POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

www.cartoriobgr.com.br
Avenida Ari Rocha, 4462, Centro.
CEP 64000-830 - Baixa Grande do Ribeiro/PI
Telefone (89) 9 9925-5345

SUMÁRIO

1. INTRODUÇÃO....3
2. OBJETIVOS....4
3. APLICAÇÃO....4
4. PRINCÍPIOS....4
5. DIRETRIZES GERAIS....5
6. PENALIDADES....10
7. PAPÉIS E RESPONSABILIDADES....10
8. GESTÃO DA POLÍTICA....12
9. VINCULAÇÃO AO ANEXO 01....12
1. ORIENTAÇÕES....13
1.1 EQUIPAMENTOS DE INFORMÁTICA - USO DA ESTAÇÃO DE TRABALHO/ NOTEBOOK.... 13
1.2 USO DA INTERNET....14
1.3 USO DE E-MAIL....14
1.4 SENHAS....15
1.5 MESA LIMPA....16
1.6 ADOÇÃO DE UMA CULTURA SEM PAPEL (SEMPRE QUE POSSÍVEL)....16
1.7 USO DE DISPOSITIVO TELEMÓVEL DE PROPRIEDADE DA SERVENTIA....16
1.8 SOCIAIS....17
1.9 CLIENTES....17
1.10 SEGURANÇA FÍSICA....18
1.11 GERÊNCIA DE SISTEMA INTERNO....18
2. DIRETRIZES DESTA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO....19
3. DISPOSIÇÕES FINAIS....20
3.1 RESPONSABILIDADE DOS COLABORADORES....20
3.2 DIREITOS DA SERVENTIA.... 21

1. INTRODUÇÃO

O Cartório do Ofício Único de Baixa Grande do Ribeiro tem como missão, servir com eficiência e agilidade de maneira que a excelência da prestação do serviço impressione o usuário.

O Cartório entende que a informação é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus clientes.

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

Dessa forma, o cartório estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações do cartório ou sob sua responsabilidade.

2. OBJETIVOS

Declarar formalmente, por meio da alta direção (Tabelião) as diretrizes do **Cartório do Ofício Único de Baixa Grande do Ribeiro**, que visam à proteção dos ativos de informação e privacidade dos dados pessoais com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade, assim como dos Ativos de Tecnologia de Informação e Comunicação que as sustentam, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio.

Estabelecer as competências, responsabilidades e limites de atuação dos colaboradores do cartório, em relação à segurança da informação e privacidade, reforçando a cultura de segurança e priorizando as ações necessárias conforme o negócio.

3. APLICAÇÃO

Esta Política de Segurança da Informação é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela é aplicada a todos os empregados, estagiários, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores, clientes, menores aprendizes, ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as Informações e os Ativos do **Cartório do Ofício Único de Baixa Grande do Ribeiro.**

4. PRINCÍPIOS

Preservar e proteger a informação em todo o seu ciclo de vida, contida em qualquer meio, suporte ou formato, por qualquer ATIVO de propriedade, responsabilidade ou autorizado pelo cartório, dos diversos tipos de ameaça.

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

Estabelecer e definir as atribuições e responsabilidades do Comitê de Segurança da informação e privacidade visando alcançar os objetivos e estabelecer os controles

definidos pelo Cartório do Ofício Único de Baixa Grande do Ribeiro.

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

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

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

5. DIRETRIZES GERAIS

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

Publicidade: Está PSI e seus documentos complementares devem ser divulgados aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com o cartório, ou que, direta ou indiretamente, são impactados.

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

Propriedade Intelectual: É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, do cartório em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto, até mesmo no âmbito acadêmico.

Classificação da Informação: Os colaboradores devem utilizar apenas os recursos disponibilizados pela serventia para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte.

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

Uso dos Ativos: Os Ativos de propriedade do Cartório do Ofício Único de Baixa Grande do Ribeiro devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

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

Manutenção dos Ativos: Todos os Ativos em uso no ambiente corporativo do cartório devem atender às recomendações de seus fabricantes e desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.

