CONASS
Conselho Nacional de Secretários de Saúde

REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA DO CONASS

Sumário

1 - INTRODUÇÃO

Este regulamento especifica os controles internos aplicáveis à segurança e ao sigilo da informação que fazem parte deste Conselho Nacional de Secretários de Saúde - CONASS, com o objetivo de prover a segurança necessária para realização de suas operações, ainda que em situações adversas.

Os termos de caráter mais técnico de Tecnologia da Informação ("TI") ou iniciados com letra maiúscula terão o significado definido no Glossário anexo à presente neste regulamento.

1.1. Público-alvo

Estão sujeitos ao disposto no presente documento todos os usuários, administradores, funcionários, prestadores de serviços e demais colaboradores do CONASS (individualmente "Colaborador" ou, em conjunto "Colaboradores"), no que a cada um for aplicável.

1.2. Revisão e Atualização

O presente documento foi elaborado e deve ser interpretado em consonância com os demais manuais e regulamentos do CONASS. Será revisado e atualizado área de Tecnologia da Informação anualmente, ou em prazo inferior, em função de mudanças legais/regulatórias ou se o CONASS entender necessário, a fim de incorporar medidas relacionadas a atividades e procedimentos novos ou anteriormente não abordados.

1.3. Responsabilidade

É de responsabilidade de todos os Colaboradores conhecer e cumprir todas as obrigações decorrentes deste Regulamento e regulamentações vigentes, bem como observar os mais altos padrões de conduta profissional ao conduzir suas atividades.

Também é dever de todos os Colaboradores informar e reportar inconsistências em procedimentos e práticas definidas no presente documento, seja para seu superior imediato e/ou para a Diretoria do Conselho.

2. OBJETIVOS E PRINCÍPIOS

2.1. Objetivos

Este Regulamento tem como objetivos:

(i) Permitir que o CONASS atenda à regulamentação, legislação e autorregulação aplicáveis;

(ii) Manter o nível de segurança da organização em um patamar definido como adequado pelo CONASS;

(iii) Garantir que as diretrizes explicitadas neste Regulamento sejam praticadas, por meio da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações.

Este Regulamento se aplica aos seguintes Ativos:

(i) Ativos de informação: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas etc.

(ii) Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

(iii) Ativos físicos: equipamentos computacionais (computadores, Servidores de Rede processadores, monitores, laptops, modems etc.), equipamentos de comunicação (roteadores, PABX, telefones fixos etc.), mídias (fitas e discos magnéticos, discos ópticos etc.), outros equipamentos técnicos (nobreaks, aparelhos de ar-condicionado etc.), mobília, acomodações etc.

Para atingir os objetivos acima listados, o CONASS estabelece o presente Regulamento como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os Ativos sejam protegidos de acordo com a sua importância estratégica para a organização.

O presente Regulamento se define como um documento que expressa a posição da organização sobre a segurança, quais são seus valores e direcionamentos para minimizar os riscos sobre seus Ativos. Desta forma ela estabelece a linha mestra de atuação do CONASS em relação a todos os aspectos da segurança da informação, incluindo equipamentos, bens, informações e pessoas.

2.2. Princípios

O Regulamento tem como princípios assegurar a:

(i) Identificação: garantir que qualquer indivíduo seja identificado unívoca e inequivocamente;

(ii) Autenticação: garantir que a identidade de cada pessoa ou recurso seja expressamente comprovada;

(iii) Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos Ativos;

(iv) Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles que possuam esse acesso como pré-requisito para o exercício de suas funções ou que sejam expressamente autorizados;

(v) Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição;

(vi) Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Com a finalidade de assegurar que os princípios acima sejam observados, o CONASS desenvolve as seguintes atividades:

(i) Classificação da informação:

a. Controle de acesso às informações;

b. Rastreamento e monitoramento.

(ii) Avaliação de risco:

a. Controle de mudanças;

b. Plano de contingência;

Segurança física dos dispositivos onde é armazenada e por onde transita a informação.

