Política de Segurança da Informação

Documento de Normas Administrativas

GSI – COGEL
V 1.0

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	19/01/2023	Lançamento da Primeira versão. Adequada a política, termos tecnológicos, comunicadores instantâneos, suporte usuários via VPN e LGPD.

Sumário

1. Sobre a Política de Segurança da Informação (PSI) 4

2. Conceitos e Definições 4

3. Objetivos da Política de Segurança da Informação 6

4. Aplicação da Política de Segurança da Informação 8

5. Princípios da Política de Segurança da Informação 8

6. Requisitos da Política de Segurança da Informação 9

7. Monitoramento e Auditoria.....12

8. Responsabilidades Específicas 13

8.1. Dos Usuários em geral 13

8.2 Dos Gestores/Gerentes 13

8.3. Dos Proprietários de Ativos de Informação 14

8.4. Da Gerência de Tecnologia da Informação 14

8.5. Do Comitê Consultivo 15

8.6. Da Assessoria Jurídica 16

8.7. Da Gerência de Pessoal.....16

9. Da Proteção de Dados Pessoais 18

10. Das Disposições Finais 19

1. Sobre a Política de Segurança da Informação (PSI)

A Política de Segurança da informação (PSI) é o documento que orienta e estabelece as diretrizes da PMS para a proteção do patrimônio da informação e prevenção da responsabilidade legal de todos os usuários. Consequentemente, deve ser respeitado e aplicado em todas as áreas do estabelecimento. Este plano segue a legislação vigente no Brasil e é baseado nas recomendações da norma ABNT NBR ISO / IEC 27002:2013, código de conduta mundialmente reconhecido para a gestão da segurança da informação. O objetivo é orientar os usuários na utilização dos ativos oferecidos, e na manipulação de dados e informações sensíveis.

2. Conceitos e Definições

Ativo: todo e qualquer bem da PMS que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado essencial para a PMS, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição.

Cavalo de Troia (*Trojan horse*): programa malicioso que cria abertura para outros programas e invasões indesejadas.

Código Executável: arquivo interpretado pelo computador como um comando de execução para determinadas funções.

Código Malicioso: programa que possibilita ações danosas, como vírus, worms, trojans, spywares, malware, botnet, ransomware, entre outros

Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de contrato de trabalho com a PMS (Exemplos: funcionários e estagiários).

Colaborador Externo: qualquer pessoa contratada por empresa terceirizada que execute alguma atividade profissional nas dependências da PMS, sem vínculo empregatício (Exemplos: consultores e prestadores de serviços).

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Comunicadores Instantâneos: aplicativos que permitem interatividade, troca de conversas e conteúdo em tempo real. Ex. WhatsApp, Telegram, outros.

Custodiante: quem detém a guarda da informação, mas não é necessariamente seu proprietário.

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa por meio de recursos tecnológicos, como publicações na internet e o envio de fotos e vídeos com mensagens ofensivas pelo celular ou qualquer outro dispositivo móvel.

Dados Pessoais: informação relacionada a pessoa natural/física identificada ou identificável.

Dados Pessoais Sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: garantia de que os usuários autorizados obtenham, sempre que necessário, acesso à informação e aos ativos correspondentes.

Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.

Informação Sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para a PMS.

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com a PMS com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte.

Peer to Peer*:* arquitetura de redes de computadores em que cada um dos pontos funciona como cliente e servidor possibilitando o compartilhamento de arquivos. Habitualmente são utilizadas para o compartilhamento de vídeos e músicas.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Spam: e-mails não solicitados e normalmente enviados para um grande número de pessoas.

Usuário: todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pela PMS.

Vírus: programa malicioso que se propaga e infecta o computador.

Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

3. Objetivos da Política de Segurança da Informação

- Estabelecer diretrizes e normas para que funcionários da PMS, prestadores de serviços, estagiários entre outros da PMS, sigam padrões de conduta desejáveis e aceitáveis, de acordo com a lei e as boas práticas mundiais, para mitigar riscos técnicos e jurídicos;

- Orientar a definição de procedimentos específicos de segurança da informação e a implementação de controles e processos para atendimento de seus requisitos;

- Proteger a confidencialidade, integridade e disponibilidade das informações da PMS;

- Prevenir possíveis acidentes e responsabilidades legais para a instituição e seus funcionários, prestadores de serviços, estagiários, etc.;
- Garantir a normalidade e continuidade das atividades da PMS, bem como, proteger os processos críticos de grandes falhas ou desastres;

- Cumprir os requisitos legais, regulamentares e contratuais relacionados às atividades da PMS;

- Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades da PMS resultante de uma falha de segurança;

- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;

- Garantir que todas as responsabilidades da Segurança da Informação sejam claramente definidas preservadas.

4. Aplicação da Política de Segurança da Informação

Todas as práticas aqui estabelecidas devem ser aplicadas em toda a rede e seguidas por todos os colaboradores, prestadores de serviço, estagiários, etc., para proteção das informações e utilização dos recursos tecnológicos.

Esta PSI obriga e responsabiliza cada usuário a manter-se informado sobre este documento e normas correlatas, e a buscar orientação de seu gestor ou da Gerência de Tecnologia da Informação caso não tenha certeza absoluta sobre a aquisição e/ou disposição das informações.

5. Princípios da Política de Segurança da Informação

Equipamentos de informática, de comunicação, os sistemas e informações devem ser utilizados para a realização das atividades profissionais, com responsabilidade e ética socialmente compartilhada e em conformidade com a lei.

Respeitar a privacidade dos utilizadores, agir de forma ética e cumprir os princípios da Lei Geral de Proteção de Dados Pessoais.

A PMS reserva-se o direito de monitorar e registrar o uso de toda e qualquer informação gerada, armazenada ou disseminada dentro da instituição. Para tanto, controles adequados, trilhas de auditoria ou registros de atividades são criados e implementados em todos os pontos e sistemas que a PMS julgar necessários para mitigar os riscos, levando sempre em consideração a ética e a legalidade, de forma a detalhar as operações dentro dos padrões de monitoramento de ativos.

6. Requisitos da Política de Segurança da Informação

A PSI deve ser comunicado a todos os funcionários, prestadores de serviços, estagiários, etc. e tem como objetivo aumentar a eficácia e a cultura autêntica de uso ético e lícito dos recursos técnicos e segurança da informação na PMS.

O Administrador do Contrato deverá notificar o GTI sempre que uma parceria ou vínculo empregatício com empresa terceirizada envolver acesso a informações e/ou recursos técnicos da PMS.

A PSI e as normas serão revistos e atualizados no mínimo anualmente ou sempre que surgirem novos fatos relevantes, com base nas análises e decisões do Comitê Consultivo.

Todos os contratos da PMS devem incluir um anexo ou cláusula de confidencialidade para garantir o acesso aos ativos de informação. Consulte a Política de
uso de ativos para obter detalhes.

A utilização do sistema PMS é restrita a usuários com conhecimento formal da PSI. Entre os alunos, a formalização deve ser feita de acordo com a Norma de Segurança da Informação Educacional.

As responsabilidades de segurança da informação devem ser atribuídas na fase de contratação para que sejam incorporadas e monitoradas durante toda a vigência do contrato.

Para empregados, prestadores de serviços, estagiários e demais empregados anteriores à publicação desta política que não tenham assinado os documentos correspondentes, o prazo de reconhecimento da PSI e a responsabilidade pela assinatura correspondente devem ser fornecidos em meio físico ou eletrônico.

Todos os funcionários, prestadores de serviços, estagiários e equivalentes que tenham acesso às informações da PMS devem ser treinados e estar cientes dos procedimentos de segurança e do uso adequado dos ativos fornecidos pela agência. O objetivo é minimizar os riscos potenciais à segurança, esclarecer as responsabilidades e informar os procedimentos de comunicação de incidentes.

Todos os requisitos de Segurança da Informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Serão criados e implementados também controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a PMS julgar necessário para reduzir os riscos dos ativos de informação.

