RESOLUÇÃO DIREX Nº 50/2025

Aprova a Política de Segurança da Informação (PSI) da Agência Brasileira de Apoio à Gestão do SUS e dá outras providências.

A DIRETORIA EXECUTIVA DA AGÊNCIA BRASILEIRA DE APOIO À GESTÃO DO SUS - AgSUS, no uso das atribuições que lhe confere o art. 14, III, de seu Estatuto, e:

Considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados; e

Considerando o disposto na Lei nº 12.527 de 18 de novembro de 2011, denominada Lei de Acesso à Informação;

Resolve:

Art. 1º Aprovar a Política de Segurança da Informação - PSI da Agência Brasileira de Apoio à Gestão do SUS nos termos do Anexo Único desta Resolução.

Art. 2º A presente resolução entra em vigor na data da sua publicação.

ANDRÉ LONGO ARAÚJO DE MELO
Diretor Presidente

SUPER GOV.BR

Documento assinado eletronicamente por **Andre Longo Araujo De Melo**, **Diretor(a) - Presidente**, em 12/09/2025, às 12:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.agenciasus.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0098592** e o código CRC **133ABA0B**.

AgSUS

Agência Brasileira de Apoio à Gestão do SUS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

Sumário

APRESENTAÇÃO

Atentos ao contexto da sociedade atual, os dados possuem grande valor estratégico e econômico, pois permitem a tomada de decisões bem fundamentadas, alimentam os mais variados sistemas e ferramentas de trabalho, otimizando processos, melhorando a eficiência e eficácia dos serviços prestados. Ao possibilitar um aumento expressivo da produtividade, a segurança da informação é uma atividade prioritária nas organizações.

Inseridos no tempo, conhecido como a Quarta Revolução Industrial, em que sistemas inteligentes cooperam a nível global, ou seja, estão conectados, o cenário é de fusão dos meios físicos e digitais. E desse modo, ganham relevo um valioso instrumento com comunicação ubíqua, que impulsiona a inovação e a prestação de serviço com maior qualidade e cobertura, quais sejam, os dados, as informações, que transitam por diversos meios.
A internet das coisas, a inteligência artificial, o uso de Business Intelligence- BI, são instrumentos indissociáveis do processo produtivo moderno, onde a velocidade que impulsiona os mecanismos e a organização do trabalho vem acompanhada de evidente necessidade de regulamentação no ambiente corporativo.

Diante das vantagens proporcionadas pelo ambiente tecnológico, já mencionadas anteriormente, surgem também desafios e obstáculos, como os crescentes riscos cibernéticos, a busca contínua pela segurança dos dados tutelados e a proteção da informação. Para enfrentar essas questões, é indispensável implementar controles adequados de forma integrada, o que inclui a definição e estruturação de processos, a padronização de procedimentos, a organização da estrutura corporativa e o monitoramento constante desses controles.

Nesse sentido, a Diretoria Executiva da Agência Brasileira de Apoio à gestão do SUS - AgSUS, no uso das atribuições que lhe confere seu Estatuto apresenta a Política Segurança da Informação - Posi da Agência com a intenção de definir as regras e procedimentos a serem adotados para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, também observando os preceitos trazidos pela Lei Geral de Proteção de Dados – LGPD (Lei n. 13709/18).

Portanto, esta PSI deve apoiar e orientar a tomada de decisões institucionais e otimizar os investimentos em segurança que visem à eficácia e eficiência das atividades de tecnologia da informação, tanto no âmbito digital quanto físico.

Ademais, considerando-se as regulamentações relacionadas à proteção de dados pessoais, com destaque à Lei Geral de Proteção de Dados brasileira (Lei n. 13.709/2018), a AgSUS busca a constante adequação legal ao tema, objetivando a conformidade legal e o respeito à privacidade dos titulares de dados pessoais. Para tanto, deve sempre observar o disposto na lei de privacidade (e suas regulamentações), bem como realizar consultas prévias e demais planejamentos em conjunto com o Encarregado (DPO), quando desenvolver e implementar medidas relacionadas com a Segurança da Informação que envolvam o tratamento de dados pessoais.

1. ABRANGÊNCIA

A Política de Segurança da Informação - PSI é de observância obrigatória por todos os empregados e os Diretores da AgSUS, bem como aplica-se a todos que tenham acesso às informações custodiadas e de responsabilidade ou propriedade da AgSUS.

Esta Política estabelece princípios, diretrizes e normas para a implementação e o uso de todos os sistemas de Tecnologia da Informação - TI, bases de dados, dispositivos de rede, dispositivos móveis, sistemas financeiros e informações sensíveis, incluindo dados pessoais e operacionais. Isso compreende as informações em trânsito, armazenadas ou processadas em sistemas internos ou em nuvens públicas ou privadas, usadas pela AgSUS, por parceiros e/ou terceiros.

Com a observância desta política e do Programa de Integridade da Agência, quer a AgSUS a adoção de boas práticas e a proteção dos ativos de tecnologia de todos os dados tutelados e utilizados pela agência, sejam eles digitais ou físicos, nos sistemas críticos que impactam diretamente a prestação de serviços da AgSUS.

Os acordos de cooperação, contratos, convênios ou outros instrumentos celebrados com a AgSUS também devem observar o conteúdo desta PSI.

1.2 Base Legal

Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n. 13.709/18);

Práticas de mercado – Exemplo: ISO/IEC 27001;

Resolução CD/ANPD nº 18 de 16/07/2024.

2. PRINCÍPIOS

A Política de Segurança da Informação - PSI da AgSUS visa proporcionar maior segurança e estabilidade ao tratamento das informações que são tuteladas pela Agência, incluindo considerações relacionadas com as responsabilidades previstas pela LGPD, quando relacionadas com dados pessoais. Com essa perspectiva, são princípios norteadores da PSI AgSUS:

a) A disponibilidade da informação: que garante que as informações e sistemas da AgSUS estejam sempre acessíveis e utilizáveis quando necessários para as operações e os serviços prestados. Os planos de continuidade de negócios e recuperação de desastres devem ser implementados para assegurar a manutenção da disponibilidade, mesmo em situações adversas. Dessa forma, pode-se assegurar que as operações necessárias nas rotinas de trabalho da AgSUS sejam conduzidas de forma eficiente e sem interrupções;

b) A integridade da informação: que assegura que os dados estejam corretos e completos, sem alteração indevida, seja intencionalmente ou acidentalmente. Mecanismos de verificação e controle são aplicados para garantir que as informações permaneçam íntegras e precisas ao longo de seu ciclo de vida;

c) A confidencialidade: que garante que as informações sejam acessadas apenas por pessoas ou sistemas devidamente autorizados, protegendo-as contra acessos não autorizados e vazamentos. Aplicação de controles de acesso, como autenticação multifator e criptografia, para proteger dados sensíveis;