(iii) Testes de segurança e de continuidade dos negócios.

Este documento serve como um guia de melhores práticas definido pelo CONASS em relação à segurança da informação e tem o propósito de oferecer uma base comum de atuação para ser usado por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros Ativos que compõem o dia a dia da organização. O CONASS tem como compromisso assegurar que as orientações definidas neste Regulamento sejam seguidas por todos os Colaboradores.

Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo Ativos do CONASS, o usuário deve consultar este Regulamento para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida o usuário deve consulta sua Coordenação e/ou a Área de TI para assegurar-se que a atividade seja permitida. Cabe aos Coordenadores de área e pela Equipe de TI avaliarem os riscos das atividades não previstas nas diretrizes de segurança do CONASS, levando ao conhecimento da Secretária Executiva a prática de alguma dessas atividades.

3. DEVERES E RESPONSABILIDADES

As responsabilidades aqui citadas seguem o mapeamento de riscos, consultorias de TI e outros documentos correlatados do CONASS.

São deveres de todos os Colaboradores do CONASS no âmbito deste Regulamento:

(i) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

(ii) Cumprir o presente Regulamento, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

(iii) Utilizar os Sistemas de Informações do CONASS e os recursos relacionados somente para os fins previstos pela área de TI;

(iv) Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação;

(v) Manter o caráter sigiloso da senha de acesso aos recursos e sistemas, sem compartilhar

acessos e permitir usos por outras pessoas (“caronas”);

(vi) Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;

(vii) Responder por todo e qualquer acesso aos recursos do CONASS, bem como pelos efeitos decorrentes de acesso efetivado através de suas credenciais, ou outro atributo para esse fim utilizado;

(viii) Solicitar acesso a informações restritas somente quando houver real necessidade de acessar estes recursos;

(ix) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente, e;

(x) Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio verificado no âmbito do presente Regulamento, com a garantia que sua comunicação será tratada de modo sigiloso e sem identificação pública de que foi feita.

3.1. Responsabilidades dos Gestores de Áreas

(i) Gerenciar o cumprimento deste Regulamento, por parte de seus funcionários e prestadores de serviço;

(ii) Identificar os desvios praticados e adotar as medidas corretivas apropriadas, reportando a situação as suas Coordenações e a área de TI;

(iii) Impedir o acesso de empregados demitidos ou, se for o caso, demissionários aos ativos de informação;

(iv) Fornecer à TI informações sobre movimentação de funcionários em sua equipe (desligamento, contratação, transferência etc.) para que os responsáveis promovam a criação, modificação ou cancelamento da respectiva permissão de acesso;

(v) Proteger os ativos de informação e de processamento do CONASS;

(vi) Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger todos os ativos de informação do CONASS;

(vii) Comunicar formalmente a área de TI, concessão de privilégios a usuários de tecnologia da informação quais são os empregados e prestadores de serviço, sob sua supervisão, que podem acessar as informações do CONASS, e;

(viii) Comunicar formalmente a concessão de privilégios aos usuários de tecnologia da informação, quais são os empregados demitidos ou transferidos, para que a TI possa prosseguir com as respectivas exclusões no cadastro de usuários.

3.2. Responsabilidades da TI

(i) Estabelecer as regras de proteção dos Ativos do CONASS;

(ii) Revisar frequentemente as regras de proteção estabelecidas;

(iii) Restringir e controlar o acesso e privilégios de usuários remotos e externos;

(iv) Auxiliar a Secretaria Executiva do CONASS a elaborar e a manter atualizado o Plano de Contingência e manter a continuidade do Negócio;

(v) Executar as regras de proteção estabelecidas por este Regulamento;

(vi) Detectar, identificar, registrar e comunicar as chefias, violações ou tentativas de acesso não autorizadas;

(vii) Definir e aplicar, para cada usuário de tecnologia da informação, restrições de acesso à rede, como horário e dia autorizados, entre outras;

(viii) Limitar ao período da contratação o prazo de validade das contas de prestadores de serviço;

(ix) Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos;

(x) Solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários;

(xi) Excluir ou desabilitar as contas inativas;

(xii) Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;

(xiii) Garantir o cumprimento do procedimento de backup para os servidores e Ativos, e;

(xiv) Organizar treinamentos relacionados à segurança dos Ativos de informação periodicamente, com a finalidade de capacitar e avaliar os Colaboradores.