O ambiente de produção e o ambiente de desenvolvimento técnico devem ser separados e rigorosamente controlados.

Planos de contingência e continuidade de negócios devem ser implementados e testados anualmente. O objetivo é reduzir o risco de perda de confidencialidade, integridade e disponibilidade dos ativos de informação por meio de uma combinação de medidas de proteção e recuperação. Estes planos devem, também, estar de acordo com o Plano Diretor de Tecnologia da Informação (PDTCI), e a Estratégia de Governo Digital.

Os ativos críticos ou sensíveis devem ser armazenados em áreas seguras, protegidas por perímetro de segurança definido, com barreiras de segurança adequadas aos riscos identificados, bem como controle de acesso, registro e rastreamento.

Qualquer ativo de informação deve ser protegido contra divulgação, alteração, furto ou furto por meio do uso de controles.

Regras e responsabilidades devem ser estabelecidas para a propriedade, armazenamento e relatórios de ativos de informação. Bem como definir os procedimentos específicos e responsabilidades para o uso e gestão dos ativos de informação fornecidos pela PMS off-site.

Todas as pessoas devem ser claramente identificadas. Sejam visitantes, estagiários, parceiros, colaboradores ou prestadores de serviços. Os dados coletados e armazenados devem ser segmentados para aplicar controles específicos e cumprir a legislação de proteção de dados aplicável. As regras para armazenamento e tratamento de dados pessoais também devem ser estabelecidas por regras específicas.

O uso de dispositivos móveis, assim como comunicadores instantâneos devem ser devidamente regrados em normativos próprios, atendendo sempre aos princípios da privacidade, respeito ao usuário e à necessidade da coleta de autorização, quando aplicável, devendo ser informado na Política de Privacidade, informações sobre as condições de tratamento.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação desta norma, ou ainda o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos de informação, o responsável e/ou solicitante deverá documentá-las imediatamente à GTI. Dessa forma será possível adotar medidas alternativas para minimizar riscos, bem como organizar um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

A PMS exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos aos usuários. Reservando-se o direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.

Esta atualização da PSI será implementada na PMS por meio de procedimentos específicos e obrigatórios a todos os funcionários, prestadores de serviços, estagiários e afins, independentemente do nível hierárquico

ou função na instituição.

Todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente à GTI, que, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Toda e qualquer atividade que não estejam tratadas nesta política ou normativos específicos, devem ser realizados apenas após consulta e autorização do gestor da área.

O não cumprimento dos requisitos previstos nesta PSI e nas Normas de Segurança da Informação acarretará violação às regras internas da instituição, e o usuário estará sujeito a medidas administrativas e legais cabíveis.

7. Monitoramento e Auditoria

Para garantir as regras mencionadas nesse PSI, bem como para fins de segurança e prevenção à fraude, A PMS reserva-se o direito de:

- Implementar sistemas de controle de acesso a estações de trabalho, servidores internos e externos, e-mail, navegação, Internet, dispositivos móveis ou sem fio e outros componentes de rede. As informações geradas por esses sistemas de monitoramento podem ser usadas para identificar usuários e seus acessos;
- Fazer inspeção de dos arquivos na rede, na unidade de disco local ou em qualquer outro ambiente para garantir o cumprimento estrito deste PSI
- Instalar sistemas de intrusão e vigilância para garantir a segurança dos dados e a segurança das utilizações;
- Instalar câmeras nas dependências.

Funcionários, prestadores de serviços, estagiários e outros entendem que o ambiente da organização, recursos de tecnologia, telefones, sistemas, computadores, dispositivos móveis e redes são sujeitos a monitoração e registros para cumprir a lei e a conformidade vigente.

O uso de dispositivos móveis pessoais está sujeito a regras próprias, porém, funcionários ou prestadores de serviços entendem que ao aceitar ou optar pelo uso de dispositivos pessoais para fins profissionais, a PMS poderá auditar e fiscalizar os recursos de TIC, a seu critério quando necessário, dentro de suas instalações ou interagindo com seu ambiente lógico, observando a não discriminação e à proporcionalidade devida, respeitando a razoabilidade e privacidade.

