POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Responsável: Naurican Ludovico Lacerda
Desenvolvido em: 06/09/2021

Sumário

1. HISTÓRICO DAS REVISÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A edição atual deste Documento será publicada internamente em rede para acesso ilimitado da equipe.

A emissão, aprovação, distribuição, revisão, recolhimento e revogação deste documento será controlado pelo Titular e/ou responsável pelo SI. As versões anteriores do manual ficaram armazenadas nos repositórios controlados por sistema de backup. A versão disponível para consulta pública conterá apenas as informações da última revisão.

Revisão	Data	Descrição da Alteração	Aprovado por	Meio de Divulgação
04	25/10/23	Adequações para integrar as regulações da norma 27701/2019 a Política.	Encarregado da Proteção de Dados (DPO)	RQ004-Lista Mestra de Documentos Internos e Site do Cartório.
05	27/11/23	Alteração no procedimento 7.14	Encarregado da Proteção de Dados (DPO)	RQ004-Lista Mestra de Documentos Internos e Site do Cartório.

APROVAÇÃO

Ao aprovar esta Política, o Titular estabelece todas as responsabilidades e autoridades dos colaboradores, conforme o organograma e tabelas de responsabilidades, e solicita a obediência aos documentos normativos estabelecidos na Serventia.

Data: 27/11/2023

Naurican Ludovico Lacerda
Titular

2. POLÍTICA DA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

O **1° Registro de Pessoas Jurídicas, Títulos e Documentos e Protestos de Goiânia** trabalha com um conjunto de controles e mecanismos de modo a garantir a confidencialidade, integridade e segurança das informações que estão sob sua guarda através das seguintes diretrizes:

a) Satisfazer os requisitos aplicáveis à segurança da informação e privacidade.

b) Melhorar continuamente o sistema de gestão da segurança da informação e privacidade.

c) Estabelecer Objetivos de Segurança da Informação respeitando os atributos básicos relacionados à confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade.

d) Aplicar a presente política a todos os colaboradores e partes interessadas da Serventia.

O Cartório entende que o sistema de segurança da informação e privacidade somente será eficaz com o comprometimento de **TODOS** em respeitar e seguir a Política de Segurança da Informação e Privacidade.

3. ESCOPO DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE E SUA ABRANGÊNCIA

"O escopo deste SGI é: **Serviços de Protestos, Registros de Títulos e Documentos e Pessoas Jurídicas,** visando os interesses legítimos do usuário, de acordo com a legislação aplicável, garantindo a conformidade dos atos e a satisfação do usuário, por meio dos serviços prestados com eficiência, agilidade e segurança jurídica, bem como o atendimento ao antissuborno, à antifraude, ao combate à lavagem de dinheiro, ao compliance e a segurança da informação e privacidade. "

O **1º Registro de Pessoas Jurídicas, Títulos e Documentos e Protestos de Goiânia**, é uma Serventia Extrajudicial que possui três competências distintas, sendo elas o registro civil das pessoas jurídicas, o registro de títulos e documentos e o tabelionato de protesto.

Todas as atividades vinculadas as competências acima podem ser configuradas como tratamento de dados e informações, assim, os serviços realizados pela serventia incluem dados pessoais e sensíveis existentes nos registros, bem como informações dos colaboradores e da própria serventia. O SGSIP – Sistema De Gestão de Segurança da Informação e Privacidade está implementado em todas as áreas da Serventia, em todos os processos e atividades realizadas e é incorporado ao SGI (Sistema de Gestão Integrado) do Cartório.

O SGSIP é composto por controles, políticas, procedimentos e processos, todos criados e implementados para garantir a confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade da informação em conformidade com a legislação que circunda o tema.

O SGSIP abrange todos os sistemas de informação, físicos e digitais, desde os arquivos físicos (definitivos e temporários) até os dispositivos móveis.

O SGSIP da Serventia é gerenciado pelo comitê de Segurança da Informação, na pessoa do Encarregado de Segurança da Informação e Privacidade, que tem o papel de monitorar, revisar e agir sempre que necessário de modo a garantir a sua aplicação. O SGSIP será auditado/inspecionado periodicamente de modo a garantir que os requisitos de segurança da informação do Cartório sejam atendidos e que as medidas de segurança sejam atualizadas para lidar com as ameaças emergentes.

O escopo será revisado sempre que necessário para garantir que continue sendo relevante e adequado às necessidades da Serventia e para atender a quaisquer requisitos legais e relevantes ao serviço.

4. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação e Privacidade tem como principal objetivo documentar conceitos, procedimentos e comportamentos de modo a minimizar riscos, reduzindo as vulnerabilidades dos sistemas que tratam as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização, bem como a proteção de dados pessoais e sensíveis tratados.

Esta política tem a premissa de documentar e orientar quanto a ações de controle adotadas internamente, assegurando que os tratos das informações sejam realizados com a maior segurança possível, respeitando todas as legislações que tratam do tema segurança da informação e proteção de dados pessoais.

Este documento se dividirá em tópicos por assunto, onde cada item será trabalhado de modo a mostrar uma visão geral sobre o tema, estabelecendo ações de controle para assegurar seu cumprimento.

5. DEFINIÇÕES

SEGURANÇA DA INFORMAÇÃO: São medidas praticadas para garantir a proteção e preservação dos dados contra perigos, ameaças e incertezas, garantindo a confidencialidade, disponibilidade, integridade, confiabilidade, autenticidade e irretratabilidade.

Confidencialidade: capacidade garantir que as informações não serão acessadas sem permissão.

Disponibilidade: estar acessível e pronto para uso quando solicitado, desde que devidamente autorizado.

Integridade: capacidade de manter a informação precisa e integra.

Confiabilidade: relativo à consistência no comportamento e nos resultados desejados.

Autenticidade: comprovação de que são corretas as características que uma informação ou ativo possui.

Irretratabilidade: para toda informação armazenada, é possível verificar e provar o que foi feito, por quem foi feito e quando foi feito, impossibilitando a negação das ações dos usuários.

PRIVACIDADE DE DADOS: sistema usado para a proteção de dados pessoais e sensíveis vinculado a LGPD.

SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO: é usada para manter a segurança dos sistemas operacionais, tais como: banco de dados; computadores; provedores; servidores;

INFORMAÇÃO: É um conjunto de dados de forma organizada, capaz de transmitir significado e compreensão dentro de um determinado contexto. Seria o conjunto ou consolidação dos dados de forma a fundamentar o conhecimento.

RISCO: Relação entre probabilidade e impacto, ajudando a determinar onde concentrar investimentos em segurança da informação.

AMEAÇA: Elemento externo capaz de explorar vulnerabilidades existentes que pode ocasionar prejuízo em um sistema ou organização.