3.3. Responsabilidades inerentes ao "Compliance"

(i) Assessorar o CONASS na elaboração e verificação da legalidade dos Regulamentos, termos e controles utilizados para proteger os Ativos de informação;

(ii) Liderar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos do CONASS, ainda que auxiliado pela equipe de TI;

(iii) Assegurar que as atividades do CONASS sejam desenvolvidas com base nos princípios estabelecidos em seus Manuais/Regulamentos internos e em consonância com a regulamentação, legislação e autorregulação aplicável;

(iv) Dirimir ou mitigar ao máximo a existência de conflitos de interesse relacionados ao desenvolvimento das atividades do CONASS, especialmente, para fins do disposto neste Regulamento;

(v) Garantir a segregação física e lógica entre as atividades que necessitarem de segregação nos termos da regulamentação em vigor ou pelo nível de confidencialidade das informações que forem conduzidas pelas áreas do CONASS, por meio da restrição de acessos e da criação de perfis de usuários para a rede interna;

(vi) Elaborar e controlar o Regulamento de perfis e acessos do CONASS, inclusive quanto ao acesso a portas de transferência de dados, como USB, criando os perfis de acesso e designando-os a cada Colaborador de acordo com as atividades por ele desenvolvidas e com o cargo por ele ocupado;

(vii) Atualizar o Regulamento de perfis e acessos, bem como solicitar à área de TI a liberação ou o bloqueio de perfis de acordo com as necessidades verificadas ou sob demanda dos Colaboradores quando julgar pertinente;

(viii) Aprovar a criação ou exclusão de usuários quando houver contratação ou demissão de Colaboradores, sendo certo que os usuários novos devem ser cadastrados sem nenhum acesso, os quais devem ser solicitados posteriormente pela sua Gerência/Coordenação, e;

(ix) Para permitir que cumpra suas obrigações conforme as acima expostas, a TI possui acesso irrestrito a todas as dependências do CONASS, inclusive, a toda a rede interna.

3.4. Responsabilidade Jurídica

(i) Assessorar a Secretaria Executiva, na elaboração e verificação da legalidade dos termos, Regulamentos e controles utilizados para proteger os ativos de informação;

(ii) Garantir que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula de confidencialidade e que preserve a segurança das informações do CONASS, e;

(iii) Garantir que a existência das diretrizes estabelecidas com base neste Regulamento e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos com

terceiros, bem como nos contratos firmados com os Colaboradores do CONASS, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito desta Regulamento.

3.5. Responsabilidades Administrativas – SE/CONASS

(i) Executar as atividades de administração dos meios de informação não informatizados da organização, tais como: copiadoras, telefonia, controle de acesso físico, limpeza, arquivo, correio, mensageiros, impressoras, cabeamento, fragmentadores, salas de reunião, entre outros;

(ii) Distribuir as funções específicas de segurança dos Ativos de informação entre os integrantes de sua equipe;

(iii) Classificar os meios de informação não computadorizados que administra quanto à criticidade que representam, provendo as condições mínimas necessárias de continuidade, disponibilidade, integridade e legalidade desses meios, incluindo locais, serviços e equipamentos;

(iv) Executar as ações para proteger os ativos de informação sob sua responsabilidade;

(v) Administrar os serviços de proteção, limpeza, transporte, armazenamento e destruição dos ativos de informação;

(vi) Informar a área de TI situações em que haja vulnerabilidade quanto à proteção dos Ativos de informação;

(vii) Assessorar a área de TI, na criação, alteração e manutenção de novas normas, códigos ou regulamentos de segurança da informação;

(viii) Participar, quando cabível, na apuração das responsabilidades e causas relacionadas a incidentes ou violações da segurança da informação, e;

(ix) Divulgar e providenciar adesão dos novos Colaboradores, caso cabível, às normas, Regulamentos, códigos internos do CONASS, no ato da admissão.