d) A autenticidade: que garante que as informações e as identidades são genuínas, ou seja, que as fontes de dados são verificáveis e que os remetentes das informações são de fato quem afirmam ser. Os métodos de autenticação (como assinaturas digitais, certificados digitais) são usados para garantir a autenticidade dos dados e transações;

e) A padronização e normatização das atividades de gestão de segurança da informação e comunicações: essencial para evitar discrepâncias e lacunas na proteção da informação. Com normas e padrões bem definidos, todos os departamentos e equipes seguem as mesmas diretrizes, o que resulta em uma abordagem coerente para a segurança e reduz o risco de falhas ou vulnerabilidades decorrentes da implementação desigual de medidas de proteção;

f) A confiabilidade: que assegura que os dados e sistemas de TI da agência são confiáveis, precisos e atualizados. Isso permite que decisões baseadas nas informações da AgSUS sejam feitas com confiança. A confiabilidade também envolve a garantia de que o ciclo de vida dos dados (desde a coleta até o descarte) seja feito de maneira segura e consistente;

g) O não repúdio: que garante que uma parte envolvida em uma transação ou comunicação não possa negar posteriormente que realizou essa transação. Tal princípio é crucial para eventual responsabilização de usuários por ações indevidas realizadas em sistemas da AgSUS. Para isso, serão utilizados mecanismos de auditoria e logs de eventos mantendo um registro detalhado e verificável de todas as operações realizadas, incluindo quem as executa e em que momento. Esses mecanismos registram ações críticas, como acessos, alterações e exclusões de dados, permitindo monitoramento contínuo e rastreamento de atividades. Com isso, é possível garantir a transparência e a integridade das operações, além de fornecer subsídios para correições, investigações e auditorias internas e externas;

h) A privacidade: deve AgSUS manter medidas rigorosas para proteger a privacidade das informações corporativas sigilosas, pessoais, especialmente as sensíveis sob sua custódia, visando minimizar os riscos de acessos, usos ou exposição de dados pessoais ou confidenciais. São norteadores deste princípio: a pseudonimização, substituindo informações identificáveis por dados artificiais ou códigos, de forma que a pessoa não possa ser identificada sem a utilização de informações adicionais mantidas em separado sob segurança rigorosa; e a anonimização que é o processo de modificar os dados de maneira que não possam mais ser associados, direta ou indiretamente, a um indivíduo, ainda que se tenham dados adicionais.

i) Agilidade de flexibilidade: Para ser bem-sucedida, a inovação deve ser parte da cultura organizacional. Isso significa promover um ambiente que incentive a automação dos processos, a experimentação de ferramentas e a aprendizagem contínua, além de ser flexível para adotar novas soluções. A velocidade com que novas vulnerabilidades e ameaças cibernéticas surgem exige que as organizações sejam ágeis na adaptação e implementação de tecnologias inovadoras para mitigar riscos rapidamente. A inovação não deve ser vista apenas como uma oportunidade de melhorar a eficiência ou os serviços, mas também como uma forma de reforçar a segurança. Tecnologias inovadoras devem ser incentivadas, mas de forma que não criem vulnerabilidades, novos riscos para os dados e a privacidade.

3. OBJETIVOS

O objetivo da PSI é estabelecer disposições gerais para garantir a segurança de dados da AgSUS, trazendo ferramentas para garantir a disponibilidade, confidencialidade, integridade, privacidade, autenticidade e a autoria (não repúdio) da informação.

A Direção, o Comitê de Segurança da Informação, o Responsável pela Segurança da Informação (CSO) e o Encarregado pelo Tratamento de Dados Pessoais (DPO), bem como todos os demais responsáveis pelas suas áreas de atuação dentro da Agência, estão comprometidos com uma gestão efetiva de Segurança da Informação na AgSUS. Desta forma, sempre buscarão adotar as medidas cabíveis para garantir que esta Política seja adequadamente comunicada, entendida, implementada e respeitada em todos os níveis da organização. Revisões periódicas (preferencialmente de forma anual) serão realizadas para garantir sua contínua pertinência e adequação às necessidades da AgSUS, incluindo a observação quanto às legislações aplicáveis.

Neste contexto, todos os envolvidos, direta ou indiretamente pela Segurança da Informação, devem buscar os seguintes objetivos:

a) divulgar interna e externamente, quando aplicável as normas e procedimentos de Segurança da Informação, garantindo que os requisitos essenciais de Confidencialidade, Integridade e Disponibilidade da informação da AgSUS sejam atingidos através da adoção de controles contra ameaças provenientes de fontes / fatores externos e internos;

b) orientar os treinamentos e a conscientização, de forma periódica, sobre as práticas adotadas pela AgSUS quanto às medidas de Segurança da Informação para todos os envolvidos no acesso e tratamento das informações sob responsabilidade da Agência.

c) tratar as vulnerabilidades e Incidentes de Segurança da Informação, para que estes sejam adequadamente identificados, registrados, classificados, investigados, corrigidos (incluindo, quando possível, medidas preventivas de mitigação ou prevenção), documentados, e, quando necessário, comunicando as autoridades apropriadas e/ou titulares, na forma da lei;

d) Garantir a continuidade do negócio através da elaboração, implementação, teste e melhoria contínua de planos de continuidade de negócios e recuperação de desastres.

4. DEFINIÇÕES

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Ativo de informação: patrimônio intangível da AgSUS, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a AgSUS por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico e/ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da AgSUS ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Confidencialidade: propriedade dos ativos da informação da AgSUS, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Disponibilidade: propriedade dos ativos da informação da AgSUS, de serem acessíveis e utilizáveis sob demanda, por partes e/ou sistemas autorizadas.

Encarregado (ou DPO – Data Protection Officer): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Incidente de segurança da informação: um evento, ou conjunto de eventos, indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações (ativos da informação) da AgSUS, ou sob responsabilidade desta.

Integridade: propriedade dos ativos da informação da AgSUS, de serem exatos e completos.

Pseudonimização: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Risco de segurança da informação: efeito da incerteza sobre os objetivos de segurança da informação da AgSUS.

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da AgSUS.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuário da informação: gestores, colaboradores, parceiros, empregados, prestadores de serviços e terceiros alocados na prestação de serviços a AgSUS, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da AgSUS para o desempenho de suas atividades profissionais.

Vulnerabilidade: causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações (ativos da informação) da AgSUS.