Mobilidade: Os Ativos que permitem mais mobilidade ao colaborador devem ser utilizados somente quando fornecidos ou autorizados pelo cartório. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições do colaborador.

Ativos Particulares: O uso de Ativos Particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações do cartório deve ocorrer somente após solicitação formal e fundamentada do colaborador solicitante e autorização expressa do seu gerente e da TI.

Repositórios digitais: É vedado aos colaboradores o uso de repositórios digitais não homologados pela TI para armazenar ou publicar informações de propriedade ou sob a responsabilidade da serventia, salvo casos em que a informação esteja classificada como “pública”.

Softwares de comunicação instantânea: É vedado aos colaboradores a instalação e o uso de softwares de comunicação instantânea não homologados pela TI nos Ativos do cartório

Mídias Sociais: A participação do colaborador nas mídias sociais por meio dos Ativos da serventia deve ser realizada de acordo com controles estabelecidos em documento específico e estar relacionada às atividades profissionais.

O colaborador é responsável por sua conduta no uso das mídias sociais. Por isso,

cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade, etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.

Controle de acesso: O Cartório do Ofício Único de Baixa Grande do Ribeiro controla o acesso físico e lógico às suas dependências e aos seus Ativos. Desse modo, cada colaborador deve possuir um login e senha de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

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

Ambientes Lógicos: Os sistemas e processos que suportam os Ativos do cartório devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

Ambientes Físicos: O cartório deve estabelecer perímetros de segurança para proteção de suas propriedades, bem como implementar controles de identificação e registro de acesso em suas dependências para assegurar o acesso somente de colaboradores autorizados e ativos homologados.

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

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

Auditoria junto aos prestadores de serviço: Cláusulas contratuais que dispõem sobre a realização de auditorias eventuais ou periódicas para certificar a conformidade com a PSI e seus documentos complementares devem ser estabelecidas junto aos prestadores de serviço da serventia.

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

Documentação: O cartório deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus Ativos.

Salvaguarda (backup): A serventia deve definir e manter um processo de salvaguarda e restauração das informações e de seus ativos críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

Análise dos processos e Ativos: O cartório deve analisar, em intervalos regulares, seus processos e Ativos, visando assegurar que estes estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

Monitoramento: O Cartório do Ofício Único de Baixa Grande do Ribeiro realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, Ativos e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.

Inspeção dos Ativos: O cartório, sempre que considerar necessário, pode auditar ou inspecionar os Ativos que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os Ativos de propriedade de terceiros, quando autorizada a entrada em suas dependências, independentemente da interação com seus ambientes e informações.

Gestão de Configuração e Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica do cartório devem preservar os controles relacionados à disponibilidade, integridade, sigilo e autenticidade das informações.

Continuidade do Negócio: No escopo das ações de Segurança da informação e privacidade, os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação e

privacidade estabelecidos para proteção dos Ativos críticos.

Conformidade: A serventia deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

Capacitação: O cartório deve possuir pessoas capacitadas para exercer a Conscientização em Segurança da informação e privacidade para capacitação e disseminação da cultura de Segurança da Informação, proteção de dados e privacidade junto aos seus colaboradores.

Investimentos: Os investimentos em Segurança da informação e privacidade no cartório devem ser estudados e deliberados conjuntamente com o CSI, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

Comitê de Segurança da informação e privacidade (CSI): A serventia deve manter um Comitê de Segurança da informação e privacidade (CSI), cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da informação e privacidade, além de avaliar os controles, violação de dados pessoais e incidentes relacionados.

Equipe de Resposta a Incidentes: O cartório deve manter uma Equipe de Resposta a Incidentes em Segurança da informação e privacidade, com composição fixa ou variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação.

Comunicação de Incidentes: O Cartório do Ofício Único de Baixa Grande do Ribeiro deve possuir um canal de comunicação divulgado aos seus colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação e privacidade, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

Alterações: As alterações desta PSI e de seus documentos complementares devem ser devidamente comunicadas aos seus colaboradores pela serventia.