3.6. Responsabilidades dos Prestadores de Serviço

(i) Respeitar as obrigações previstas nos respectivos contratos de prestação de serviço, especialmente, para fins desse Regulamento, no que tange à segurança da informação.

4. GESTÃO DA INFORMAÇÃO

4.1. Classificação da Informação

As informações, sejam itens, dados, conjuntos ou documentos que circulam ou são produzidas pelo CONASS são confidenciais por definição, salvo disposição interna ou regulação ou legislação que obrigue sua divulgação. Todo Colaborador deve zelar pela manutenção de níveis de confidencialidade adequados, e sempre que possível tornar a classificação adotada de maneira explícita, seja no desenho dos processos ou fluxos de informação, seja no próprio documento ou documentação daquele conjunto de informações. Todas as informações obtidas ou geradas pelo CONASS e terceiros são classificadas nos seguintes níveis:

(i) Confidencial: É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem do CONASS. São protegidas por rigorosos controles de acesso e criptografia.

(ii) Restrita: É o nível intermediário de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de Colaboradores. São protegidas por controle de acesso à módulos de sistemas e/ou diretórios em nuvem.

(iii) Uso interno: Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

(iv) Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

Abaixo uma tabela, não exaustiva, que lista alguns itens de informação em cada categoria:

Categoria de Classificação	Exemplos de itens, conjuntos ou elementos de informação
Confidencial	Planos de negócio, Documentos de apreciação para SE/CONASS, memorandos ou atas de reuniões restritas à Diretoria do CONASS, dados de Remuneração e Pessoais dos Colaboradores e Diretores, Documentos resultantes de Auditorias internas e externas, Documentos restritos de reguladores. Resultados de *Background Check* feito sobre Colaboradores e outros prestadores de serviço.
Restrita	Estratégias inerentes ao negócio do CONASS, Documentos de projetos sobre operações a serem realizadas ou em realização, documentos e dados pessoais de Colaboradores externos e documentos e dados pessoais de Colaboradores do CONASS.
Uso Interno	Apresentações internas das mais diversas, trocas de informações entre áreas, materiais de divulgação interna, Regulamentos e manuais não públicos, documentos e dados de processos internos.
Pública	Apresentações institucionais, materiais de divulgação, textos, documentos relativos que devem estar disponibilizados em sites públicos ou de forma pública nos sites do CONASS;

4.2. Manutenção do Sigilo da Informações

As seguintes regras devem ser observadas por todos os Colaboradores quando da utilização de informações confidenciais e/ou restritas:

(i) Os Colaboradores devem proteger a confidencialidade de quaisquer informações obtidas durante o exercício de suas funções no CONASS, que não devem ser, (1) divulgadas a terceiros, (2) divulgadas ou disponibilizadas em domínio público, (3) copiadas ou transferidas (mesmo que por foto) a celulares, tablets, computadores pessoais ou quaisquer outros dispositivos portáteis e/ou (4) enviadas para correio eletrônico (e-mails) externos, ainda que pertencentes ao próprio Colaborador;

(ii) A obrigação de sigilo prevista no item anterior, se aplica mesmo após a rescisão do vínculo do Colaborador com o CONASS, qualquer que seja a razão, permanecendo o Colaborador obrigado a manter sigilo e a proteger a confidencialidade das informações obtidas durante o exercício de suas funções no Conselho;

(iii) Os Colaboradores respondem individualmente, civil e criminalmente, pela divulgação indevida de Informações Confidenciais ou pela divulgação de quaisquer informações que tenham por objetivo atingir a honra ou a imagem do CONASS ou dissuadir seu relacionamento com os seus Colaboradores e o público em geral.