VULNERABILIDADE: Fragilidade de um ativo ou de um controle que pode ser explorado por uma ou mais ameaças.

PROBABILIDADE: Oportunidade de uma vulnerabilidade ser explorada por uma ameaça.

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: evento isolado ou série de eventos inesperados detectados no ambiente da organização, seja um sistema, serviço ou rede que indique uma possível violação ou falha com probabilidade significativa de comprometer as operações do negócio e de ameaçar a segurança da informação.

GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: processos para gerir o incidente (detecção, notificação, avaliação, resposta, tratamento) até sua resolução, seja por medidas corretivas, definitivas ou paliativas.

GESTÃO DE RISCO: Atividades coordenadas para dirigir e controlar uma organização em relação ao risco, aplicabilidade de suas políticas de segurança, bem como monitoramento e revisão dos riscos.

PLANO DE CONTINUIDADE DO NEGÓCIO: fornece estratégias para garantir que serviços essenciais sejam identificados, para garantir sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento da instituição. Também prevê quais planos de ação devem ser realizados em cada momento.

DADOS: Toda e qualquer informação vinculada a registro ou a colaborador da Serventia.

DADO PESSOAL: O dado pessoal é aquele que possibilita a identificação, direta ou indireta, da pessoa natural.

DADO SENSÍVEL: O dado sensível é aquele que trata de aspectos mais íntimos do indivíduo.

EQUIPAMENTO: Elementos que compõem a estação de trabalho do usuário, tais como microcomputadores, impressoras, scanners etc.

ESTAÇÃO DE TRABALHO: Local onde o colaborador exerce suas atividades laborais;

REDE DE COMPUTADORES: São dispositivos de computação interconectados que podem trocar dados e compartilhar recursos entre si.

USUÁRIO: Colaboradores e prestadores de serviço que utilizam um computador ou serviço de rede interna ou de internet da empresa.

SEGURANÇA FISICA E LÓGICA: Segurança física é a forma de proteger equipamentos e informações contra usuários que não possuam autorização para acessá-los. Enquanto a segurança lógica é um conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou programas desconhecidos.

SEGURANÇA FÍSICA (estrutura): A segurança física é responsável pela proteção de todos os ativos físicos da organização, razão pela qual sua abrangência

é extensa, englobando parte interna e externa, compreendendo também a proteção dos ativos quando estão sendo transportados como valores ou fitas de backup. Tratando da segurança física, é importante frisar que existem áreas que carecem de maior atenção no que diz respeito ao controle de entrada e saída de pessoas. São exemplos os departamentos que manipulam informações confidenciais ou equipamentos que devem ter sua segurança física assegurada (sala de Servidores/Centro de Processamento de Dados, Recursos Humanos e Arquivo). Os acessos a estas áreas são controlados para assegurar maior segurança das informações nelas contidas.

6. RESPOSANBILIDADES

6.1. Responsabilidade por garantir o cumprimento do SGSIP: Alta direção e membros do comitê de segurança da informação.

6.2. Responsabilidade por instruir a equipe de colaboradores sobre o SGSIP: Setor de Recursos Humanos e membros do comitê de segurança da informação.

6.3. Responsabilidade pelo cumprimento dos preceitos elencados na presente política: Todos os colaboradores e demais partes interessadas.

7. PROCEDIMENTOS BÁSICOS PARA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DO 1º PROTESTO COM FOCO NO ATENDIMENTO À POLÍTICA

7.1. REGRA DE CLASSIFICAÇÃO

As informações processadas pela Serventia devem ser categorizadas de acordo com um documento controlado denominado "Inventário de Informações". Essa categorização é realizada com foco principal na avaliação dos três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Além

disso, é essencial considerar sempre as necessidades das partes interessadas, especialmente em relação à segurança da informação, garantindo, assim, a segregação adequada do acesso às informações.

Uma vez classificadas, as informações receberão rótulos de identificação, facilitando sua gestão e controle.

Dessa forma, as informações serão adequadamente categorizadas e gerenciadas, garantindo a proteção efetiva das informações sensíveis e atendendo às necessidades de segurança da organização.

7.2. ACESSO AO PERÍMETRO DA SERVENTIA

O perímetro é a linha que delimita o território ou espaço físico da Serventia. Falando de rede de dados, é uma linha imaginária que separa a rede e seus dispositivos de outras redes e da internet, garantindo padrões de segurança contra acessos indevidos. A segurança desse perímetro é essencial para controlar tudo que tente ultrapassar os limites estabelecidos. É importante que todos os envolvidos sigam todas as orientações da política para minimizar ou até mesmo impedir que elementos perigosos e intrusos tenham acesso aos ambientes internos e por consequência as informações tratadas. Para a garantia de segurança do perímetro, as seguintes orientações devem ser respeitadas:

a) Todos os colaboradores da instituição devem conhecer e viver os preceitos contidos na Normativa Interna, Manual Interno de Tratamento de Dados, Política de Compliance e Antissuborno e Código de Ética da serventia;

b) Todos os visitantes, prestadores de serviços e quaisquer outras pessoas que acessem ao interior da Serventia (que não componham o quadro de colaboradores da serventia) deverão ser identificados na recepção e acompanhados por um responsável e ser orientados quanto as regras básicas dos sistemas (esse treinamento terá validade de um ano).

c) Todo acesso externo aos sistemas (bancos de dados, drives de rede e outros), seja ele feito de forma presencial ou remoto, devem ser acompanhados por pessoa competente (membro do TI).

d) Os colaboradores possuem acesso aos sistemas (bancos de dados, drives de rede e outros), são feitos conforme permissões de acesso de usuários criados pós admissão.

e) As áreas físicas classificadas como "Restrita" só poderão ser acessadas por pessoas não autorizadas (mesmo sendo um colaborador) mediante acompanhamento de um responsável, sendo proibida a sua permanência, desacompanhada, no local.

f) As seguintes áreas são classificadas como restritas: Sala do Titular, Centro de Processamento de Dados - CPD (Local dos servidores), Recursos Humanos, e Arquivo documental (passagem permitida a colaboradores, mas impedidos de acessar as pastas e arquivos sem autorização). Apenas membros do Setor e responsáveis pela atividade poderão acessar essas áreas livremente. As demais dependências físicas do Cartório poderão ser acessadas por usuários, prestadores de serviço e operadores mediante acompanhamento.