8. Responsabilidades Específicas

8.1. Dos Usuários em geral

Funcionários da PMS, prestadores de serviços, estagiários, etc. são responsáveis, em todos os níveis hierárquicos de sua esfera de responsabilidade, pelo cumprimento e zelar pela concretização e efetiva implementação das normas e princípios de segurança da informação. É dada especial atenção ao cumprimento das normas legais e éticas que afetem a PMS.

O Usuário assume total responsabilidade por qualquer perda ou dano causado ou sofrido pela PMS e/ou por terceiros em decorrência do descumprimento das diretrizes e normas aqui estabelecidas. O uso de senhas seguras também é de responsabilidade profissional e deve ser alterada de acordo com a periodicidade estabelecida pela PMS.

Cabe a todos os usuários as seguintes práticas:

- Cumprir fielmente as políticas, regras e procedimentos de segurança da informação, incluindo os contidos neste documento;
- Cumprir Decreto 34.915/21 e Instrução Normativa 02/2021, referentes ao uso e controle das ferramentas de e-mail;
- Cumprir a Instrução Normativa 10/2021 da SEMGE, referente a regras para uso de dispositivos computacionais;
- Procurar orientação de seu supervisor se tiver dúvidas sobre segurança da informação;
- Assinar o Termo de responsabilidade, expressando formalmente a consciência e a responsabilidade pelo cumprimento das normas nesse PSI e de segurança da informação;
- Proteger as informações contra acesso não autorizado, alteração, divulgação ou destruição não autorizada pela PMS;
- Assegurar que os recursos técnicos sejam utilizados somente para fins profissionais autorizados e em benefício da instituição;
- Garantir a segurança da informação sensível, incluindo todo e quaisquer dados pessoais a que tenham acesso;
- Cumprir à Leis Geral de Proteção de Dados Pessoais e proteger sempre os dados que forem acessados ou processados de acordo com as normas da PMS;
- Notificar imediatamente a GTI sobre qualquer descumprimento ou violação da PSI e/ou de suas regras e procedimentos

8.2 Dos Gestores/Gerentes

- Assegurar a implementação dos mecanismos necessários para a disponibilização segura da informação;

- Manter uma postura voltada para a Segurança da Informação e servir de modelo de conduta sob a orientação de colaboradores, prestadores de serviço, estagiários e outros que estejam sob sua gestão;
- Cumprir esta política, normas e procedimentos de Segurança da Informação;
- Garantir o acesso e conhecimento desta política e das normas e procedimentos nela estabelecidos;
- Inserir nos contratos com prestadores de serviços, clientes, terceiros e parceiros que necessitem de contato com informações da PMS, disposições sobre responsabilidade, proteção de dados pessoais, conhecimento da PSI e confidencialidade, exigindo o repasse das obrigações a seus próprios empregados e colaboradores;
- Solicitar permissão prévia para a GTI, apresentando listando os ativos de informação que serão fornecidos a terceiros
- Adaptar normas, processos, procedimentos e sistemas sob a responsabilidade do cumprimento da PSI;
- Observar e fazer cumprir as normas e leis relativas à proteção de dados pessoais;
- Relatar imediatamente quaisquer violações de segurança da informação, incluindo violações de dados pessoais, à GTI.
- Definir processos e normas, bem como manter manual atualizado, com os procedimentos para cópia e restauração de segurança, de sistemas e bancos de dados;
- Definir processos e normas, bem como manter manual atualizado, com os procedimentos para controle de acesso físico às dependências dos datacenters utilizados na PMS
- Definir processos e normas, bem como manter manual atualizado, com os procedimentos para controle de acesso lógico aos servidores, sistemas e banco de dados, em produção ou em homologação.

8.3. Dos Proprietários de Ativos de Informação

O titular da informação pode ser o gestor ou coordenador de determinada área ou projeto, sendo responsável por manter, revisar e descredenciar determinada informação ou conjunto de informações pertencentes ou sob o controle da PMS.