Exceções: As exceções que ocorram de forma exclusiva e excepcional a essa PSI, devem ser formalizadas e fundamentadas pelo colaborador solicitante, e podem ser revogadas a qualquer tempo, por mera liberalidade do cartório.

As medidas alternativas às previstas nesta PSI, realizadas de modo excepcional

para mitigar riscos em ocasiões específicas e justificadas, inclusive em situações emergenciais, devem ser formalizadas e fundamentadas pelo colaborador de forma imediata ou assim que possível ao CSI.

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

6. PENALIDADES

Violações: Os incidentes de segurança da informação devem ser avaliados pelo CSI,Cartório do Ofício Único de Baixa Grande do Ribeiro. Ao constatar uma violação, o CSI deverá avaliar o caso, podendo instaurar e apurar as responsabilidades dos envolvidos em procedimento administrativo disciplinar, visando aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, regimento pessoal e outros documentos normativos do cartório, além da legislação vigente.

6.1.2 Verificada a ocorrência de incidente com dados pessoais, o CSI consultará o encarregado previamente, para que a serventia promova à comunicação ao Juiz Corregedor do Tribunal de Justiça do Estado de Piauí no prazo de 24h conforme.

6.1.3 Sem prejuízo, os incidentes de segurança com dados pessoais serão imediatamente comunicados pelo CSI ao controlador.

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

7. PAPÉIS E RESPONSABILIDADES

Comitê de Segurança da Informação e Privacidade (CSI)

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

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

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

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

Tecnologia da Informação (TI)

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

Apoiar o CSI em suas deliberações;

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

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

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

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

Encarregado nomeado.

Periodicamente revisar as políticas geradas sob sua responsabilidade;

Receber da serventia as reclamações e sugestões e prestar assessoria técnica para que aquela forneça as devidas informações aos usuários;

Auxiliar tecnicamente a serventia nas respostas e comunicações entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Usuários

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

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

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

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

Recursos Humanos

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

Estipular controles de segurança e proteção de dados especificamente

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

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

Cabe ao RH entregar a PSI na ocasião da admissão do novo colaborador e colher assinatura no documento “Termo de Compromisso para colaborador interno” ou “Termo de Sigilo para Colaborador Interno”;

Realizar a guardar o documento na pasta funcional do colaborador;

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

8. GESTÃO DA POLÍTICA

A Política de Segurança da Informação é aprovada pelo Comitê de Segurança da Informação, em conjunto com o cartório, e o Oficial Eron da Silva Lemes Júnior.

9. VINCULAÇÃO AO ANEXO 01

A Política de Segurança da Informação é indissociável ao Anexo 01, o qual servirá para vinculação de comprometimento dos colaboradores.

ANEXO 01 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONTROLE DE FLUXO DE DADOS.

1. ORIENTAÇÕES

1.1 EQUIPAMENTOS DE INFORMÁTICA - USO DA ESTAÇÃO DE TRABALHO/ NOTEBOOK

1.1.1 Cada colaborador possui uma estação de trabalho, sendo de sua responsabilidade qualquer dano físico ao mesmo;

1.1.2 Cada estação possui um código interno que identifica o mesmo na rede (caso aplicável), significando que tudo que for executado nessa máquina é de sua responsabilidade;

1.1.3 O bloqueio de tela ou desligamento do computador ao se ausentar do local de trabalho é de sua responsabilidade;

1.1.4 Não instale software ou hardware sem autorização da equipe técnica ou da equipe de segurança;

1.1.5 Não tenha MP3, filmes, fotos, arquivos de âmbito pessoal, softwares de direitos autorais ou qualquer tipo de pirataria em seu computador;

1.1.6 Todos os dados e arquivos da serventia devem estar no local devidamente recomendado pelo Delegatário ou Interino;

1.1.7 A serventia atende clientes de forma remota, desta forma qualquer não conformidade que afete um cliente, referente a segurança da informação que tenha sido gerado pelo login de sua máquina, será de sua responsabilidade;

1.1.8 Utilizar programas “antivírus” disponíveis no sistema de rede, nos computadores e notebooks, periodicamente, conforme orientação da Serventia. Utilizar programas “antivírus” em todo e qualquer meio eletrônico de procedência externa;

1.1.9 Comunicar imediatamente a área de informática quando o programa “antivírus” identificar a existência de qualquer problema, abstendo-se do uso do computador até segunda ordem.