7.2 ACESSO AOS SERVIDORES/CENTRO DE PROCESSAMENTO DE DADOS - CPD

O ambiente deverá ser acessado apenas por colaboradores autorizados e quaisquer outros acessos deverão ocorrer mediante supervisão de um dos responsáveis pela área. Valem para este ambiente as recomendações abaixo:

a) Apenas pessoas autorizadas terão livre acesso ao local;

b) Pessoas estranhas à gestão e ao setor de TI não poderão permanecer no ambiente sem o acompanhamento de um responsável;

c) Deverá ser localizado em local isolado dos demais setores do Cartório e afastado do atendimento ao público, o local deverá possuir câmera de segurança (para monitoramento), detector de incêndio, extintor de incêndio, climatização do ambiente e com barreira física entre hall de atendimento ao público e maquinários.

7.3 ACESSO AO AMBIENTE DOS SETORES DE RECURSOS HUMANOS E ARQUIVO.

Ambos os ambientes são locais considerados como restritos, diante disso, as seguintes orientações deverão ser respeitadas:

a) Apenas as pessoas autorizadas terão acesso as chaves de acesso aos locais; havendo perda das chaves, deverão comunicar imediatamente aos responsáveis.

b) O tratamento dos documentos administrados pelos dois setores será feito apenas pelos responsáveis pelas atividades, qualquer terceiro que necessite manusear esses documentos o fará de maneira supervisionada, com autorização do responsável ou de membro da Alta Direção.

c) Os ambientes deverão ser monitorados por câmera de segurança.

7.4 ARQUIVOS TEMPORÁRIOS

O acesso a documentos localizados em arquivos temporários (documentos em tratamento dentro dos setores) deverá ser realizado apenas por membros do setor responsável pela guarda do documento. Sendo proibido o acesso de membros de outros setores sem autorização ou supervisão.

7.5 ESTAÇÕES DE TRABALHO

As estações de trabalho são os locais onde os colaboradores exercem sua atividade funcional primária, são as mesas de trabalho e suas extensões. Para falar das estações de trabalho, primeiro dividiremos e definiremos em dois tipos, a física e a digital.

Digital: cada estação de trabalho possui identificação única (login e senha monitorados pelo endereço de IP), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário, reforçando que todas as ações feitas na estação de trabalho digital, sistemas e rede são gravadas, geram log e podem ser

monitoradas. Por isso, sempre que se ausentar da estação de trabalho, o usuário deve ter certeza de que efetuou o logoff ou bloqueio da estação de trabalho, evitando que sejam executadas ações em seu nome.

Física: cada colaborador é responsável por uma variedade de atividades dentro da Serventia, sendo ele responsável por todos os documentos e registros que estejam com ele. Respeitar os preceitos e padrões dos Sensos de organização, limpeza e utilização faz com que as chances de vazamento de informações sejam reduzidas exponencialmente.

Documentos espalhados pelas mesas de forma desorganizada geram riscos grandes, como por exemplo acesso indevido de terceiros a registros e informações que não tem autorização para acessar, gerando assim, possíveis incidentes de segurança.

O colaborador é responsável por uma variedade de atividades dentro da Serventia, inclusive pela guarda e proteção dos documentos que estão sob sua responsabilidade. **Para que tenhamos segurança no trato de documentos e de informações nas estações de trabalho (física e digital), é vital que as seguintes recomendações a seguir sejam respeitadas:**

a) Não utilizar nenhum tipo de software/hardware sem autorização da área de TI;

b) Não utilizar qualquer software sem licença;

c) Não gravar nas estações de trabalho arquivos não autorizados como MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

d) Não é permitida a manutenção de registros ou documentos controlados fora do drive H/Lista mestra;

e) Todos os dados relativos ao cartório devem ser mantidos em drives onde existe sistema de backup diário e confiável;

f) Os arquivos gravados em diretórios temporários das estações de trabalho podem não possuir backup, portanto seu armazenamento é inseguro. Recomenda-se a utilização dos drives controlados para salvar arquivos importantes;

g) A política do 5 Sensos se aplica tanto à estação de trabalho física quanto a digital, devendo o colaborador manter suas pastas, organizadas, identificadas e os documentos nomeados com padrões de segurança (dar preferência para números de protocolos), evitando sempre que possível exposição de dados pessoais como nome e número de CPF/RG; pedimos especial atenção aos sensos de organização, utilização e limpeza;

h) Sempre que o colaborador se ausentar de sua estação de trabalho por tempo prolongado, deve organizar os documentos de modo a evitar que terceiros não relacionados a atividade tenham acesso a seu conteúdo. Mantenha sobre sua mesa apenas os documentos que estão sendo trabalhados. Se não estão sendo utilizados, mantenho-os arquivados ou armazenados em local específico no setor. Em intervalos curtos de tempo, organize os documentos de modo a não deixar as informações nele contidas expostas (documentos com dados visíveis a quem passa pelo local);

i) É proibido o compartilhamento de pastas, arquivos, documentos com pessoas não autorizadas e que não tenham relação com o tratamento das informações ali contidas;

7.6 DESCARTE DE DOCUMENTOS

Todo documento tratado pela Serventia, deverá ser descartado ou utilizado como rascunho quando seu uso ou armazenamento não for mais necessário. Havendo possibilidade de uso do documento como rascunho (papeis sem informações restritas ou confidenciais), estes deverão ser locados na caixa existente em cada setor identificada com "rascunho". Os demais documentos deverão ser direcionados para caixa de descarte, assim, este documento passará por um processo de descaracterização ou eliminação, evitando que as informações

e dados contidos nele fiquem expostos a vazamentos. Tenham atenção aos seguintes detalhes:

a) Possuindo dados pessoais ou sensíveis, deve o documento ser descaracterizado, picotado ou rasgado de modo a impedir a visualização das informações;

b) Não possuindo dados pessoais ou sensíveis, porém, podendo ser reutilizado como rascunho, direcione-o para caixa de rascunhos.

c) Não possuindo dados pessoais ou sensíveis e não podendo ser utilizado como rascunho, direcione-o para caixa de descarte ou dependendo para lixeira comum.

7.6.1. Descarte de ativos de informática.

Todo e qualquer ativo que chegar ao fim de seu ciclo de vida deverá ser eliminado com base nos procedimentos de eliminação existentes no Setor de TI. Tais procedimentos deverão ser executados de modo que as informações ali contidas não se percam e uma vez eliminadas não possam ser recuperadas. Maiores informações podem ser localizadas no POP-SGSI002-DESCARTE DOS ATIVOS DA INFORMAÇÃO.

7.7 REGRAS DE UTILIZAÇÃO DO E-MAIL

Os e-mails institucionais são de propriedade da Serventia, devendo seu uso ser feito exclusivamente para fins ligados à atividade. Esse tópico visa definir as normas de utilização de e-mail, compreendendo o envio, recebimento e gerenciamento das contas.