Cabe ao proprietário da informação:

- Criação de uma matriz de todas as informações sob sua responsabilidade, relacionando os cargos e funções da PMS aos direitos de acesso concedidos;
- Manter registros e controles atualizados de todas as permissões concedidas e decidir revogar imediatamente o acesso ou alterar as permissões concedidas, se necessário;
- Reavaliar as permissões conforme necessário e remover aquelas que não são mais necessárias;
- Cumprir e fazer cumprir os regulamentos e leis relativos à proteção de dados pessoais.
- Comitê de Segurança da Informação participará de reuniões, se solicitado, e fornecerá explicações, se solicitado.

8.4. Da Gerência de Tecnologia da Informação

A Gerência de Tecnologia da Informação (GTI) é responsável por gerenciar a implantação da tecnologia necessária ao bom funcionamento e prevenção dos negócios da PMS. Deve estabelecer uma equipe de segurança da informação para planejar e implementar medidas preventivas em caso de incidente, garantindo assim um maior nível de segurança.

Cabe à GTI:

- Apresentar as atualizações da PSI e das Normas de Segurança da Informação ao Comitê de Segurança da Informação para aprovação e posterior publicação;
- Propor as metodologias e processos específicos para a Segurança da Informação, como a avaliação de risco;
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da PMS;
- Promover com as demais gerencias a conscientização dos funcionários, prestadores de serviços, estagiários e afins quanto à relevância da Segurança da Informação para as atividades da PMS por meio de campanhas, palestras, treinamentos, entre outros meios;
- Apoiar a avaliação e a adequação dos controles específicos da Segurança da Informação para novos sistemas ou serviços;
- Desenvolver normas e regras específicas conforme à Lei de Proteção de Dados Pessoais;
- Promover adequação dos recursos técnicos e de infraestrutura necessários para atender à Lei de Proteção de Dados Pessoais;
- Indicar o encarregado pela Proteção de Dados Pessoais;
- Analisar criticamente incidentes com o Comitê Consultivo;
- Manter a comunicação efetiva com o Comitê Consultivo para mantê-lo informado sobre assuntos relacionados ao tema e que afetem ou tenham potencial para afetar a PMS;
- Outras responsabilidades devem ser formalizadas em norma específica.

8.5. Do Comitê Consultivo

O Comitê Consultivo deve ter um perfil multidisciplinar e contar com a participação de gestores de diferentes áreas da PMS.
Deve ser formado por um representante das principais instâncias da instituição, e entre elas a própria GTI. Pode, ainda, utilizar especialistas internos ou externos para apoiarem nos assuntos que exijam conhecimento técnico específico.
O Comitê Consultivo deve reunir-se formalmente, no mínimo, uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar algum incidente grave ou definição relevante para a PMS.

São atribuições do Comitê Consultivo:

- Recomendar investimentos relacionados à segurança da informação para maximizar a mitigação de riscos;
- Sugerir alterações na versão da PSI e acréscimos, exclusões ou alterações em normas complementares;
- Discutir e propor iniciativas para fortalecer, melhorar e sustentar a segurança da informação;
- Avaliar incidentes de segurança e sugerir ações corretivas;
- Discutir e sugerir ações apropriadas no processo disciplinar para violações de PSI e/ou normas suplementares de segurança da informação;
- Determinar de questões relativas à proteção de dados pessoais;

As atas e resumos das reuniões do Conselho Consultivo são de responsabilidade do GTI.