1.1.10 É proibido o uso das portas USB, Pen Drives, Mídias de CD/DVD para transferência de dados de dispositivos da Serventia para qualquer fim sem autorização expressa da diretoria administrativa e/ou de tecnologia e segurança.

1.2 USO DA INTERNET

1.2.1 Acesso a sites de conteúdo pornográfico, jogos, bate-papo (salvo os utilizados para comunicação interna e com os clientes), apostas e semelhantes está proibido;

1.2.2 O uso da internet poderá ser auditado ou controlado por um firewall ou dispositivo de rede conforme for definido pela equipe de segurança;

1.2.3 Fica restrito o uso da internet para downloads em torrent, vídeos e música;

1.2.4 Devem ser acessados somente dos sites que possuem relação com as tarefas e trabalhos do usuário, e o acesso aos demais sites, sejam de qualquer natureza, são proibidos.

1.2.5 A rede wi-fi será de uso exclusivo dos equipamentos pertencentes a Serventia que são instrumento de trabalho e o acesso à internet de dispositivos móveis de titularidade dos colaboradores serão feitos por meio de rede específica e devidamente autorizada pela Serventia e não se confundirá com a rede dos equipamentos de Serventia.

1.3 USO DE E-MAIL

1.3.1 Fica TERMINANTEMENTE PROIBIDO o envio de correspondências de interesse particular/pessoal dos colaboradores da Serventia através do e-mail oficial da serventia;

1.3.2 É, TERMINANTEMENTE PROIBIDO, a criação de e-mail em nome da Serventia, pelo colaborador ou por particular, sem autorização prévia, em qualquer domínio;

1.3.3 Não se deve abrir anexos desconhecidos, caso não se tenha certeza absoluta do conteúdo;

1.3.4 Desconfie de todos os e-mails com assuntos estranhos e/ou inglês. Os ataques de Phishing são uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos. Ransomware normalmente são enviados por e-mails de forma abstrata. Sempre que você desconfiar que um email pode ser fraudulento ou conter conteúdo

malicioso por favor avise imediatamente diretoria administrativa e/ou de tecnologia e segurança da Serventia;

1.3.5 O envio de e-mail marketing deve ser feito de forma coerente e sempre supervisionado e alinhado com o setor responsável. O uso incorreto de plataformas de envios de e-mail marketing e domínios da Serventia podem causar sérios danos a entregabilidade de emails para nossos clientes.

1.3.6 O e-mail da Serventia é usado exclusivamente para trabalho ou treinamentos da Serventia, não podendo ser utilizado para fins pessoais.

1.4 SENHAS

1.4.1 Uma senha “segura” deve conter no mínimo 8 caracteres alfa numéricos, com diferentes caixas (alta/baixa). Poderá conter símbolos e caracteres especiais na medida do possível;

1.4.2 As senhas terão um tempo de vida útil determinado pela equipe administrativa e/ou de segurança da Serventia, devendo a mesma ser respeitada, podendo ser cancelado os acessos aos sistemas da mesma;

1.4.3 Sempre utilize a autenticação de dois fatores (caso aplicável) quando disponível nas ferramentas digitais fornecidas pela Serventia para seu trabalho. A autenticação de dois fatores dificulta o acesso não autorizado de pessoas mal intencionadas a informações confidenciais da Serventia através do envio de códigos via SMS ou e-mail corporativo.

1.4.4 Cada colaborador é responsável por sua senha e jamais deve passar a outros;

1.4.5 Tudo o que for executado, instalado ou tratado por sua senha é de inteira responsabilidade sua;

1.4.6 Caso um cliente solicite a criação de uma senha que não esteja dentro da PSI da Serventia, o fato deve ser registrado no sistema interno, com a data/hora do ocorrido e nome do responsável.