5. DISPOSIÇÕES GERAIS

5.1. Atuação e Responsabilidades do Comitê de gestão da Segurança da Informação, responsável pela Segurança da Informação (CSO) e do Encarregado pelo tratamento de dados pessoais (DPO)

5.1.1. Do Comitê gestor da Segurança da Informação

O Comitê Gestor da Segurança da Informação e, sempre que necessário, em conjunto com o departamento jurídico, atuam no desenvolvimento de políticas, normas e procedimentos de segurança para ajudar na proteção dos ativos da AgSUS.

Ademais, o Comitê dedicado ao planejamento, educação e conscientização sobre segurança. As responsabilidades específicas do deste incluem:

a. desenvolver, analisar, revisar periodicamente e propor a aprovação de políticas, procedimentos e normas relacionadas à Segurança da Informação, incluindo procedimentos de resposta a incidentes, sempre que necessário;

b. planejar e, em conjunto com a Alta Direção, buscar a garantia de disponibilidade dos recursos (humanos, materiais e financeiros) necessários para uma efetiva gestão de Segurança da Informação;

c. implementar, gerenciar, executar e fiscalizar as operações relacionadas à Segurança da Informação, tendo como base esta Política e as demais resoluções, normas internas e leis aplicáveis, em conjunto com todos os responsáveis e usuários;

d. implementar treinamentos e medidas que visem a divulgação e conscientização do conteúdo nesta Política, bem como demais documentos internos e legais relacionados, e gerenciar as ações necessárias para disseminar uma cultura de Segurança da Informação no ambiente da AgSUS.

e. monitorar, identificar, registrar e avaliar as principais vulnerabilidades e ameaças à Segurança da Informação, bem como propor e, quando aprovado, implementar medidas corretivas para gerenciar, reduzir/mitigar, evitar ou compartilhar riscos, conforme Resolução DIREX nº 22/2024;

f. executar o monitoramento e a gestão dos incidentes de segurança da informação, garantindo o tratamento adequado.

g. atuar de forma preventiva e corretiva, dentro de seu âmbito de trabalho, na adequação técnica, educação e conscientização quanto à segurança da informação durante o tratamento de dados pessoais.

O Comitê designado pelo diretor-presidente será também composto pelo Encarregado (DPO) que deverá se reunir de forma periódica para realizar suas tarefas preventivas e remediadoras, nos termos desta Política.

5.1.2. Responsável pela Segurança da Informação (Chief Security Officer – CSO)

O Responsável pela Segurança da Informação (ou também conhecido como Chief Security Officer – CSO) atua como o coordenador do plano de Segurança da Informação, bem como executar as ações relacionadas nesta Política e demais normativas relacionadas, sempre com o devido auxílio dos responsáveis das áreas da AgSUS, buscando as melhores práticas relacionadas à Confidencialidade, Integridade e Disponibilidade dos ativos de informação da AgSUS.

Ademais, deverá coordenar a análise, em conjunto com o Encarregado (DPO), da implementação e revisão periódica de medidas de Segurança da Informação relacionadas à adequação legal quanto às leis de proteção de dados pessoais aplicáveis (com destaque para a LGPD e seus regulamentos).

5.1.3. Da Alta Direção

A Alta Direção, como principal gestora, e responsável pela administração da Agência, deverá buscar analisar e implementar, em sua política de gestão, princípios, diretrizes e considerações relacionadas com a Segurança da Informação, visando atender aos previsto neste documento.
Ademais, a Direção, além de considerar o previsto nesta Política em suas ações de alta gestão, atuará em:

a. analisar e aprovar políticas, procedimentos e normas relacionadas à Segurança da Informação, incluindo procedimentos de resposta a incidentes, sempre apresentado pelo respectivo Comitê / Responsável;

b. planejar e buscar a garantia de disponibilidade dos recursos (humanos, materiais e financeiros) necessários para uma efetiva gestão de Segurança da Informação;

c. dar suporte aos Comitês e responsáveis, nos termos do previsto nas Políticas e normas legais, bem como aprovar, reprovar ou apresentar prazos para implementação de medidas de Segurança da Informação, sempre que estas não forem passíveis de implementação imediata, e/ou a curto prazo, considerando-se os recursos já existentes nos respectivos setores da Agência.

5.1.4. Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO)

O Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO) atua nos termos previstos na Lei Geral de Proteção de Dados pessoais (Lei n. 13.709/18 - LGPD) e demais normas relacionadas (tal como a Resolução CD/ANPD nº 18 de 16/07/2024).

As principais definições e atribuições do Encarregado (DPO) estão registradas na respectiva "CARTA DE NOMEAÇÃO DO ENCARREGADO PELA PROTEÇÃO DE DADOS PESSOAIS (DPO)", a qual deverá ser considerada como parte complementar desta Política.

Ademais, deverá dar suporte ao Comitê de Segurança da Informação, durante os processos de implementação e revisão periódica de medidas de Segurança da Informação relacionadas à adequação legal quanto às leis de proteção de dados pessoais aplicáveis (com destaque para a LGPD e seus regulamentos).

5.2. Atuação e Responsabilidades de outras áreas/funções

5.2.1. Usuários

É de fundamental importância que todos os usuários ativos da informação da AgSUS estejam cientes sobre os riscos, cuidados e as suas responsabilidades relacionadas à Segurança da Informação, sempre que acessarem e/ou utilizarem informações e dados sob responsabilidade da AgSUS. Assim, os usuários devem sempre estar conscientes e devidamente treinados, a fim de prevenir eventuais incidentes que possam acarretar algum tipo de risco ou danos às informações gerenciadas pela AgSUS.

As seguintes responsabilidades, não excluindo-se outras regulamentadas, são aplicáveis a todos os Usuários de ativos da informação da AgSUS:

a. acessar, inclusive mediante treinamentos regulares, compreender e cumprir integralmente os termos desta Política de Segurança da Informação, bem como as demais normas (legais e/ou internas) e os procedimentos de segurança aplicáveis;

b. solicitar eventuais esclarecimentos sobre esta Política de Segurança da Informação, proteção de dados pessoais, bem como as demais normas (legais e/ou internas) e os procedimentos de segurança aplicáveis ao Responsável pela Segurança da Informação (CSO) e/ou Encarregado (DPO);
c. comunicar ao Responsável pela Segurança da Informação (CSO) qualquer evento que viole esta Política e/ou coloque/possa vir a colocar em risco a Segurança das Informações ou dos recursos computacionais da AgSUS;

d. assinar termo de ciência desta Política da AgSUS, formalizando a ciência e o aceite integral das disposições desta Política de Segurança da Informação e termo de confidencialidade, quando aplicável, bem como as demais normas (legais e/ou internas) e os procedimentos de segurança e proteção de dados pessoais aplicáveis, assumindo responsabilidade pelo seu integral cumprimento;

e. responder pela inobservância desta Política de Segurança da Informação, bem como as demais normas (legais e/ou internas) e os procedimentos de segurança e proteção de dados pessoais aplicáveis, conforme definido no item sanções e punições (e demais disposições aplicáveis).

