uninterruptable Power Supply), fonte alternativa de alimentação de energia que é ativada automaticamente quando ocorre a queda na alimentação de energia;

- Os equipamentos devem ser instalados em uma rede elétrica seguindo os padrões recomendados pelos fabricantes; e

- As instalações elétricas devem sofrer revisões periódicas.

iv. Equipamentos Contra Incêndio:

- Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os funcionários; e

- Devem existir equipamentos de prevenção de incêndios adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio.

v. Iluminação:

- A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

vi. Precauções quanto à disponibilização das mídias de armazenamento:

- Quando as mídias removíveis de armazenamento forem vendidas, devolvidas ao fabricante ou enviadas para manutenção, as informações nelas contidas devem ser destruídas antes de deixar as dependências do Cartório. Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destruam.

G. Segurança Física dos Servidores de Rede Este item destina-se aos usuários de sistemas operacionais com características de servidores de rede. O objetivo é garantir que o Cartório administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

i. Normas para segurança física dos servidores de rede: As mídias removíveis de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas. Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

ii. Responsabilidades na segurança física dos servidores de rede: Será necessário

- Elaborar e manter atualizado o inventário de hardware e software; e

- Garantir o controle de acesso físico aos equipamentos.

H. Padrões para Instalação dos Servidores de Rede

O padrão de instalação para servidores de rede deve atender a todas as normas estipuladas pelo Cartório. A estrutura para manter a segurança física dos equipamentos de uma rede deverá adequar-se às mesmas especificações utilizadas para a instalação de computadores com as seguintes especificações adicionais:

i. Sala: - Fechada, mas permitindo a visualização interna do ambiente, com divisórias até o teto.

ii. Rede elétrica: - Nos servidores, fazer uso de equipamento UPS (homologado por técnicos autorizados) com ”No Break”; É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica.

iii. Equipamentos Contra Incêndio: - Se possível, e no caso das salas de servidores e/ou demais instalações do Cartório, poderão ser utilizados dispositivos automatizados de combate a incêndios, agentes extintores limpos como gases e outros recursos específicos a este tipo de ambiente.



iv. Precauções quanto à disponibilização dos meios de armazenamento:

- As manutenções mídias removíveis, realizadas no próprio local, devem ser acompanhadas pelo responsável da área.

I. Backup e Restore Este tópico se destina aos usuários e administradores locais do Cartório ou prestadores de serviços contratados no âmbito do Provimento 74 do CNJ, visando administrar e utilizar os recursos de informática de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, softwares ou sistemas.

i. Normas para Backup/Restore: A elaboração do plano de Backup/Restore deverá levar em consideração os aspectos abaixo:

- Os períodos de atualização dos dados;

- Particularidades do Cartório; e

- Regras descritas no Provimento 74 do CNJ.

As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups do Cartório, levando-se em consideração a periodicidade de atualização dos dados. As informações devem estar sujeitas às rotinas de backups conforme critério definido pelo usuário. As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas. Deve-se manter uma cópia do plano de Backup/Restore. Devem ser realizados testes de restore periodicamente, mantendo evidências do último teste realizado. Devem ser mantidas, no mínimo, as duas últimas versões dos backups.

A quantidade de versões será determinada por exigência legal ou norma interna.

ii. Plano de Backup/Restore - Conteúdo: Abrangência: Relação dos arquivos e diretórios a serem copiados no processo de backup. Periodicidade: Intervalo de tempo após o qual o sistema é submetido à rotina de backup. Retenção: Prazo pelo qual os backups devem ser mantidos. Procedimentos: Descrição dos procedimentos de backup. Quantidade de cópias: Número de cópias de backup, locais e meios de armazenamento. Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados. Registro do uso das cópias de backup: A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações. Manutenção das cópias Backup: Quando o prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados em novo meio, periodicamente.

J. Responsabilidades quanto ao Backup/Restore É de responsabilidade prestador de serviço contratado para atender às exigências descritas no Provimento 74 do CNJ, elaborar, manter e documentar o plano de backups e garantir a execução de seus procedimentos.