8.6. Da Assessoria Jurídica

A PMS, quando solicitado pela GTI, deverá contar com apoio jurídico para análise, parecer e estudo de casos. Para questões voltadas à tecnologia, como a Segurança da Informação, contratos de tecnologia, Proteção de Dados Pessoais, entre outros assuntos, a PMS deverá ter o apoio de equipe especifica voltada a assuntos jurídicos especializado em direito digital, que terá as seguintes funções:

- Dar apoio, respaldo e embasamento legal para ações voltadas à Segurança da Informação, à exposição na mídia, ao uso dos recursos tecnológicos e à proteção de dados pessoais;
- Acompanhar incidentes que envolvam saber jurídico
- Orientar a melhor forma de coletar e preservar uma prova eletrônica, com o propósito de manter sua eficácia para o uso em juízo, quando necessário;
- Elaborar e revisar documentos jurídicos relacionados a contratos de tecnologia e Segurança da Informação;
- Acompanhar o processo disciplinar, validando as sanções e exceções, quando houver;
- Revisar periodicamente e sugerir adaptações a esta Política e a normas de Segurança da Informação, de acordo com as necessidades e o perfil de incidentes causados ao longo do tempo;
- Analisar e adequar toda e qualquer regulamentação interna a fim de que esteja alinhada à Constituição Federal, ao Código Civil, ao Marco Civil da Internet e, à Lei Anticorrupção e à Lei de Geral de Proteção de Dados Pessoais;
- Analisar e promover o compliance a projetos de leis, quando aprovado, e que impactem nos negócios da PMS e no uso dos recursos tecnológicos e da legislação pertinente a sua área de atuação;
- Atender e propor demandas judiciais.

8.7. Da Gerência de Pessoal

Cabe à Gerência de Pessoal:

- Na fase de contratação de colaboradores, prestadores de serviços, estagiários, etc., atribuir responsabilidades pelo cumprimento da PSI e pela proteção de dados pessoais, formalizadas em contratos individuais de trabalho;
- Coleta o arquivamento de assinaturas de ponto responsabilizar e conscientização sobre as políticas e normas de segurança da informação dos profissionais já contratados;
- Fornecer notificação formal e imediata à GTI dentro de pelo menos 2 horas após qualquer mudança de pessoal, contratação, demissão, título ou mudança de cargo (Objetivo de revogar ou ativar acessos);
- Receber informações do GTI sobre violações de políticas e normas e incentivar processos comerciais e disciplinares quando apropriado;
- Apoiar e promover com a GTI ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais para todos os profissionais da PMS;
- Assegurar e promover a proteção adequada dos dados pessoais de acordo com os regulamentos internos e leis aplicáveis.

9. Da Proteção de Dados Pessoais

A PMS em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados de forma permanente como dados confidenciais.

Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11º da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.

O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados em norma específica, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva norma.

A classificação das informações deverá seguir o Decreto 8759/1990 que trata da classificação, conservação e destinação de documentos e informações, sob responsabilidade de cada órgão e setor da PMS.

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar a política de privacidade adotada pela PMS desde a sua concepção.

Além dos princípios mencionados, deverá ser elaborar um plano de resposta à violação de dados pessoais, elaborar o Relatório de Impacto sempre que necessário, utilizar processo de anonimização e pseudonimização sempre que necessário, fazer registro das operações de tratamento de dados pessoais, utilizar protocolos de criptografia na transmissão e armazenamento de dados pessoais, bem como implementar um sistema de gestão de dados pessoais.

10. Das Disposições Finais

As violações deste PSI e das Regras de Segurança da Informação estão sujeitas a medidas disciplinares que vão desde meras advertências até a rescisão temporária e ou permanente do contrato de trabalho.

O GTI poderá, a qualquer momento, bloquear temporariamente o acesso do usuário em caso de violação material das regras acima e comunicar os motivos ao Especialista e Gerente de Área.

O uso de recursos da PMS para atividades ilegais é motivo de demissão por justa causa, e o órgão cooperará ativamente com as autoridades. A PSI da PMS é complementada por regulamentos de segurança da informação que abrangem questões como o uso de e-mail, redes corporativas, Internet e proteção de dados pessoais. Sendo considerados parte integrante deste PSI.

Este PSI e as normas de segurança da informação estão disponíveis em documento interno em local de fácil acesso e com restrições de acesso.

Assuntos técnicos e confidenciais que requerem acesso por equipes ou indivíduos específicos podem ser disponibilizados apenas para indivíduos autorizados.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da PMS