5.3. Da Gestão de Riscos

Para o êxito e sustentabilidade das atividades desenvolvidas pela AgSUS em um ambiente cada vez mais complexo e dinâmico é necessário que se realize uma gestão de riscos adequada ao Sistema de gerenciamento de riscos e controles internos publicados na Política de Gestão de Riscos, Resolução DIREX nº 22 de 12 de novembro de 2024. Essa prática permite identificar, avaliar, monitorar e mitigar potenciais eventos de riscos que podem comprometer os objetivos estratégicos estabelecidos, não apenas protegendo os dados tutelados, mas também, conquistando a confiança dos atores com quem se relaciona e promovendo a entrega de valor que se propõe.

Além disso, a gestão de riscos da AgSUS possui diretrizes e estruturas que promovem uma cultura organizacional integrada, onde todas as pessoas se sentem responsáveis pela identificação, monitoramento e controle de riscos. Isso não só aumenta a conscientização sobre os desafios que a organização pode enfrentar, mas também estimula a inovação e a melhoria contínua.
Não obstante, a gestão de riscos visa aprimorar a governança da AgSUS no auxílio às tomadas de decisões, bem como às ações de gestão estratégica, definindo o apetite de risco da instituição e os meios e instrumentos mais adequados para o tratamento dos potenciais eventos de riscos identificados e avaliados.

Para auferir esses benefícios da política, é necessário o uso de instrumentos que permitam a contínua identificação de riscos, que envolve mapear as fragilidades e ameaças que possam comprometer a segurança da informação. Nesse sentido, faz-se necessário prever, na construção do contexto de iniciação de programas, projetos e processos de trabalho ou ainda, no ato de elaboração da Matriz de Riscos, eventos de risco relacionados à segurança da informação provenientes de:

a) **Ameaças internas:** acessos não autorizados por colaboradores, uso inadequado de sistemas, falhas acidentais, negligência ou comportamento inadequado.

b) **Ameaças externas:** ataques cibernéticos, como phishing, ransomware, malware, e outras formas de intrusão. Há um foco especial para roubo de dados e sequestro de informações (ransomware), que podem gerar grandes prejuízos financeiros e de imagem institucional.

c) **Vulnerabilidades técnicas:** falhas em sistemas, softwares desatualizados, brechas de segurança em aplicações ou configurações inadequadas de rede.

d) **Dependência de terceiros:** riscos relacionados ao uso de fornecedores externos para serviços essenciais. A AgSUS utiliza diversos sistemas contratados, e essa dependência exige uma avaliação rigorosa da segurança dos fornecedores e suas infraestruturas conforme apresenta-se:

- Na fase pré-contratual deve-se atentar, na elaboração do termo de referência ou documento equivalente, para que os fornecedores que armazenam e processam dados da AgSUS devem garantir o mesmo nível de proteção exigido pela política de segurança da agência. Isso inclui a conformidade com a LGPD e os normativos internos, além de garantir que os dados não sejam expostos a vulnerabilidades. Deve-se também exigir garantias de disponibilidade e continuidade, de maneira que contratos com fornecedores externos devem incluir acordos de níveis de serviços (SLA) que garantam alta disponibilidade e continuidade dos sistemas, pois interrupções nos serviços contratados podem causar impacto nas operações da AgSUS. Outra necessidade corresponde a realização de uma avaliação de segurança de terceiros, ou seja, antes de qualquer contratação ou renovação de contratos de sistemas com terceiros, é obrigatório que a Unidade de Tecnologia e Informação - UTIC e o Comitê de Segurança da Informação realizem uma avaliação de segurança do fornecedor. Esta avaliação poderá incluir uma análise dos controles de segurança, auditorias de conformidade e revisões de vulnerabilidades.

- As medidas de mitigação específicas para a dependência de terceiros também incluem que as cláusulas contratuais sejam realizadas exigindo que os fornecedores adotem medidas de segurança robustas, como criptografia de dados, backups regulares e proteção contra ameaças cibernéticas.

- É necessário também que seja feito o monitoramento contínuo da segurança dos fornecedores, com revisões periódicas de conformidade e testes de segurança nos sistemas contratados, aplicando planos de contingência para garantir que, no caso de falhas nos serviços de terceiros, a AgSUS tenha alternativas para manter a continuidade das operações.

Por fim, deve-se destacar ainda que os controles preventivos e ações corretivas implementados para tratamento de riscos relacionados à sistemas e segurança da informação devem levar em consideração os princípios e diretrizes desta política.

5.4. Do uso aceitável dos ativos de informação e recursos de TI

Os ativos de informação e os recursos de TI só podem ser utilizados para as necessidades de negócios e com o propósito de executar tarefas relacionadas com a AgSUS.

Cada ativo de informação tem um proprietário designado, e este é o responsável pela Confidencialidade, Integridade e Disponibilidade das informações no ativo em questão, nos termos desta Política e demais documentos e leis aplicáveis.

Todos os recursos de TI estão sob responsabilidade do Usuário designado, e este deverá utilizar os recursos apenas para fins relacionados com as atividades vinculadas à Agência, bem como de forma ética, legal e preservando a sua integridade física e lógica / sistêmica (softwares e dados), nos termos desta Política e demais documentos e leis aplicáveis.

Quando do tratamento e utilização dos ativos de informação e recursos de TI, a AgSUS deverá projetar e disponibilizar sistemas e equipamentos adequados, atualizados e configurados visando a Confidencialidade, Integridade e Disponibilidade das informações, incluindo, dentre outros, softwares e hardwares de segurança (tais como firewall, Anti-malware, VPN etc.), sistemas de gerenciamento de cópias de segurança (backup), controles de gerenciamento de acesso / senhas e registro de logs.

Ademais, os Usuários deverão ser treinados e conscientizados quanto às medidas de segurança e governança, quando da utilização dos ativos de informação e os recursos de TI, incluindo, entre outros: política de mesa limpa, política de senhas, localização e forma de armazenamento de dados, bloqueio de telas, uso adequado de envio/recebimento de e-mails e demais tipos de mensagens, uso de recursos em áreas externas ao da Agência, regras quanto aos usos proibidos/restritos, respeito ao previsto nas leis aplicáveis (tais como a LGPD, MCI, etc.), entre outros a serem analisados e implementados.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Segurança e Uso Aceitável dos ativos de informação e recursos de TI.

5.5. Comunicação com Autoridades / Órgãos / Públicos Externos

Nos termos legais e normas internas, determina-se que qualquer comunicação externa relacionada à segurança da informação, que incluem, mas não se limitam, a entidades reguladoras, entidades de conformidade, governo, empresas terceiras vinculadas e titulares de dados pessoais, devem ser previamente autorizadas, e gerenciadas, pelo Responsável Pela Segurança da Informação (CSO) e/ou Encarregado de Dados Pessoais (DPO) (na hipótese de haver incidentes envolvendo dados pessoais).