K. Testes regulares

Todo e qualquer meio de armazenamento assim como os procedimentos de recuperação devem ser regularmente testados, garantindo sua efetividade. A periodicidade deve ser uma por ano, a ser

determinada pelo Comitê de Segurança e Contingência, considerando o nível de risco do negócio. Devem ser mantidas evidências do sucesso dos testes feitos.

L. Pirataria

Este item se destina a todos os usuários, clientes, fornecedores ou prestadores de serviço com acesso aos computadores, inclusive portáteis, conectados ou não a uma rede e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de softwares dentro das instalações das empresas do Cartório.

i. Normas contra pirataria: A quantidade de licenças de softwares não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente. Não é permitido duplicar software de propriedade do Cartório a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas. Uma licença de uso de software do Cartório só pode ser instalada em computadores do Cartório. Não é permitido executar ou instalar qualquer software (inclusive software livre e de domínio público), telas de "screen saver", “papéis de parede” etc., que não estejam autorizados para uso. Todo software de demonstração deve vir acompanhado de uma autorização formal da empresa proprietária, indicando onde pode ser instalado e por quanto tempo. A utilização de software do tipo “shareware” só deve ser feita após a obtenção do registro junto ao proprietário. É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

ii. Responsabilidades quanto à pirataria: É da responsabilidade do colaborador:

- Verificar se o software a ser instalado é original, conferindo o mesmo com as devidas licenças de uso;

- Se a instalação foi autorizada pelo Tabelião ou CGSI, verificar se o software foi previamente homologado; e

- Implementar mecanismos que dificultem a pirataria através de qualquer meio.

M. Utilização Segura de Hardware e Software Todos os equipamentos portáteis (notebooks, laptops, netbooks, ultrabooks, tablets e smartphones) que tenham capacidade de armazenamento de dados, devem ser protegidos conforme especificação do Cartório. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, as mesmas devem ser criptografadas ou ter seu acesso protegido por senha. É proibida a utilização de qualquer equipamento particular, exceto smartphones, nas dependências do Cartório. É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de “softwares” ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas do Cartório ou desenvolvidos por terceiros para o Cartório.



N. Acesso à Internet

A Internet abrange vários aspectos e serviços (websites de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de

negócio. A restrição a websites não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de Internet. O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento). O usuário deve restringir o acesso aos websites ainda não bloqueados que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos etc.). Deve também comunicar o endereço eletrônico desses websites ao Tabelião ou CGSI, que deverá realizar seu imediato bloqueio. O acesso à Internet deve ser feito através de "Servidores de Acesso" protegidos por sistemas de Firewall. Quando for necessário o acesso utilizando uma segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem ser respeitados (antivírus e firewall local). Casos específicos como esses devem ser aprovados pelos responsáveis.

O. Acesso ao Correio Eletrônico

O Cartório disponibiliza aos seus funcionários a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial com o mesmo. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios. As mensagens de correio eletrônico devem ser rastreadas, a fim de permitir o monitoramento para identificar o uso indevido da tecnologia.

Q. Plano de continuidade do negócio

Um plano de continuidade do negócio deve garantir a recuperação dos processos críticos do Cartório quando da indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações das áreas de negócio. É de responsabilidade de cada área envolvida no desenvolvimento dos negócios, elaborar, testar e implantar seus planos de contingência. A definição de processos críticos de uma área, obrigatoriamente, deve obedecer a critérios emanados pelos Tabelião ou CGSI.

i. Pontos a serem observados no plano de continuidade do negócio: Na elaboração de um plano de continuidade do negócio os pontos abaixo devem ser observados:

- As funções críticas devem ser identificadas e definidas;

- Traçar uma estratégia para recuperação de cada função crítica;

- Priorizar as funções críticas para ordenar sua recuperação; - Identificar as atividades necessárias para recuperar cada função;

- Quantificar os recursos humanos e técnicos necessários ao cumprimento do plano;

- Documentar os processos críticos;

- Identificar os responsáveis pela recuperação de cada processo ou função;

- Ações para restabelecer a operação normal;