(iv) Questões envolvendo informações confidenciais e restritas de titularidade do CONASS não devem ser discutidas pelos Colaboradores em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes etc.

(v) Os programas de correio eletrônico (e-mails) disponibilizados pelo CONASS às pessoas autorizadas devem ser utilizados exclusivamente para mensagens de âmbito profissional e não podem, em hipótese alguma, ser usados para transmitir ou retransmitir mensagens ou seus anexos de qualquer natureza e conteúdo que possam comprometer o CONASS.

(vi) O CONASS adota a prática de mesas limpas. Todos os Colaboradores devem evitar manter papéis e documentos confidenciais expostos em suas mesas de trabalho. Documentos confidenciais devem ser guardados em local apropriado e com chave, mesmo no decorrer do expediente, para evitar o acesso de terceiros não autorizados. Ao final do expediente, as mesas devem permanecer sem papéis ou documentos, e gaveteiros devem ser trancados.

(vii) As informações confidenciais enviadas ou entregues ao CONASS para execução para tramitação são protegidas por lei. O compartilhamento destas informações com terceiros depende de expressa autorização da Secretária Executiva do CONASS por escrito.

(viii) Nas operações passivas do CONASS, em especial quando se tratar da distribuição de documentos confidenciais, quando aplicável, os Colaboradores devem firmar documentos específicos prevendo:

a. A obrigação de adotar a política de privacidade e confidencialidade de dados nestes documentos;

b. A garantia da devida observância deste Regulamento pelas pessoas a eles vinculadas;

c. Minimização de riscos de imagem para o CONASS, evitando que terceiros vinculem o CONASS a uma eventual falha na proteção das Informações Confidenciais.

(ix) O CONASS poderá revelar as informações confidenciais e restritas nas seguintes hipóteses:

a. Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

b. Aos órgãos de proteção e prestadores de serviços autorizados pelo CONASS a defender seus direitos e créditos;

c. Para outras instituições, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

4.3. Utilização de Conteúdo Protegido por Direitos Autorais

A maioria das informações e softwares que estão disponíveis em domínio público (incluindo a internet) está protegida por leis de Propriedade Intelectual, portanto:

(i) Não é permitido obter softwares, mídias e outros conteúdos destas fontes, exceto quando houver permissão explícita por parte do respectivo proprietário e autorização pela TI do CONASS;

(ii) Deve-se ler e compreender todas as restrições dos direitos autorais do conteúdo e, caso o CONASS não possa cumprir com as condições estipuladas, não faça download e não utilize o respectivo material;

(iii) É proibido o uso de qualquer foto, imagem ou desenho que possua marca registrada de terceiros. Podem ser utilizadas imagens originais do Sistema Operacional ou imagens não relacionadas a Produtos, Empresas ou Pessoas. Imagens consideradas agressivas também não devem ser utilizadas;

(iv) Em caso de dúvidas em relação às licenças ou a qualquer dos pontos acima, o Colaborador deve entrar em contato com área de TI do CONASS.

5. RECOMENDAÇÕES DE SEGURANÇA

5.1. Privacidade

O CONASS tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou "nuvem", que se encontrem fisicamente no mobiliário do escritório, como, por exemplo, em mesas, estantes, gaveteiros, armários etc. Dessa forma, ainda que o Colaborador possa se utilizar da estrutura de tecnologia da organização para algum uso particular não conflitante, tais informações podem ser acessadas pelo CONASS mesmo sem o prévio consentimento do respectivo Colaborador.

Com relação às mensagens de e-mail e outros canais de comunicação internos, o CONASS se reserva o direito de monitorar e armazenar registros destes.

Sem prejuízo do acima exposto, o CONASS se compromete a zelar pelo sigilo de qualquer informação, incluindo de caráter pessoal, que eventualmente se depare nos processos de monitoramento.