1.5 MESA LIMPA

1.5.1 Você é responsável por sua mesa de trabalho, seja ela compartilhada ou não, a falta de cuidado com a área de trabalho pode levar ao comprometimento de informações pessoais e organizacionais. Senhas, dados financeiros, e-mails, dados sensíveis podem ser divulgados, impactando a privacidade ou diferencial competitivo. Um documento perdido contendo informação sobre o prazo de um contrato/proposta pode causar a perda de um contrato e redução na receita esperada. Então mantenha-a sempre organizada, limpa e sem anotações importantes de fácil acesso.

1.6 ADOÇÃO DE UMA CULTURA SEM PAPEL (SEMPRE QUE POSSÍVEL)

1.6.1 Documentos não devem ser impressos desnecessariamente, e lembretes com informações sensíveis e comprometedoras não devem ser deixados em monitores ou sob teclados. Lembre-se, mesmo pequenos pedaços de informação podem ser o suficiente para pessoas mal-intencionadas descobrirem aspectos de sua vida, ou dos processos da Serventia, que possam ajudá-los a comprometer informações.

1.7 USO DE DISPOSITIVO TELEMÓVEL DE PROPRIEDADE DA SERVENTIA

1.7.1 Utilizar os dispositivos móveis com os mesmos critérios de segurança que nas estações de trabalho/notebooks.

1.7.2 Definir senhas rígidas e autenticação usando digital quando disponível para liberação da tela e acesso aos principais aplicativos;

1.7.3 Toda e qualquer instalação de aplicativo deve passar pela autorização expressa da equipe de Tecnologia e Segurança da Serventia.

1.7.4 O aparelho deve ser usado somente com o Chip autorizado pela Serventia e em caso de envio para manutenção esse chip deve ser retirado.

1.7.5 É expressamente proibido passar a senha de acesso do celular para qualquer pessoa que não tenha autorização da Serventia.

1.7.6 A senha deveria ter no mínimo 10 dígitos com caracteres especiais.

1.7.7 Se houver cartão de memória o mesmo deve estar criptografado.

1.7.8 Todos os celulares corporativos devem estar com a opção de criptografia dos

dados habilitada.

1.7.9 Nenhum dado de âmbito pessoal deve ser salvo no celular e ele é de uso exclusivo para trabalho.

1.7.10 Deve ser usada autenticação em dois fatores em todos os aplicativos instalados nos celulares quando disponível.

1.8 SOCIAIS

Todos somos sociáveis e podemos nos tornar uma falha de segurança da Serventia. Desta forma, deve-se respeitar os seguintes tópicos:

1.8.1 Não diga sua senha para ninguém;

1.8.2 Não digite as senhas de acesso aos sistemas da Serventia em máquinas de terceiros ou fora dela;

1.8.3 Não libere acesso remoto ao seu computador para nenhum sistema externo, salvo com autorização da coordenação;

1.8.4 Não comente casos de clientes para pessoas que não fazem parte da equipe técnica;

1.8.5 Não passe informações de cliente por telefone ou bate-papos a terceiros;

1.8.6 Não passe informações de colaboradores internos por telefone ou mensagens instantâneas a terceiros.

1.9 CLIENTES

1.9.1 Nossos clientes e/ou usuários são nosso maior bem, por isso devemos seguir as seguintes políticas:

1.9.2 Não leve dados de clientes para fora da Serventia;

1.9.3 Não use mídias de clientes para fins pessoais;

1.9.4 Não divulgue qualquer informação de cliente para terceiros, excetuando se for por meio de um ato previsto em lei, a exemplo de certidão cartorária e/ou outros documentos públicos, devidamente autorizados;

1.9.5 Não libere acessos remotos para pessoas não autorizadas pelo(a) Delegatário(a)

1.9.6 Utilize políticas de senhas para o cliente, conforme já mencionado;

1.9.7 Sempre oriente o uso de produtos de segurança reativa ao cliente;

1.9.8 Não instale softwares não autorizados nas estações dos clientes;

1.9.9 Não instale softwares piratas ou maliciosos nos desktops dos clientes;

1.9.10 Relate no sistema interno de comunicação, dia e hora, e nome do responsável que não seguiu nossas orientações de segurança;