Todos os usuários de e-mail devem ter ciência que a Internet opera em domínio público e que não está sob o controle da equipe técnica de TI. As mensagens podem estar sujeitas a conteúdos e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia é feita através de e-mails, e é importante lembrar que uma parte relevante dos vírus eletrônicos atuais chega por

esse meio. Os vírus atuais são enviados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo pode conter vírus. É necessário ter bastante atenção. Diante dessa situação recomendam-se as orientações abaixo:

a) O serviço de e-mail não deve ser usado para fins pessoais, seu uso é restrito às atividades de interesse do Cartório.

b) A utilização da ferramenta deve ser feita de forma consciente e condizente com os padrões da Serventia, tanto no que diz respeito à linguagem usada, quanto à segurança da Serventia. A utilização de linguagem informal, gírias e afins não é permitida.

c) Atenção ao enviar ou encaminhar mensagens, assegure-se de estar endereçando para pessoa correta, evitando assim que dados pessoais ou de registros sejam vazados.

d) Recebendo e-mails por engano (que não são de sua responsabilidade), informe ao remetente o ocorrido. Se for assunto de interesse do Cartório, direcione ao Setor responsável.

e) É obrigatória a manutenção e organização da caixa de e-mail, evite acúmulo de e-mails e arquivos inúteis;

f) O acesso às caixas de e-mail deve ser realizado por webmail ou software homologado pela área de TI. É preferível que contas compartilhadas sejam acessadas através de webmail, sempre evitando que seja feita a leitura "incorreta" de um e-mail. Caso marque um e-mail como lido sem querer, volte o status dele para não lido e avise ao responsável pela resposta, assegurando assim que aquele não fique sem retorno.

g) Não executar ou abrir arquivos anexos enviados por emitentes desconhecidos ou suspeitos. Sempre verifique o remetente antes de clicar em links ou abrir anexos. Não abra arquivos com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza da segurança do e-mail;

h) Desconfiar de todos os e-mails com assuntos estranhos e/ou em outros idiomas;

i) Evitar anexos muito grandes. Os anexos possuem limitação de tamanho, em algumas situações, se necessário solicite a equipe de TI que armazene os anexos em uma nuvem para envio de link.

j) É proibida a utilização de e-mails particulares para tratar de assuntos relacionados ao Cartório.

k) As contas de e-mail pertencem ao Cartório, portanto, este tem acesso a todo o conteúdo.

7.8 REGRAS DE ACESSO A INTERNET

Esse tópico visa definir as normas de utilização da Internet que abrangem a navegação em sites, downloads e uploads de arquivos.

Em meio a esse novo cenário, o direito, por meio de suas diversas legislações vigentes, funciona como um regulador das relações no mundo virtual. É preciso que as pessoas tenham consciência de que tudo que fazem no mundo virtual gera efeitos jurídicos no mundo físico.

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos colaboradores do cartório. Não é permitido acesso a sites de conteúdo inapropriado (fofocas, pornografia e outros). Diante dessa situação recomendam-se as orientações abaixo:

a) É permitida somente navegação em sites. Outros tipos de serviços, como downloads e uploads diferentes dos já autorizados deverão ser solicitados diretamente para a área de TI da Serventia.

b) Não será permitido software de comunicação instantânea não homologados/autorizados pela área de TI;

c) Os acessos a sites com conteúdo estranho ao serviço poderão ser bloqueados, e as tentativas de acesso serão monitoradas.

d) É considerada falta gravíssima o acesso a sites com conteúdo pornográfico, discriminatório ou que faça apologia as variadas formas de crimes;

e) É proibida a realização de uploads, armazenamento em nuvem ou compartilhamento de qualquer tipo de informação ou documentos do Cartório através da internet sem a prévia autorização dos responsáveis;

f) É proibido o envio de fotos, pdfs e quaisquer outros tipos de arquivo que contenham informações de registros ou a ele relacionados por meio de ferramentas de comunicação não autorizadas (e-mail, whatsapp, telegrama e outros). Somente as pessoas previamente autorizadas poderão realizar a troca dessas informações.

g) É permitida a navegação em sites de conteúdo educativo, desde que o acesso seja realizado com autorização da coordenação que avaliara o melhor momento e o volume de trabalho no Setor.

h) O uso indevido e ou excessivo da ferramenta poderá ser considerada como falta grave;

7.9 REGRAS DE SENHAS

Senhas são mecanismos de validação da identidade do usuário, garantindo maior segurança ao usuário e ao controlador do ambiente acessados. A concessão de permissões de usuário é controlada e os logins e senhas são individuais e intransferíveis.

As senhas são utilizadas para garantir o acesso à rede e a todos os sistemas e portais. Elas garantem acesso exclusivo do usuário às ferramentas necessárias para execução de suas atividades. Alguns acessos poderão ser feitos por biometria.

A eficiência das senhas depende do usuário, pois cabe a ele definir sua senha dentro de padrões mínimos de segurança (letras maiúsculas e minúsculas, números e caracteres especiais). É vedado seu compartilhamento com outros colaboradores. Diante dessa situação recomenda-se as orientações abaixo:

a) Senhas devem ser alteradas periodicamente e não devem ser armazenadas de forma desprotegida;

b) As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas, compartilhadas em nenhuma hipótese.

c) Tudo que for executado com a senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário. Sendo de suma importância bloquear o computador quando se ausentar de sua estação de trabalho.

7.10 REGRAS DE USO DAS IMPRESSORAS

Esse tópico visa definir as normas de utilização das impressoras disponíveis na rede do cartório. Orientamos o que segue:

a) Antes de realizar a impressão, confirme a impressora de destino. Impressões em local incorreto além de desperdício, gera risco de vazamento de dados;

b) Verificar imediatamente se o que foi solicitado já está disponível na impressora, sendo vedado que documentos fiquem nas bandejas das impressoras mais tempo do que o necessário. Essa conduta minimiza riscos com vazamento de dados uma vez que terceiros tenham acesso às informações no documento;

c) Manter a impressora sempre abastecida de papel, evitando o acúmulo de trabalhos na fila de impressão, prejudicando as solicitações;

7.11 REGRAS DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrange o LOGIN, a manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens serão tratados junto a todos os usuários da rede de computadores, bem como pelos prestadores de serviços do Cartório que tenham ou possam vir a ter acesso a rede. Diante dessa situação recomendam-se as orientações abaixo:

a) Conceder privilégio mínimo aos usuários, de modo que só acessem informações necessárias as atividades de sua responsabilidade. É recomendável que nunca se libere privilégios e acessos além do necessário, pois estes aumentam os riscos sem qualquer benefício em troca. Tais políticas de acesso e privilégios são reguladas no POP-TI012-USUÁRIOS E SENHAS.

b) Não são permitidas tentativas de obter acesso sem autorização. Qualquer tentativa de acesso não autorizado será considerada como tentativa de invasão. Tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta, será tida como falta grave. Isso inclui tentativa de acesso a dados que não pertencem ao perfil de acesso do colaborador ou fornecedor.

c) Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques e tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "invadir" um servidor;

d) O usuário deve fazer manutenção no seu diretório pessoal periodicamente, evitando o acúmulo de informações desnecessárias (prática do 5S digital);

e) Materiais de natureza: política (salvo registros públicos), pornográfica, racista ou sexista não podem ser armazenados, distribuídos, editados ou gravados através do uso dos recursos da Serventia;

f) Jogos ou qualquer tipo de software/aplicativo não podem ser gravados ou instalados no diretório pessoal do usuário, no computador local ou em qualquer outro diretório da rede;

g) É proibida a instalação de softwares sem o acompanhamento da equipe técnica da área de TI, instalações e remoções de aplicativos ou acessos devem ser feitas com autorização da coordenação imediata;

h) Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como quaisquer outras modificações que não sejam justificadas e efetuadas pela área de TI;

i) A utilização de equipamentos de informática particulares, computadores, celulares, impressoras, entre outros é restrita, ressalvadas situações excepcionais. Reforçando que a utilização de qualquer equipamento particular deve ser autorizada pela coordenação, o uso sem autorização e controle será considerado como falta grave, pois aumenta os riscos com incidentes de segurança;

j) Os acessos a sistemas, de qualquer fornecedor (externo ou interno), devem ser controlados pela identificação do usuário. As senhas compartilhadas devem ser excepcionais e autorizadas pelo responsável pela área de TI.

k) Todo o acesso realizado deve ser autenticado por login e senha individual ou biometria;

l) É obrigatório armazenar os arquivos inerentes ao Cartório na rede. As máquinas locais não possuem backup;

m) É proibida a abertura de computadores ou outros equipamentos para qualquer tipo de reparo. Caso seja necessário o reparo, este deverá ser feito pelo responsável da área de TI;

n) Quando existe a transferência de um funcionário de um setor para outro, o coordenador que solicitou a transferência, deve informar para o setor de TI os novos privilégios de acesso;

o) Quando ocorrer o desligamento do funcionário, os responsáveis pelo TI devem providenciar a desativação dos acessos do usuário a qualquer recurso a rede, sistemas, aplicativos, e-mails e sites conforme descrito no POP-TI012-USUÁRIOS E SENHAS.

p) Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

7.12 REGRAS DE ADMINISTRAÇÃO DE CONTAS

Este tópico visa definir as normas de administração das contas que abrangem: criação, manutenção e desativação da conta.

Todo colaborador que necessite de acesso as informações compartilhadas através da rede ou de algum sistema que esteja instalado nela, terá uma conta com acesso aos recursos (login geral do Windows). Os acessos aos sistemas e portais serão concedidos mediantes solicitação do coordenador conforme a necessidade do cargo. Para a criação de nova conta ou alteração dos perfis de

acesso dos colaboradores, os coordenadores deverão proceder conforme descrito abaixo:

a) O coordenador do setor deverá fazer a solicitação da criação ou liberação de acessos através de suporte aos responsáveis pelo Setor de TI.

b) Na solicitação de criação deverá informar o nome completo do colaborador, bem como a quais programas/aplicativos ele terá acesso.

c) O Setor de TI informará para o colaborador as informações de acesso e comunicará o coordenador sobre os acessos disponibilizados.

É reservado a Serventia, o direito de desativar uma conta de usuário. Havendo necessidade o responsável da área de TI irá providenciar a desativação. São motivos que poderão dar ensejo a ação:

a) Incidentes suspeitos de quebra de segurança;

b) Utilização de programas para quebra de senhas;

c) Desligamento de colaborador;

Maiores informações em POP-TI012-USUÁRIOS E SENHAS.

7.13 REGRAS DE BACKUP

A política está relacionada a segurança da informação, sendo de extrema importância a consecução do plano de continuidade de serviços. Consiste no armazenamento seguro das informações do Cartório, sendo os backups divididos em diversos locais (redundâncias), garantindo cópias idênticas em tempo real ou em rotinas programáveis.

Os procedimentos de backup (processos de execução e garantias de segurança) possuem procedimento próprio localizado na Lista Mestra de Documentos Internos.

a) Os backups só podem ser feitos por membro do TI ou por pessoa por ele delegada, a depender de autorização do Titular, Substitutos ou Coordenador da área de TI;

b) Os backups só podem ser acessados por pessoa autorizada pelo Titular, Substitutos ou Coordenador da área de TI;

c) Os backups devem ser protegidos com travas de segurança como: senhas, criptografia e outros que o Titular julgar necessários;

d) Os backups físicos deverão ser armazenados em locais distintos, garantindo a segurança contra acidentes no local de armazenamento;

e) Os backups deverão ser restaurados periodicamente (test restore) de modo a garantir a integridade dos dados;

Maiores informações em POP-TI006-BACKUPS.

7.14 REGRAS DE CAPACIDADE DE ARMAZENAMENTO

A Serventia deve possuir capacidade de armazenamento suficiente para armazenar todas as informações sob sua guarda. A gestão do Cartório através dos membros do TI devem monitorar e avaliar frequentemente a capacidade de armazenamento interna ao Cartório e a de seus parceiros (serviços em nuvem) através do R-TI004-Checklist Infraestrutura de TI. A gestão de Descarte de informações deverá seguir as orientações do POP-SGSI002-DESCARTE DOS ATIVOS DA INFORMAÇÃO.

7.15 REGRAS DE CONFIGURAÇÕES

Os hardwares devem estar devidamente conectados e instalados, atualizar regularmente os drivers e o firmwares para garantir a segurança e o desempenho ideais, manter o sistema limpo e livre de poeira para evitar o superaquecimento, e realizar backups regulares dos dados importantes. Além disso, é importante seguir as instruções do fabricante ao montar ou instalar novos componentes e utilizar software de segurança confiável para proteger o hardware contra ameaças cibernéticas.

As configurações de software devem manter os softwares atualizados com as últimas correções de segurança e patches para proteger contra vulnerabilidades

conhecidas, utilizar conexões seguras, como HTTPS, para proteger a transmissão de dados confidenciais pela rede, exigir senhas fortes e atualizar regularmente para proteger contra acesso não autorizado, limitar o acesso aos dados e funcionalidades apenas para usuários autorizados, seguindo o princípio do menor privilégio, implementar sistemas de monitoramento proativo para detectar e responder a ameaças em tempo real, realizar backups regulares dos dados importantes para garantir a recuperação em caso de incidentes de segurança.