5.6. Segurança da Informação no desenvolvimento e gerenciamento de novos projetos e tratamentos / utilização de ativos da informação

Visando a busca constante pela segurança e adequação integral no desenvolvimento de novos projetos, sistemas e modos de utilização de ativos da informação da AgSUS, todos os projetos devem incluir a análise e o gerenciamento relacionados à Segurança da Informação, e a observância das demais normas externas e internas aplicáveis, dentro do seu ciclo de vida. Esta análise e implementação de medidas visa identificar, avaliar e tratar adequadamente os eventuais riscos de Segurança da Informação e impactos à privacidade, em consonância com a Política de Gestão de Riscos da Instituição.

Ainda, com a orientação do Encarregado (DPO), deve-se buscar a permanente aplicação dos princípios de Privacidade desde a Concepção e por Padrão (Privacy by Design / Privacy by Default) em todos os projetos de novos sistemas / modos de utilização que envolvam o tratamento de dados pessoais.

5.7. Da Classificação da Informação

Visando à busca pela constante confidencialidade, integridade e disponibilidade dos ativos da informação, deverá ser implementado e mantido um sistema de classificação e gestão das informações (físicas e digitais) de acordo com o seu nível de confidencialidade. A limitação e controle de acesso adequado devem ser definidos de acordo com o previsto por normas externas, internas e/ou cláusulas contratuais.

Como parâmetro geral, os níveis de classificação a serem utilizados são: a) confidencial; b) restrito; c) interno e d) público. Estas classificações deverão ser ajustadas e registradas junto aos respectivos dados/ informações.

5.8. Do Controle de Acesso e Auditabilidade

Visando à busca pela constante confidencialidade, integridade e disponibilidade dos ativos da informação, todos os bancos de dados (físicos e digitais) e os sistemas de informação da AgSUS devem ser analisados e configurados de forma a estarem adequados aos parâmetros de controle de acesso regulamentados pelo Responsável Pela Segurança da Informação (CSO) e, quando aplicável, pelo Encarregado (DPO).

Ainda, de acordo com as regras previstas nas normas externas, internas e/ou cláusulas contratuais, deverá ser implementado um sistema segregação de funções (a ser revisado periodicamente), visando a concessão de acesso / tratamento de ativos da informação de acordo com a necessidade, nível de responsabilidade e/ou nível do cargo do Usuário.

Este sistema deverá efetuar verificações, controles e registros quanto: à autenticação de quem acessa (Usuário); autorização de acordo com o perfil pré-determinado e controle do que foi efetuado pelo Usuário, para fins de auditoria ("logs").

A definição de autorização de acesso e a segregação de funções relacionadas à informação, sistema e/ou área física serão definidas pelo responsável pelo ativo da informação, Responsável pela Segurança da Informação (CSO) e/ou Encarregado (DPO), de acordo com as regras previstas nas normas externas, internas e/ou cláusulas contratuais.

Ademais, visando a possibilidade de realizar auditorias quanto ao acesso e tratamento de dados e informações, bem como rastrear, investigar e registrar Vulnerabilidades e/ou Incidentes de Segurança da Informação, deverão ser implementadas medidas que visem o controle e registro detalhado dos acessos e dos atos praticados pelo Usuário ("logs").

Os "logs" devem ser armazenados de forma segura (sem possibilidade, ou de difícil possibilidade, de exclusão ou modificação), com acesso restrito e cópias de segurança atualizadas no menor prazo possível. Ademais, tais registros deverão estar disponíveis para consulta, mediante requisição e acesso aos Gestores / Diretores da Agência, e apresentados de forma legível e completa (informações apresentadas com "layout" de fácil análise / interpretação).

5.9. Das Senhas e demais medidas de segurança ao acesso de informações

Visando a efetiva implementação do controle de acesso aos sistemas e/ou dados, deverão ser implementadas medidas que impeçam, ou dificultem, o acesso por terceiros não autorizados.

O sistema de gerenciamento de senhas deverá ser implementado e configurado de forma a se prever, dentre outros: a) proibição de uso de senhas padrão (ex. disponibilizadas pelo serviço contratado ou de uso inicial) após o primeiro acesso / configuração; b) proibição de uso de senhas de baixa complexidade (ex. deve conter mínimo 10 caracteres e ao menos um caractere maiúsculo, uso de letras e números, bem como caracteres especiais); c) proibição de uso de senhas por prazos indefinidos (ex. definir um prazo de validade da senha configurada, especialmente aos acessos de sistemas / dados contendo dados pessoais e/ou sensíveis, em período de até 90 dias de validade, não podendo ser reutilizadas senhas anteriores); d) bloqueio de contas na hipótese de múltiplas tentativas de acesso de login fracassadas.

Ainda, treinamentos e conscientização aos Usuários quanto ao não fornecimento e/o compartilhamento de senhas de acesso se torna fundamental, visando o devido controle de acesso e de uso do Usuário registrado, haja vista a responsabilidade quanto ao seu login / senha individual e o uso destes.

Neste contexto, a AgSUS adotará múltiplos níveis de autenticação e autorização para garantir que apenas usuários autorizados possam acessar sistemas críticos, incluindo:

a) **Autenticação Multifator (MFA):** Implementada em sistemas sensíveis e de acesso crítico, para isso o usuário deve fornecer ao menos dois fatores de autenticação, como senha e um token de segurança ou biometria.

b) **Autorização baseada em função (RBAC):** a atribuição de permissões lastreia-se nas funções desempenhadas pelo empregado dentro da organização, assegurando que cada um tenha acesso apenas aos sistemas e informações necessários para o seu trabalho.

c) **Autenticação biométrica:** aplicável, a autenticação por meio de dados biométricos (como impressão digital) é utilizada para garantir um nível adicional de segurança.

Outras medidas de segurança, visando o controle de acesso a sistemas e/ou dados deverão ser analisados e implementados, a depender da estrutura e necessidade.

Ademais, medidas de segurança no âmbito físico também devem ser analisadas, revisadas e implementadas quanto ao acesso à ambientes controlados, especialmente quando conter dados pessoais, sensíveis e/ou sigilosos, tais como o controle de acesso por meio do uso de senha, chaves, biometria entre outros.

Visando um maior regramento e parametrização, o tema será regulado em Manual próprio.

5.10. Do armazenamento e eliminação

Devem ser observados aspectos relativos ao armazenamento de informações, a fim de se evitar a perda de acesso e/ou gerenciamento destes (de forma parcial ou total).