5.2. Proteção do Patrimônio Físico e Intangível

Integram o patrimônio físico e intangível do CONASS, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo eles serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos do CONASS para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vetada nos casos em que interfira no seu trabalho, ou se ainda:

(i) Interferir ou concorrer com os negócios do CONASS;

(ii) Fornecer informações a terceiros;

(iii) Envolver solicitação comercial ou outra solicitação não apropriada, e;

(iv) Envolver custo adicional para o CONASS.

5.3. Uso do E-mail

O uso do e-mail no CONASS está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. O e-mail não deve substituir uma conversa presencial ou um telefonema, quando este for mais eficiente. Mas pode e deve ser usado como documento de comunicação, interno e externo. Com isso em vista, seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização desta ferramenta:

(i) O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua conta e senha;

(ii) O uso da conta de e-mail corporativo do CONASS é somente, e somente só, para fins profissionais, sendo permitido seu uso pessoal com bom-senso, para assuntos que não sejam conflitantes com as atividades do CONASS nem que prejudiquem qualquer lei, regulação ou regimento e/ou Regulamentos internos do CONASS;

(iii) As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela;

(iv) Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e existência de prévia expectativa do recebimento da mensagem;

(v) Dentro do aplicativo ou visualizador de e-mails, devem sempre estar desabilitadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

(vi) Não deve ser utilizado e-mail para fins ilegais;

(vii) Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

(viii) Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

(ix) Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

(x) O Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

(xi) Não devem ser utilizados os serviços de e-mail para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa prejudicial;

(xii) Não devem ser transmitidas mensagens não-solicitadas, conhecidas como *spam* ou *junk mail*, correntes, *chain letters* ou distribuição em massa de mensagens não-solicitadas, salvo mensagens informativas de produtos e serviços do CONASS, aprovada pela chefia imediata, por lista controlada e via ferramentas oficiais contratas pelo CONASS. Quando este envio ocorrer, deve contar com sistema de cancelamento de cadastramento na própria mensagem;

(xiii) Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que se esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;

(xiv) O e-mail deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;

(xv) É proibido aos administradores de rede ou e-mail ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte, salvo por necessidade de apuração de eventos que tenham causado danos, ou tenham sido classificados como potencialmente danosos ao CONASS ou

a terceiros ou por determinações da Secretaria Executiva, desde que devidamente justificado, ou, ainda, de Reguladores ou Autoridades para apuração de eventos de infração de alguma regulação ou legislação, e;

(xvi) Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura de rede local ou que violem as leis de direitos autorais.

5.4. Uso do Telefone Fixo

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização destas ferramentas:

(i) O uso do telefone fixo no CONASS deve ter uso para fins profissionais. É permitido o uso para fins pessoais com bom-senso, para assuntos que não sejam conflitantes com as atividades do CONASS nem que prejudiquem qualquer lei, regulação ou regimento e/ou Regulamentos internas do CONASS.

(ii) Não se deve deixar mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas, e;

(iii) Ao coordenar uma teleconferência ou videoconferência, deve-se garantir que todos os participantes foram devidamente autorizados antes de começar a reunião.

5.5. Uso da Internet

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização da internet em dispositivos da organização ou na utilização de dispositivos pessoais na rede corporativa do CONASS:

(i) Alguns sites (páginas da internet) contêm ou distribuem material não apropriado ao ambiente de trabalho, portanto, os Colaboradores não devem acessar tais sites nem tampouco distribuir / obter material similar;

(ii) Os acessos a sites podem estar sendo monitorados a qualquer tempo, portanto, em caso de dúvida, deve-se verificar junto aos superiores imediatos ou o time de TI se o respectivo site pode ser acessado;