1.9.11 Aja de forma coerente e honesta com os clientes, sempre visando o melhor para o mesmo;

1.9.12 Oriente os clientes a manterem softwares de segurança atualizados na medida do possível;

1.9.13 Não ceda acessos indevidos a colaboradores.

1.10 SEGURANÇA FÍSICA

1.10.1 O acesso físico aos setores da Serventia são restritos aos colaboradores;

1.10.2 O acesso de um visitante a Serventia deverá sempre ser acompanhado por um colaborador.

1.11 GERÊNCIA DE SISTEMA INTERNO

1.11.1 Os usuários cadastrados nas ferramentas utilizadas pela Serventia devem apenas ser de colaboradores ativos e os demais devem ser removidos;

1.11.2 Toda e qualquer informação do cliente deve permanecer nas ferramentas utilizadas pela Serventia, não sendo fornecida a terceiros;

1.11.3 O usuário das ferramentas utilizadas pela Serventia é de uso do colaborador e intransferível, não devendo divulgá-lo para ninguém.

1.11.4 Ao compartilhar documentos nas ferramentas utilizadas pela Serventia, certifique-se que esse documento não está com permissões públicas e que somente pessoas autorizadas estão configuradas para visualizar ou editar o documento.

1.11.5 Mesmo internamente, tenha bom senso de quem pode editar uma informação e quem precisa somente visualizá-la para evitar qualquer tipo de manipulação de dados internos sem autorização.

2. DIRETRIZES DESTA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 Respeitar a privacidade de colaboradores, clientes e sociedade por meio de atividades de proteção dos direitos fundamentais de liberdade e de privacidade, seja em meio digital ou físico;

2.2 Ler e formalizar sua concordância com a Política de Segurança da Informação (PSI), além de anualmente participar de treinamentos e revisões de concordância com novas versões do documento;

2.3 Manusear informações da Serventia quando autorizado, informando e/ou respeitando o sigilo da informação e, quando necessário, efetivar o descarte da informação de modo a não disponibilizar a informação física ou digital para pessoas não autorizadas;

2.4 Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Serventia, seguindo práticas estabelecidas pela Serventia, de acordo com as rotinas de seu cargo e função;

2.5 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada pela Serventia;

2.6 Avaliar o risco de segurança da informação de suas atividades, operações e projetos a partir das interações com o responsável pela serventia;

2.7 Adotar controles de segurança da informação alinhado com o apetite de risco formalizado pelas áreas da organização e representante da Serventia;

2.8 Ser responsável por seus acessos aos ativos digitais e/ou físicos da Serventia;

2.9 Praticar o uso seguro de senhas, assim: não criar senhas fracas, não informar sua senha para outras pessoas, não escrever sua senha em papel acessível por outras pessoas e trocar sua senha periodicamente;

2.10 Ser responsável pela navegação de internet e uso de e-mail, não infringindo as políticas de segurança atribuídas a ela, como usuário de recurso tecnológico, utilizando de qualquer método alternativo que possa pôr em risco a rede de computadores e toda infraestrutura computacional e sistemas da Serventia;

2.11 Disponibilizar informações e acessos para auditorias com foco em segurança da informação, seja em ativo da Serventia ou ativos de terceiros regidos por contrato válido;

2.12 Comunicar imediatamente ao seu gestor qualquer descumprimento ou violação do item mencionado acima, por qualquer colaborador, inclusive ao que se refere a si próprio;

2.13 Buscar orientação através do gestor imediato em caso de dúvidas relacionadas à segurança da informação;

2.14 Os sistemas, as informações e os serviços utilizados pelos colaboradores são de exclusiva propriedade da Serventia, não podendo ser interpretados como de uso pessoal;

2.15 O uso das informações e dos sistemas de informação da Serventia podem ser monitorados, os registros assim obtidos poderão ser utilizados para detecção de violações da PSI e normas de segurança da informação e, conforme o caso, servir como evidência em processos legais.