Quando da escolha e implementação de sistemas de armazenamento (locais ou externos), deverão ser observadas medidas jurídicas e técnicas. No âmbito jurídico, devem ser verificadas e/ou entabuladas cláusulas e/ou documentos que prevejam as responsabilidades e/ou medidas segurança disponibilizadas ao sistema sob análise.

No âmbito técnico, medidas relativas à segurança física, elétrica e/ou digital devem ser estudadas e implementadas, incluindo sistemas de prevenção de quedas de energia, criptografia, cópias de segurança e sistemas de gerenciamento e auditoria das informações tratadas, dentre outras.

Preferencialmente, todas as informações deverão ser armazenadas em sistemas centralizados (podendo ser mais de um), os quais podem ser monitorados, protegidos e gerenciados pela equipe técnica responsável. Armazenamento em sistemas isolados e/ou fora do ambiente controlado (tais como terminais de Usuários e/ou mídias externas) devem ser evitados e desencorajados.

Nas situações em que será necessária a eliminação de informações, medidas adequadas devem ser implementadas, visando que o ato seja efetivamente realizado, incluindo o uso de máquinas de fragmentação (ou similares) para impressos / documentos físicos e softwares específicos para a eliminação de dados no âmbito digital. Ademais, caso seja utilizado mídias removíveis, a formatação, realizada de forma adequada, e/ou a destruição física do objeto deverá ser efetuada antes do descarte.

O processo de eliminação de informações sempre deverá ser precedido por um processo de análise de temporalidade e observação quanto a eventuais guardas para fins que sobrepõe tais períodos, tais como registros históricos e/ou utilização em um procedimento judicial ou extrajudicial. O Responsável pela informação sempre deverá ser consultado antes da efetivação da eliminação.

5.11. Da cópia de segurança (backup)

Visando à busca pela constante Integridade e Disponibilidade dos ativos da informação, todos os bancos de dados digitais devem possuir um sistema de gerenciamento e controle de cópias de segurança (backup) ativo e periodicamente testado. Ainda, as cópias de segurança devem ser armazenadas, preferencialmente de forma criptografada, bem como em local seguro e com acesso controlado.

O sistema deve manter cópias dos dados / informações, preferencialmente, em tempo real (ou no menor prazo possível entre cada atualização, caso o instantâneo não seja viável) e em mais de um local, de forma simultânea. Ainda, sempre que viável, cópias de segurança locais e/ou em serviços de terceiros devem ser efetivadas sempre que houver a utilização de serviços “em nuvem”.

Ademais, visando a efetivação das cópias de segurança e a preservação de dados / informações, devem ser evitados e desencorajados os armazenamentos destes em sistemas terminais isolados (tais como os off line), incluindo HD’s não sincronizados em rede e/ou mídias removíveis, sem o devido mapeamento e gestão de cópias de segurança adequados.

No mesmo sentido, testes periódicos deverão ser realizados, tanto quanto a verificação da efetiva execução das cópias de segurança, quanto de sua recuperação.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política / Manual complementar sobre o tema.

5.12. Do compartilhamento de dados

Visando à busca pela constante Confidencialidade, Integridade e Disponibilidade dos ativos da informação, quando da necessidade de compartilhamento de dados, medidas jurídicas (tais como cláusulas contratuais e/o leis aplicáveis) e técnicas devem ser analisadas implementadas, visando segurança durante o processo de compartilhamento e o devido tratamento por parte de terceiros.

Quando ocorrer compartilhamento interno, as partes envolvidas deverão possuir a devida autorização de acesso (considerando-se o controle de acesso e a classificação da informação), bem como deverão ser utilizados sistemas adequados e configurados para se buscar a devida segurança do tratamento realizado.

Na hipótese de haver compartilhamento externo, medidas jurídicas deverão ser verificadas e/ou implementadas (autorização do responsável pela informação, cláusulas contratuais, exigência legal ou de Autoridade etc.). Ademais, medidas técnicas, visando a segurança durante o compartilhamento deverão ser analisadas e implementadas (tais como criptografia da informação e/ou da rede utilizada, softwares / ferramentas adequadas ao tratamento, contendo registros e controle de acesso, recibos identificados e com informações sobre o compartilhamento, devidamente datados e assinados etc.).

5.13 Da atualização de sistemas e softwares

Quando do desenvolvimento, contratação, utilização e/ou disponibilização de sistemas / softwares, seja no âmbito de produtos ou serviços a serem utilizados para a atividade fim da AgSUS, ou para o uso por parte de colaboradores / prestadores de serviços, a Agência deverá manter um gerenciamento de quanto a atualização destes, especialmente quanto às alterações / melhorias vinculadas às questões de segurança.

Ademais, os sistemas / softwares utilizados deverão ser periodicamente revisados, a fim de se analisar se há alguma vulnerabilidade, risco e/ou falta de suporte que possa vulnerabilizar Segurança de Informação da AgSUS.

5.14. Da Criptografia, Pseudonimização e Anonimização

Sempre que necessário e viável, de acordo com as regras previstas nas normas externas, internas e/ou cláusulas contratuais, e especialmente quanto aos Dados Pessoais tratados (nos termos legais aplicáveis), deve-se utilizar um sistema de criptografia robusta e/ou de pseudonimização dos dados pessoais, conforme os padrões aceitos pelo mercado, de modo a se buscar pela constante Confidencialidade, Integridade e Disponibilidade dos ativos da informação.

Ademais, sempre que possível, as informações deverão ser anonimizadas, eliminadas e/ou não armazenadas (não efetuar a coleta – atendendo ao princípio legal da necessidade previsto na LGPD), visando reduzir a probabilidade de ocorrência de um evento indesejado ou inesperado que pode causar danos, perdas ou interrupções, ou seja, os denominados, riscos de incidentes.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Gestão de Criptografia.

5.15. Da Segurança Física e do Ambiente

Visando a proteção dos ativos de informação contra danos, furto / roubo ou qualquer evento que possa gerar afetar a Confidencialidade, Integridade e/ou Disponibilidade destes, deve-se estabelecer e implementar medidas de segurança física, de modo a se gerenciar e controlar o acesso, preservação da estrutura e proteção física destes ativos (ex. sistemas de alarmes / monitoramento, CFTV, portas e janelas reforçadas, controle de acesso por senha / chave / similares).

No âmbito das estações de trabalho, deve-se adotar as políticas de “mesa limpa” (guarda de documentos impressos ou dispositivos em locais fechados tais com gavetas ou armários) e bloqueio de tela de computadores e dispositivos sempre que o usuário se ausentar do local (além do bloqueio manual, deverá ser configurado bloqueio automático da tela para no máximo 2 minutos de inatividade).