(iii) É permitido o uso de serviços de mensagens, chat ou Vídeo conferência (WhatsApp, Google Meet, Skype, Zoom, Microsoft Teams etc.) desde que para fins profissionais. O uso pessoal desses aplicativos deve ser limitado e com bom-senso, nunca com finalidades conflitantes com os interesses do CONASS, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e Regulamentos internos do CONASS. Vale lembrar também que todas as comunicações feitas em computadores do CONASS ficam armazenadas e podem ser consultadas pelo CONASS como determinam seus Regulamentos, bem como que o compartilhamento de qualquer assunto referente ao CONASS é expressamente proibido, sendo apenas autorizado com expressa comunicação da Secretária Executiva;

(iv) É permitido o acesso a redes sociais (Facebook, LinkedIn, X, Instagram, etc.), desde que com bom- senso, nunca com finalidades conflitantes com os interesses do CONASS, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e Regulamentos internos do CONASS. Vale lembrar também que todas as comunicações feitas em computadores do CONASS ficam armazenadas e podem ser consultadas como determinam seus Regulamentos. Vale lembrar que o compartilhamento de qualquer assunto referente ao CONASS é expressamente proibido, sendo apenas autorizado com expressa comunicação da Secretária Executiva*;*

(v) O acesso a e-mails não corporativos nos computadores de propriedade do CONASS é permitido, dentro do bom-senso, desde que não causem prejuízos à instituição e infrinjam as regras deste Regulamento;

(vi) Não é permitido o uso de compartilhadores de informações como redes peer-to-peer (uTorrent, BitTorrent etc.), também conhecidas como redes P2P dentro das dependências do CONASS;

(vii) Não é permitido o download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais;

(viii) É permitida a utilização de programas de *Streaming* de áudio nos computadores do CONASS, desde que com bom-senso, respeitando e priorizando o uso da infraestrutura de rede para fins profissionais e desde que sejam acessos lícitos e individualizados, e da mesma forma, o uso de programas de Streaming de vídeo, somente com aprovação expressa e limitada pelas Secretaria Executiva e equipe de TI do Conselho.

5.6. Uso das Impressoras

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização deste equipamento:

(i) Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

(ii) Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

(iii) As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pelo CONASS. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses do CONASS, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e Regulamento interno do CONASS, e;

(iv) Impressões coloridas apenas devem ser feitas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

5.7. Mesa Limpa

A prática de mesa limpa consiste em não deixar informações confidenciais ou bens do CONASS, incluindo, mas não se limitando a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.

Ao final do dia de trabalho, computadores portáteis devem ser devidamente trancados em gaveta ou armário, ou serem presos a cabos de segurança ou levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.

5.8. Tela Limpa

Computadores, notebooks e outros dispositivos devem estar protegidos por senha quando não estiverem sendo utilizados. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 5 minutos de inativação.

5.9. Senhas

O CONASS adota a prática de troca obrigatória de senhas com período de uso contínuo de no máximo 45 (Quarenta e cinco) dias.

A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

(i) Manter sua confidencialidade;

(ii) Criar senhas fortes, respeitando, ao menos, os critérios abaixo:

a. As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário), e;

b. Devem ter pelo menos 8 caracteres, com ao menos um caractere especial, uma letra maiúscula e um número.

Os acessos, validados por meio da utilização de senha do usuário, serão limitados aos recursos e serviços de rede necessários para o desempenho das atividades exercidas por cada Colaborador, e poderão ser revogados rapidamente quando necessário.

6. GESTÃO DA SEGURANÇA CIBERNÉTICA

6.1. Autenticação e Controle de Acesso

A prática de Controle de Acesso tem o objetivo de prevenir o acesso de indivíduos não autorizados aos ambientes e aos sistemas, garantindo assim a confidencialidade das informações.

Para garantir um nível aceitável de controle de acessos, são executados os seguintes processos:

(i) Controles de acesso são dados pela função, cargo ou setor, o que inclui equipes de Colaboradores;

(ii) Execução de procedimentos formalizados para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a segregação de função;

(iii) Todos os usuários são orientados a possuírem acesso apenas à informação de acordo com as necessidades de negócio;

(iv) É de responsabilidade do gestor cada equipe o informe do nível de acessos para novos Colaboradores. Os acessos são limitados aos ativos de informação sob domínio da equipe do gestor.