Regras de configuração de serviços e redes devem ser estabelecidas, implementadas, monitoradas e revisadas. Atualizações regulares dos sistemas e softwares para corrigir vulnerabilidades conhecidas, utilização de conexões seguras, como VPNs, para proteger a transmissão de dados, implementação de políticas de senhas fortes e multi-fator de autenticação para reforçar a segurança das contas de usuário, restrições de acesso baseadas em segregação como funções e necessidades para limitar a exposição a dados sensíveis, monitoramento proativo de atividades suspeitas e potenciais ameaças à segurança da rede, realização de backups regulares para garantir a disponibilidade e integridade dos dados em caso de incidentes de segurança.

7.16 CIRCUITOS FECHADOS DE TV (CFTV)

A Serventia possui circuitos fechados de tv que fazem o monitoramento do perímetro, captando imagens por meio do uso de câmeras e transmitindo-as remotamente.

a) As gravações só podem ser acessadas por pessoa autorizada pelo Titular, Substitutos ou Coordenador da área de TI;

b) As gravações do perímetro têm como objetivo aumentar a segurança dos ambientes do Cartório. A gravação além de inibir comportamentos inapropriados, garante as partes envolvidas maior probabilidade de fazer valer seus direitos quando violados.

c) As gravações são armazenadas pelo prazo de 25 dias.

Para maiores informações POP-TI010-MONITORAMENTO CFTV E DE GRAVAÇÕES DE ÁUDIO.

7.17 GRAVAÇÕES TELEFÔNICAS

A serventia faz a gravação das ligações com a premissa de garantir a segurança das partes envolvidas, mitigando riscos e garantindo o direito de acesso as comunicações realizadas.

Os atendimentos realizados por meio de telefone são gravados e armazenados pela Serventia, sendo eles acessados em caso de necessidade de apuração de denúncias, reclamações ou situação similar.

Os seguintes itens de segurança devem ser respeitados quando tratamos das gravações telefônicas:

a) As gravações só podem ser acessadas por pessoa autorizada pelo Titular, Substitutos ou Coordenador da área de TI;

b) As gravações são protegidas por controle de acesso em local seguro;

Para maiores informações POP-TI010-MONITORAMENTO CFTV E DE GRAVAÇÕES DE ÁUDIO.

7.18 REGRAS DE TRABALHO REMOTO

Os colaboradores que porventura venham a realizar trabalho remoto (home office/tele trabalho), deverão ter passado pelos treinamentos que tenham relação com a proteção de dados (Compliance, LGPD e Segurança da Informação e Privacidade) e assinado os respectivos termos de ciência e adesão aos compromissos de guarda e sigilo das informações.

Para acessar as ferramentas e sistemas necessários a realização das atividades em home office, será utilizado ferramenta de acesso remoto validada e testada pela equipe de TI. Não serão feitos acessos diretos aos sistemas, rede ou documentos fora do perímetro da Serventia.

Em regra, os computadores utilizados pelo colaborador em home office serão de propriedade da Serventia. Havendo necessidade de uso de computador pessoal, este deverá estar atualizado e possuir mecanismos de segurança (antivírus).

As seguintes recomendações devem ser respeitadas para que os níveis de segurança da informação se mantenham elevados:

a) Utilização de conexão segura, rede privada com conexão VPN;

b) Os softwares utilizados devem estar atualizados (sistema operacional, antivírus e outros);

c) Utilize senhas seguras, evite a utilização de senhas frágeis, fáceis de adivinhar;

d) Para troca de arquivos considerados confidenciais, sempre que possível utilize criptografia ou outro meio de proteger essa informação;

e) Mantenha as mesmas políticas existentes na instituição, visando manter a confidencialidade, principalmente se o espaço utilizado para trabalhar é compartilhado ou pode ser acessado por terceiros;

f) Sempre que o trabalho remoto cessar, ou uma informação ou dado se tornar desnecessário, elimine-o.

g) Esteja atento e vigilante a e-mails suspeitos, mensagens com phishing.

h) Esteja atento e atualizado as políticas de segurança do Cartório.

7.19 REGRAS DE DISPONIBILIZAÇÃO DE ATIVOS

Sempre que necessário a Serventia poderá disponibilizar ativos de seu inventário a colaboradores, principalmente computadores a periféricos. Os ativos serão disponibilizados para execução de trabalho remoto e durará enquanto o colaborador estiver em home office.

Os ativos disponibilizados deverão possuir as últimas atualizações disponíveis para garantir a segurança da informação. O colaborador em home office que fará uso destes ativos assinará termos de guarda e uso, se

comprometendo a utilizar boas práticas de uso (manter o ativo em local seguro, em rede elétrica estável e ter atenção aos critérios de segurança dispostos nessa política) e devolvê-lo assim que o período de home office cessar.

7.20 REGRAS DO USO DE CRIPTOGRAFIA

A criptografia é uma ferramenta importante em uma política de segurança da informação, pois ajuda a proteger os dados confidenciais contra acessos não autorizados. Na serventia utilizamos as seguintes criptografias:

Criptografia de transmissão: A criptografia de transmissão é usada para proteger a comunicação de dados enquanto eles estão em trânsito no site e transferência dos backups para a nuvem. Isso é feito usando protocolos de criptografia SSL, que são comumente usados em conexões HTTPS seguras.

Criptografia de senha: A criptografia de senha nos bancos de dados é usada para proteger as senhas dos usuários contra acesso não autorizado.

7.21 REGRAS PARA TRANSFERÊNCIA DE INFORMAÇÕES

As transferências de informações se dão principalmente de forma verbal, por e-mail, uploads em centrais eletrônicas ou plataformas de órgãos controladores e por meio físico. Para que tenhamos mais segurança durante a realização destas transferências, os colaboradores deverão seguir minimamente as seguintes recomendações:

a) Repasse de informações de forma verbal (presencialmente ou telefone) deve o envolvido se certificar que as informações repassadas se limitem ao necessário, sendo autorizado repassar informações apenas a partes interessadas dentro das autorizações constantes nos procedimentos operacionais; respeitando sempre o dever de sigilo constante no código de ética e normativa interna;

b) O dispositivo que estiver realizando a transferência das informações deverá estar conectado a uma rede segura;

c) Os acessos aos e-mails ou plataformas deverá ser realizado através de senha segura ou outro mecanismo de autenticação seguro (biometria ou certificado digital);

d) Sempre antes de realizar o envio, principalmente quando este for feito via e-mail, confirme o endereço do destinatário;

e) As operações de transferência de informações devem ser limitadas a um número reduzido de pessoas, somente colaboradores previamente autorizados poderão realizar a operação;

f) É importante que as informações transferidas possuam backup de segurança;

g) Transferências de informações por meio físicos, sejam estes ativos de informática ou documentos deverão ser executadas respeitando os procedimentos padrões estabelecidos no setor responsável;