2.16 Nos casos em que houver violação desta política ou das normas de segurança da informação, poderão ser adotadas sanções, como a possibilidade de desligamento do colaborador e eventuais processos criminais, se aplicáveis.

2.17 A área de Segurança da Informação da Serventia através desta política estabelece o alicerce das práticas de segurança da informação, ficando à disposição de colaboradores e entidades externas para eventuais dúvidas, alertas e pontos de melhoria da segurança e privacidade.

3. DISPOSIÇÕES FINAIS

3.1 RESPONSABILIDADE DOS COLABORADORES

3.1.1 Os dispositivos de acessos autorizados deverão observar as limitações e autorizações concedidas pela Serventia, sendo vedada a alteração de seus direitos de acesso por conta própria, ou transferi-los a terceiros;

3.1.2 É dever de todo colaborador proteger os dados dos clientes de qualquer acesso não autorizado e situações acidentais de compartilhamento de dados que possam afetar a privacidade do titular dos dados de acordo com a Lei Geral de Proteção de Dados Pessoais 13709/2018.

3.1.3 Garantir a:

3.1.3.1 Confidencialidade dos dados atentando-se para que a informação fique

compartilhada somente por pessoas autorizadas ou processos digitais que tenham autorização para tal;

3.1.3.2 Disponibilidade dos dados fazendo com que os mesmos fiquem acessíveis às pessoas ou processos autorizados no momento que for requisitado;

3.1.3.3 Integridade dos dados de forma que a informação seja acessada somente pelas pessoas ou processos que tenham autorização.

3.1.3.4 Manter sigilo de todas as informações de propriedade da Serventia que processa e utiliza, excetuando na prática de atos previstos em lei;

3.1.3.5 Todo usuário é responsável pelo conteúdo da sua correspondência eletrônica (e-mail) recebida e emitida, ressalvado que estas apenas deverão ser utilizadas para fins profissionais ligados às atividades da Serventia e também responsável por bloquear ou desligar sua estação de trabalho/notebook ao se ausentar do local de trabalho;

3.1.3.6 Comunicar imediatamente o seu gestor e a equipe de Segurança de Informação da Serventia, caso suspeite de violação da segurança da informação e proteção de dados e outras irregularidades no acesso a dispositivos técnicos da rede, bem como de processamento e/ou utilização de dados da Serventia, físicos ou não que possam comprometer a privacidade do titular dos dados, conforme a Lei Geral de Proteção de Dados Pessoais 13.709/2018. Se for comprovada a suspeita de violação, a Serventia tem todo o direito de verificação ou varredura em seu equipamento de serviço, com ou sem seu consentimento ou conhecimento.

3.1.3.7 É de responsabilidade de todos dentro da Serventia colaborar com a identificação e o tratamento de incidentes relacionados à segurança da informação.

3.1.3.8 As situações que não foram previstas neste documento deverão ser encaminhadas para o representante da serventia, assim possibilitando a avaliação e análise da área responsável para tratamento e possível contemplação em um novo normativo ou na alteração/inserção da política atual, a fim de determinar novas diretrizes a partir da data de sua aprovação pelo departamento responsável.

3.2 DIREITOS DA SERVENTIA

3.2.1 A Serventia se reserva ao direito de monitorar e rastrear todas as

informações e sites da internet acessados pelos equipamentos de informática, comunicação e telecomunicação, de sua propriedade, colocados à disposição de seus colaboradores;

3.2.2 A violação de quaisquer das determinações acima será considerada falta funcional grave, podendo resultar em ações administrativas disciplinares, bem como o colaborador poderá ser responsabilizado cível e criminalmente pelos atos praticados incorrendo nas penalidades previstas em lei.

CONTROLE DE REVISÕES

REVISÃO	DATA	HISTÓRICO DAS REVISÕES	APROVAÇÃO
01	20/08/2025	Emissão	Dr. Eron da Silva