As medidas de segurança física, visando tanto a proteção dos dados e ativos quanto o controle de acesso e circulação de pessoas, deve ser estabelecida respeitando as normas legais quanto ao tema, incluindo a LGPD quanto ao que se refere ao tratamento de dados pessoais.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Segurança Física e do Ambiente.

5.15.1. Da utilização de sistemas CFTV e gravação de vídeos de segurança

Quando da utilização de equipamentos e/ou serviços de vigilância e acesso (próprio e/ou de terceiros), a AgSUS deverá analisar e armazenar informações técnicas, legais e jurídicas visando a verificação e resguardo quanto à segurança, governança e adequação legal do serviço a ser utilizado.

Aspectos relacionados à adequação legal do serviço (especialmente quanto as leis de proteção de dados pessoais), com destaque para pontos relacionados à eventual transferência internacional de dados pessoais, medidas de segurança adotadas/disponibilizadas (transmissão e armazenamento de imagens), ferramentas de gerenciamento de dados e acesso à documentos legais relacionados, devem ser obrigatoriamente observados pelas áreas responsáveis pela contratação, com a atuação e supervisão do departamento jurídico e do Encarregado (DPO).

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Segurança Física e do Ambiente.

5.16. Da Segurança nas Operações e nas Comunicações

O Responsável pela Segurança da Informação (CSO) e o Encarregado (DPO – quando aplicável) deverão desenvolver um conjunto de diretrizes e procedimentos que busquem a adequada e constante operação e comunicação dos sistemas e redes utilizados no processamento dos ativos das informações.

Estas diretrizes devem prever, dentre outros: os procedimentos de aquisição, instalação e configuração de sistemas; procedimentos para acesso e tratamento adequado da informação; procedimentos para a efetivação de cópias de segurança (backup) regulares e permanentes; procedimentos para gerenciamento de trilhas de auditoria; implementação, manutenção e atualização adequadas de softwares de segurança (ex. VPN, anti-malware, controle de vulnerabilidades e incidentes de segurança, etc.); e procedimentos de monitoramento, registros e prevenção de eventos.

Quanto à segurança nas comunicações, a Agência deverá buscar a análise e implementação de medidas que visem o tráfego protegido de informações, tanto no ambiente interno quanto externo. Ressaltam-se, como exemplos: verificação, restrição e/ou remoção de informações sensíveis, sigilosas, pessoais e/ou desnecessárias disponibilizadas na rede (especialmente externas e/ou públicas); redundância de sistemas de rede; a utilização de sistemas de criptografia nas redes (ex. TLS/HTTPS) e/ou enviar arquivos criptografados; instalação, configuração e utilização de sistemas de firewall; instalação, configuração e utilização de sistemas de anti-malware, anti-spam, filtros de e-mails; sistemas de filtro, gerenciamento e controle de tráfego de redes (respeitando leis de privacidade e trabalhistas, quando aplicável); controles de acesso por meio de senhas, dupla autenticação e/ou restrição de IP; etc.

Além disso, deve ser estabelecido um processo único de gestão de mudanças com o objetivo de controlar, e garantir, a autorização e documentação de toda mudança no ambiente.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Segurança nas Operações e nas Comunicações e/ou uma Política de Gestão de Mudanças.

5.17. Da Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação

Os procedimentos relacionados à aquisição, desenvolvimento ou manutenção de sistemas de informação, deverão ser efetivados e/ou solicitados pela área responsável, mediante análise (técnica e jurídica – incluindo a verificação quanto à devida adequação legal da Agência) e autorização prévia do Responsável pela Segurança da Informação (CSO) e, quando aplicável, do Encarregado (DPO). Ademais, devem ser efetivas análises, técnicas e jurídicas, quanto aos eventuais riscos relacionados à Segurança da Informação e/ou privacidade, bem como quanto aos seus tratamentos adequados, evidenciados a partir da aplicação dos instrumentos de execução da Política de Gestão de Riscos da AgSUS.

5.17.1. Da contratação e utilização de provedores de serviços digitais remotos (“em nuvem”)

Quando da seleção, contratação e utilização de serviços digitais remotos (“em nuvem”), deverão ser analisadas e armazenadas informações técnicas, legais e jurídicas visando a verificação e resguardo quanto à segurança, governança e adequação legal do serviço a ser utilizado.

Aspectos relacionados à adequação legal do serviço (especialmente quanto as leis de proteção de dados pessoais e demais normas relacionadas à atividade fim da AgSUS), com destaque para pontos relacionados à transferência internacional de dados pessoais, medidas de segurança adotadas/disponibilizadas, acordo de nível de serviço, cópias de segurança (backup), ferramentas de gerenciamento de dados e acesso à documentos legais relacionados, devem ser

obrigatoriamente observados pelas áreas responsáveis pela contratação, com a atuação e supervisão do Encarregado (DPO), nas hipóteses de haver tratamento de dados pessoais.

Os responsáveis devem verificar se os serviços possuem as características e ferramentas compatíveis com as políticas de segurança e gerenciamento da Agência, bem como ao nível de criticidade do tratamento demandando.

Ademais, preferencialmente, deve-se configurar e utilizar serviços de dupla autenticação de acesso / tratamento quando da utilização destes tipos de serviços.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação.

5.18. Do Gerenciamento de Dispositivos Móveis e Trabalho Remoto

Visando à busca pela constante Confidencialidade, Integridade e Disponibilidade dos ativos da informação, o Responsável pela Segurança da Informação (CSO) e o Encarregado (DPO – quando aplicável) deverão desenvolver um conjunto de diretrizes e procedimentos (Politicas, manuais, implementação de medidas e treinamentos) relacionados à Segurança das Informações, e a proteção aos dados pessoais, quando da utilização de dispositivos móveis e/ou quando da realização de trabalho remoto.

Estas diretrizes devem prever, dentre outros: os procedimentos de aquisição, ou autorização de uso, configuração e registro dos dispositivos móveis; proteção física; gerenciamento de licenças adequadas e/ou instalação de softwares e hardwares; gerenciamento de acesso à informações, de acordo com a classificação registrada; sistemas de dupla autenticação para acesso; controle e medidas de segurança relacionadas à rede utilizada para acesso a dados pela internet / nuvem (incluindo ajustes na rede utilizada e/ou softwares de criptografia, tais como VPN / TLS / HTTPS /etc.); cópias regulares de segurança (backup) controles de acesso e registro de atividades; e localização, bloqueio, eliminação de dados e/ou desabilitação de forma remota.

Quando do uso de dispositivos móveis, e/ou para trabalho remoto, deve-se, de forma preferencial, utilizar equipamentos próprios e exclusivos para tais fins, evitando-se, sempre que possível, a utilização de equipamentos de uso pessoal e/ou de uso misto. Caso tal medida não seja possível, configurações de segurança e gerenciamento, compatíveis com as diretrizes de segurança da Agência devem ser adotadas.