7.22 REGRAS DO RELACIONAMENTO COM FORNECEDORES

Os fornecedores e prestadores de serviço, sejam eles operadores ou não (nos termos da LGPD), devem exercer suas atividades atendendo as orientações da Serventia (controlador). A depender do nível de acesso que o parceiro tiver, as seguintes recomendações devem ser respeitadas:

a) Durante o processo de contratação, o setor administrativo deverá solicitar a inserção de cláusula no contrato que trate da Segurança da Informação e proteção de dados pessoais e sensíveis, tais obrigações devem estar expressas: o dever de sigilo, de proteção as informações compartilhadas, e demais obrigações vinculadas a LGPD e Prov. 134 de 2022 do CNJ.

b) O contrato entre Cartório e provedor externo deve ser avaliado pelo responsável pela Segurança da Informação de modo a avaliar a suficiência dos itens inerentes a SIP. Havendo necessidade, deverá o responsável solicitar a assinatura de um termo aditivo.

c) Sendo o prestador de serviço considerado operador nos termos da LGPD, deverá preencher os formulários e termos de responsabilidade sobre o tratamento de dados.

d) Sendo o operador de dados um fornecedor de tecnologia, sistemas ou similar, deverá este comprovar suas adequações a LGPD.

e) Via de regra todos os acessos (relacionados a TIC) serão realizados com a supervisão de um membro do setor de TI.

f) Os acessos realizados de maneira remota são controlados e monitorados, feitos através de login e senha disponibilizado por membro do TI ou via VPN.

g) Os acessos ao perímetro físico da Serventia deverão ser sempre monitorados por um responsável pela infraestrutura do Cartório ou por membro do setor de TI.

h) O fornecedor será avaliado periodicamente pela função compliance, verificando também pontos relacionados a SI.

i) Os fornecedores com acesso as informações serão avaliados periodicamente pelo Encarregado de Segurança da Informação e Privacidade, de modo a validar o seu não envolvimento com incidentes de Segurança da Informação.

7.23 REGRAS DO USO DE DISPOSITIVOS MÓVEIS

A utilização de dispositivos móveis como celulares, tablets ou notebooks só existirá com o consentimento da direção do Cartório.

Com exceção dos membros da alta direção, somente os escreventes de intimação, membros do Administrativo e do Setor de TI poderão realizar tratamento de informações através de seu telefone particular (respeitando os limites das atribuições e da atividade).

Outros dispositivos que porventura tenham a necessidade de acessar a rede deverão passar por avaliação e eventual configuração pelos membros do TI.

7.24 REGRAS DO DESENVOLVIMENTO SEGURO E AQUISIÇÃO DE APLICAÇÕES

Adotar as seguintes práticas de desenvolvimento seguro:

Avaliar os riscos potenciais que o software pode apresentar e a definição de medidas de proteção adequadas para mitigar esses riscos.

Estabelecer requisitos de segurança claros para o software e sua implementação durante o processo de desenvolvimento.

Adotar boas práticas de programação, como o uso de validação de entrada de dados e a adoção de padrões de codificação seguros.

Executar testes de segurança abrangentes durante o processo de desenvolvimento, incluindo testes de penetração, testes de vulnerabilidades e testes de segurança funcionais.

Ao adotar essas práticas, os desenvolvedores podem criar software que seja mais resistente a falhas de segurança e ofereça uma maior proteção aos usuários.

Assim como no desenvolvimento das ferramentas, esse melhor olhar deve ser tido para aquisição junto a terceiros. Os aplicativos devem garantir segurança na proteção das informações e rastreabilidade (histórico ou log) para monitoramento. Toda ferramenta que tenha relação com tratamento das informações deve ser avaliada por um membro do comitê de segurança da informação.

Para maiores informações POP-TI018-DESENVOLVIMENTO SEGURO

7.25 REGRAS PARA REALIZAÇÃO DE AUDITORIAS

Dividiremos este item em tópicos de acordo com o tipo de auditoria realizada.

7.25.1 Auditorias internas: As auditorias serão realizadas por auditores capacitados e qualificados. Os auditores poderão ser membros da equipe interna de auditores ou convidado. Em todas as situações, as práticas descritas ao final do item deverão ser respeitadas.

7.25.2 Auditorias externas: As empresas contratadas para realizar a auditoria já possuem termo de confidencialidade e as auditorias tem o sigilo como pratica funcional, entretanto, devemos nos atentar ao escopo da auditoria, de modo a não disponibilizar informações além do necessário. É importante também que qualquer informação documental fornecida para o auditor seja eliminada ao fim do processo de auditoria ou de certificação.

7.25.3 Auditoria de sistemas: Internamente os sistemas (vinculados a operação) não são auditados uma vez que não temos acesso aos códigos fonte dos programas utilizados. Entretanto, cabe ressaltar que existe ambiente de teste e homologação controlado, protegido e isolado dos servidores principais, possibilitando a realização de testes seguros, sem qualquer risco de impacto as informações tratadas.

7.25.4 Boas práticas a serem executadas durante a realização de auditorias:

a) Atenção ao escopo da auditoria, não fornecer informações além do necessário;

b) Toda e qualquer informação gerada a partir da auditoria (com exceção do relatório de auditoria) deverá ser eliminado;

c) Auditores externos deverão estar sempre acompanhados por um colaborador do Cartório;

d) Informações classificadas como confidenciais não poderão ser enviadas, caso haja necessidade, poderão ser apresentadas, mas não compartilhadas;

e) Testes e avaliações de sistemas deverão ser testados e homologados em ambiente seguro antes de serem disponibilizados aos usuários;

8 ANÁLISE DE RISCOS E TRATATIVAS, VULNERABILIDADES E AÇÕES DE CONTROLE E INTELIGÊNCIA DE AMEAÇAS

A análise de risco será realizada conforme PGE-016 - MAPEAMENTO DE RISCOS E OPORTUNIDADES e PGE-018 - GESTAO DE SEGURANCA DA

INFORMACAO E PRIVACIDADE. Parte dos controles dos riscos levantados são demonstrados através do R-SGSI002-Declaração de Aplicabilidade de Segurança da Informação e Privacidade.

As vulnerabilidades serão abordadas na mesma ferramenta de avaliação. É importante entender que as vulnerabilidades têm um impacto direto sobre o risco, aumentando a probabilidade de ocorrência. Quanto maior a vulnerabilidade, maior a probabilidade de um incidente ocorrer e, consequentemente, maior o nível de risco associado. Portanto, é crucial monitorar continuamente todas as vulnerabilidades, uma vez que a falta de controle pode resultar na concretização dos riscos em forma de incidentes. O monitoramento deverá ser feito através do controle R-TI004-Checklist Infraestrutura de TI. Para mitigar esses riscos, os controles aplicados às vulnerabilidades existentes devem ser eficazes em reduzir ou eliminar as probabilidades de um incidente ocorrer.