- Identificar os recursos de backup (infraestrutura, hardware, software, sistemas aplicativos e telecomunicações).

ii. Revisões periódicas do plano de continuidade do negócio: O plano de continuidade do negócio deverá sofrer revisões periódicas a fim de identificar pontos que estiverem em desacordo com a situação atual. Deverão ser observados os pontos abaixo:

- Troca de fornecedores ou contratados;

- Alteração de endereços ou números de telefones;

- Mudanças nas prioridades de recuperação;

- Interdependência entre sistemas e aplicativos;

- Mudanças nas funções e nos processos críticos de negócio;

- Mudanças nas práticas operacionais.

R. Plano de Conscientização de Segurança da Informação

Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir o seguinte objetivo: “Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os funcionários e colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.” As diretrizes básicas são:

- Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do Conglomerado;

- Divulgação de diversos materiais e alertas referente a Segurança da Informação para funcionários, colaboradores e clientes;

- Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;

- Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;

- Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

**ANEXO 3 – MODELO DE TERMO DE RESPONSABILIDADE:**

Eu (Nome do Funcionário), CPF/MF Nº (número) declaro para os devidos fins e efeitos de direito que a(o) Tabelionato do Segundo Ofício de Notas de Ipatinga/MG trouxe ao meu conhecimento o conteúdo das diretrizes, violações, normas e responsabilidades que regem sua Política de Segurança de Informação, que ora declaro ter lido, estando ciente e responsável pelo que segue:

1. Qualquer meio de acesso às informações ou instalações (como identificações de usuário, senhas, crachás, cartões, chaves, etc.) que a empresa me forneceu ou vier a fornecer são pessoais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades perante o Cartório, devendo ser por mim devolvidos em caso de desligamento;

2. Todas as informações utilizadas no Cartório, sejam elas de sua propriedade ou de terceiros, possuem caráter confidencial e sigiloso, motivo pelo qual comprometo-me a manuseá-las de maneira segura e somente no exercício de minhas atividades, evitando sua perda, furto, cópia, utilização indevida ou divulgação não autorizada;

3. O Cartório está autorizado a consultar e analisar informações registradas em qualquer meio localizado em suas instalações e que tenham sido geradas ou recebidas utilizando seus recursos, inclusive correspondências recebidas em nome ou endereço da mesma;

4. Não devo adquirir, reproduzir, utilizar ou distribuir cópias não autorizadas ou legalmente adquiridas de softwares ou programas produtos, mesmo aqueles eventualmente desenvolvidos internamente pelo Cartório;

5. Devo zelar pela segurança, uso correto e manutenção adequada dos equipamentos existentes no Cartório;

6. As informações por mim geradas ou recebidas durante minha jornada de trabalho deverão tratar apenas de assuntos profissionais e ligados exclusivamente ao exercício de minha função;

7. Descumprindo os compromissos por mim assumidos nesta declaração estarei sujeito as penalidades aplicáveis, como medidas administrativas/disciplinares internas e/ou ações penais/cíveis previstas em lei.

(Assinatura do Funcionário)

**ANEXO 4 – MODELO DE TERMO DE RESPONSABILIDADE PARA FORNECEDORES E PRESTADORES DE SERVIÇO**

As empresas prestadoras de serviço devem ser orientadas para que mantenham documento similar em seus arquivos, assinado pelos funcionários por ela contratados para prestar serviços no Cartório, devendo o texto abaixo ser incluído nos contratos de prestação de serviço:

"Fica a Contratada, responsável pela orientação dos funcionários por ela indicados para trabalharem junto à contratante, no que diz respeito ao cumprimento das Políticas de Segurança da Informação da Contratante, cumprimento das Leis de Copyright e de Combate a Pirataria de Softwares. Fica também a Contratada corresponsável pela utilização das senhas e uso das informações por parte dos funcionários por ela contratados e disponibilizados para atuação junto a Contratante, de acordo com o termo de responsabilidade assinado pelo funcionário da Contratada. Esta corresponsabilidade estende-se inclusive aos foros judiciais, sob todos os aspectos, inclusive o do direito das obrigações.