Os dispositivos móveis, e/ou para trabalho remoto devem ser analisados e configurados pela equipe responsável antes de sua utilização pelo usuário. Ademais, treinamento de segurança relacionados devem ser realizados de forma periódica.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Gerenciamento de Dispositivos Móveis e Trabalho Remoto.

5.19. Do desenvolvimento e utilização de ferramentas de geolocalização

Quando do desenvolvimento, utilização ou disponibilização de ferramentas, serviços e/ou dispositivos de rastreamento e/ou geolocalização, seja no âmbito de produtos ou serviços a serem utilizados para a atividade fim da AgSUS, ou para o uso por parte de colaboradores / prestadores de serviços, a Agência deverá analisar e armazenar informações técnicas, legais e jurídicas visando a verificação e resguardo quanto à segurança, governança e adequação legal do serviço / dispositivo.

Aspectos relacionados à adequação legal do serviço (especialmente quanto às leis de proteção de dados pessoais e no âmbito trabalhista / contratual), com destaque para pontos relacionados à eventual transferência internacional de dados pessoais, medidas de segurança adotadas / disponibilizadas (transmissão e armazenamento de dados pessoais), ferramentas de gerenciamento de dados e acesso à documentos legais relacionados, devem ser obrigatoriamente observados pelas áreas responsáveis pelo desenvolvimento e/ou contratação, com a atuação e supervisão do departamento jurídico e do Encarregado (DPO).

5.20. Da Gestão de Incidentes de Segurança da Informação

Visando a adequada e efetiva comunicação, gerenciamento, registro, correção e prevenção de eventos relacionados à segurança da informação (incidentes de segurança),será implementado um manual contendo os procedimentos de gestão de incidentes de segurança da informação, a qual será desenvolvido e gerenciada pelo Responsável pela Segurança da Informação (CSO) e pelo Encarregado (DPO – quando aplicável).

Caberá ao Responsável pela Segurança da Informação (CSO) e ao Encarregado (DPO), especialmente quando houver incidentes de segurança envolvendo dados pessoais, coordenar(em) todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação, incluindo, quando aplicável, a expedição de notificações a autoridades públicas e/ou titulares. Ademais, é dever de todos os usuários de informação comunicar um incidente de segurança da informação para área responsável.

Visando um maior regramento e parametrização, poderá ser desenvolvida uma Política de Gestão de Incidentes de Segurança da Informação.

5.21. Da Continuidade de Negócios

Visando à busca pela constante Confidencialidade, Integridade e Disponibilidade dos ativos da informação, bem como atender os requisitos legais para o devido tratamento de dados pessoais, a AgSUS poderá desenvolver e implementar um Plano de Continuidade de Negócios, a fim de prevenir e/ou solucionar situações que impeçam ou prejudiquem a correta efetivação das atividades fim e/ou acesso ao tratamento aos ativos da informação.

6. DA AUDITORIA E CONFORMIDADE

6.1. Da auditoria

A Unidade de Tecnologia da Informação ou Unidade de Integridade, por meio da coordenação de auditoria interna, poderão solicitar a realização de auditorias (internas e/ou externas) de segurança da informação para garantir que as políticas e procedimentos aqui estabelecidos estejam sendo seguidos e que os controles implementados sejam eficazes.

As auditorias têm como objetivo precípuo verificar a conformidade com as políticas internas de segurança e o cumprimento das mesmas, avaliar a eficácia das medidas de proteção de dados e segurança da informação e detectar vulnerabilidades que possam expor a organização a riscos.

6.2. Da Conformidade

Visando à busca pela constante adequação às obrigações legais aplicáveis, com destaque para as leis que regulamentam a atividade da Agência, de proteção de dados pessoais (LGPD e demais normas complementares aplicáveis), estatutárias, regulamentares ou contratuais, todos os gestores, colaboradores, prestadores de serviços, parceiros, empregados e demais pessoas envolvidas na utilização de ativos de informação da AgSUS, bem como os sistemas, bancos de dados e equipamentos utilizados devem estar em conformidade com o aplicável, incluindo a observância quanto à revisões periódicas.

7. DAS SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão e demissão do empregado.

A aplicação de eventuais sanções e punições será realizada conforme a análise do Responsável Pela Segurança da Informação (CSO), em conjunto com a Unidade de Gestão de Pessoas, Unidade Jurídica e a atuação direta e do Comitê de Segurança da Informação AgSUS, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas nas leis e demais normas internas aplicáveis.

No caso de terceiros contratados ou prestadores de serviço, deverá ser analisada a ocorrência e deliberação sobre a efetivação das sanções e punições conforme termos previstos em contrato e nas leis aplicáveis.

Para o caso de violações que impliquem atividades ilegais ou que possam incorrer em dano a AgSUS, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nesta política e/ou outras normas internas aplicáveis.

8. CASOS OMISSOS

Os casos omissos serão avaliados pelo Responsável Pela Segurança da Informação (CSO), em conjunto com a Diretoria da AgSUS, para posterior deliberação.

As diretrizes estabelecidas nesta política, e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças e/ou leis. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da AgSUS adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da AgSUS.

9. PROCESSOS E POLÍTICAS RELACIONADOS

Outros documentos, tais como políticas, manuais e registros complementares poderão ser criados e gerenciados pelo departamento de Compliance, equipe de Segurança da Informação, jurídico, Encarregado (DPO) e/ou outros departamentos da Agência. Tais documentos devem respeitar esta Política e as demais determinações legais aplicáveis, bem como serem disponibilizados para as partes envolvidas com o procedimento referido.

10. VIGÊNCIA

Esta política entra em vigor a partir da data de sua aprovação pela diretoria executiva da AgSUS.

11. ATUALIZAÇÕES DESTA POLÍTICA

A AgSUS pode analisar e revisar periodicamente as práticas, as políticas e os procedimentos de Segurança da Informação, inclusive esta Política de Segurança da Informação, preferencialmente de forma anual. Se forem feitas quaisquer alterações significativas, a AgSUS deverá:

a) tomar medidas razoáveis para informar, dentro do escopo adequado, a todas os setores e departamentos da AgSUS, colaboradores, parceiros de negócios, empresas parceiras, clientes e outros titulares de dados afetados pelas alterações; e

B) publicar avisos apropriados referentes às alterações nos sites relevantes – internos e externos, conforme apropriado.

AgSUS

Agência Brasileira de Apoio à Gestão do SUS

agenciasus.org.br

Setor Hoteleiro Norte, Quadra 1,
Bloco E, 2º Pavimento, Edifício
Sede CNP Asa Norte, Brasília - DF,
Cep 70701-050