Além das constantes no controle de avaliação de riscos, são exemplos de algumas vulnerabilidades a monitorar:

1. Gestão de senhas fracas: senhas fracas ou compartilhadas podem ser um grande ponto de vulnerabilidade. É importante promover o uso de senhas fortes e únicas, bem como o não compartilhamento de senhas.
2. Falta de treinamento em segurança: a falta de conscientização e treinamento em segurança da informação entre os funcionários pode resultar em erros que levam a violações de segurança.
3. Falta de atualizações e patches: sistemas e software desatualizados são frequentemente explorados por invasores. É importante aplicar regularmente patches de segurança.
4. Instalação de softwares não autorizados, sem licença ou acompanhamento de membro do Setor de TI.
5. Phishing e engenharia social: ataques de phishing e engenharia social continuam sendo uma ameaça significativa, pois os atacantes enganam os funcionários para que revelem informações confidenciais.

6. Acesso não autorizado: funcionários ou terceiros com acesso não autorizado a sistemas e dados podem representar um grande risco. A gestão rigorosa dos direitos de acesso é fundamental.

7. Malware e ransomware: a infecção por malware, incluindo ransomware, pode resultar em perda de dados e custos significativos. É importante ter proteção antivírus atualizada.

8. Falta de monitoramento e detecção de ameaças: não monitorar ou detectar atividades suspeitas pode permitir que ataques passem despercebidos.

9. Acesso remoto não seguro: conexões remotas não seguras podem ser exploradas.

10. Dispositivos móveis não gerenciados: dispositivos móveis não gerenciados podem acessar dados corporativos sem medidas de segurança adequadas.

11. Armazenamento em nuvem inseguro: o armazenamento em nuvem desprotegido pode levar ao vazamento de informações sensíveis.

12. Redes e firewalls inadequados: configurações inadequadas de rede e firewall podem permitir o acesso não autorizado a sistemas internos.

13. Gestão de terceiros: terceiros com acesso a sistemas ou dados da empresa podem ser um ponto fraco.

14. Backup e recuperação inadequados: a falta de backups adequados pode resultar em perda permanente de dados em caso de falha ou ataque.

15. Cultura de segurança fraca: uma cultura organizacional que não valoriza a segurança da informação pode levar a práticas inseguras.

16. Não atendimento as obrigações de compliance, regulamentações e conformidade: não estar em conformidade com regulamentações de segurança pode resultar em penalidades legais e perda de confiança dos clientes.

17. Falta de plano de resposta a incidentes: não ter um plano eficaz para lidar com incidentes de segurança pode aumentar o impacto de violações.

Para maiores informações sobre o tratamento de vulnerabilidades acesse PGE-018 - GESTAO DE SEGURANCA DA INFORMACAO E PRIVACIDADE.

Em caso de eventos, ocorrências ou qualquer situação identificável como um incidente de segurança, é imperativo que sejam abordados e avaliados conforme as diretrizes estabelecidas no R-SGSI010-REGISTRO E AVALIAÇÃO DE INCIDENTES DE SI. Após a conclusão do tratamento e da avaliação, quando a ocorrência é confirmada como um incidente e sua gravidade é classificada como alta, com dano ou potencial dano aos titulares, é essencial que todas as informações relevantes sejam devidamente registradas no Relatório de Não Conformidades (RNC) no SGT. Isso resultará na criação de um valioso conjunto de "inteligência de ameaças", proporcionando recursos para consultas futuras e orientações sobre como abordar e mitigar eficazmente essas ameaças.

No que tocam os controles de rede e similares, o monitoramento é feito por empresa terceirizada “Infomach”, tendo ela a responsabilidade de reportar ao Setor de T.I da serventia tudo que registrar e fizer. Os relatórios sobre tentativas de acesso, ameaças e teste de restore do ambiente são armazenados de forma controlada no H:\SGI\SETOR TI\REGISTROS\RELATÓRIO DE CONTROLE DE AMEAÇAS.

Reforçando que assim como descrito na Política de Compliance e Antissuborno, o tratamento de itens relacionados à segurança da informação deverá ser feito de forma escalonada, de modo que uma pessoa envolvida em um incidente não participe diretamente das decisões e apuração, salvo na qualidade de testemunha.

9 SANÇÕES APLICÁVEIS

A aderência a este documento é uma cláusula e condição do vínculo empregatício profissional do colaborador com o Cartório 1º REGISTRO DE PESSOAS JURÍDICAS, TÍTULOS E DOCUMENTOS E PROTESTOS DE GOIÂNIA-GO. Os Colaboradores devem estar cientes de que as violações da política, código de

ética e conduta e normas internas serão tratadas com a maior seriedade e estarão sujeitas às ações disciplinares aplicáveis, independentemente do nível hierárquico, sem prejuízo das penalidades legais cabíveis.

As violações poderão resultar em penalidades, variando de uma advertência verbal, escrita, suspensão e demissão. Violações podem também resultar em processos cíveis ou penais e sanções. Em casos onde a violação possa causar dano irreparável ao Cartório, esta pode entrar com uma ação judicial, além de reclamar danos patrimoniais.

Provedores externos, prestadores de serviço e fornecedores que se envolverem em incidentes de segurança passarão por processo disciplinar que poderá ocasionar rescisão do contrato com o a Serventia.

10 DISPOSIÇÕES FINAIS

O **1º Registro de Pessoas Jurídicas, Títulos e Documentos e Protestos de Goiânia**, possui controle de acesso às informações através de: Acesso com login e senha, biometria, gravações de vídeo, trilhas de auditoria e monitoramento da equipe.

Todos os procedimentos executados por nossos colaboradores são documentados e estes recebem periodicamente treinamentos técnicos e comportamentais a fim de fomentar o correto uso de todas as ferramentas colocadas à sua disposição.

O Cartório possui além da presente política de segurança da informação uma política de privacidade disponível em domínio público a todos os interessados.

O Cartório possui Encarregado de Dados nomeado pelo Titular da Serventia para assegurar o livre acesso dos titulares de dados a seus dados pessoais ou sensíveis que também é responsável pela manutenção da SI apoiado pelo Comitê de Segurança da Informação.

O Cartório possui equipe de TI qualificada, bem como prestadores de serviço especializados na área, se mantendo operante na manutenção dos padrões

de segurança da informação, garantindo a proteção dos dados e a continuidade do negócio em caso de perda.

Sem prejuízo aos direitos legais, a Serventia se reserva o direito de alterar esta Política de Segurança da Informação de modo a refletir avanços tecnológicos, mudanças na legislação ou normas regulatórias e boas práticas. Por este motivo, estará sempre disponível para consultas.