(v) Todos os procedimentos de Concessão e Alteração do Acesso dentro de uma equipe são aprovados pelo gestor responsável e pela área de TI;

(vi) Existem casos específicos de Colaboradores que necessitam de acesso aos ativos de informação pertencentes à outras equipes. Para estes casos, todos os procedimentos de Concessão e Alteração são aprovados pelo gestor responsável da equipe do colaborador, gestor da equipe detentora dos ativos de informação, Secretária Executiva e área de TI;

(vii) O CONASS realiza revisão de acessos, no mínimo anualmente, conforme Regulamento, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela TI, sendo o resultado da revisão enviado para a anuência da Secretária Executiva e Coordenações.

6.1.1. Serviços de diretório

Serviços de diretório desempenham um papel importante no desenvolvimento de aplicações intranet e Internet permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicações através da rede.

O CONASS utiliza 2 (dois) serviços de diretório em paralelo: um para o acesso interno aos equipamentos dos Colaboradores, Servidores de Arquivos e infraestrutura do escritório e outro para acesso aos serviços em nuvem. Os diretórios possuem sincronização ativa, logo, compartilham dos mesmos usuários, grupos, senhas e demais informações. Sempre que possível os sistemas adquiridos e desenvolvidos possuirão login integrado com o serviço de diretório local e em nuvem do CONASS, mantendo assim um canal único e centralizado de gestão de acessos.

6.1.2. Gerenciamento de Senhas e Acessos

O CONASS disponibiliza a todos os Colaboradores um serviço de acesso seguro, que é um meio ideal para armazenar e gerenciar informações confidenciais compartilhadas, como senhas, documentos e identidades digitais. O serviço é acessível apenas na rede interna do escritório ou via Rede virtual privada (VPN).

A ferramenta fornece controles de segurança preventiva e de investigação, através de fluxos para rotinas de aprovação e alertas em tempo real sobre os acessos. Permite ainda auditorias de segurança em conformidade regulamentar, como: Auditoria de Dados, Segurança de dados e Mascaramento de dados.

6.2. Controle Contra Software Malicioso

Os *malwares* de computador são programas desenhados para causar perda ou alteração de dados do computador, com isso em vista, todo equipamento do CONASS deve ter um programa antivírus instalado. Os softwares antivírus devem ser atualizados diariamente e de forma automática.

O Colaborador, ao receber alerta de vírus de qualquer fonte que não seja o antivírus, não devem acessá-lo ou encaminhá-lo a outras pessoas, pois geralmente estes alertas são falsos. De toda forma, permanecendo a dúvida, o Colaborador deve entrar em contato com a área de Tecnologia para maiores explicações e suporte técnico.

6.3. Atualizações

O Sistema Operacional, antivírus e demais sistemas devem permanecer atualizados. O sistema operacional dos equipamentos de Colaboradores deve permanecer com a atualizações automáticas sempre ativas, salvo casos específicos de compatibilidade de sistemas defasados ou testes em ambientes simulados.

6.4. Rastreabilidade

Todas as soluções, sejam elas adquiridas ou desenvolvidas, possuem geração ativa de logs de erros, eventos críticos, entrada e saída de informações relevantes, entre outros eventos. Esse registro pode ser utilizado para restabelecer o estado original de um sistema, para que um administrador conheça o seu comportamento no passado ou até mesmo para análise de auditorias internas e externas.

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

(i) Autenticação de usuários (tentativas válidas e inválidas);

(ii) Acesso a informações;

(iii) Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

6.5. Cópias de Segurança (Backup)

A importância dos backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas. Além disso, cada usuário tem uma pasta individualizada para uso profissional no servidor e/ou serviço de nuvem de arquivos.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de backup, e por isso o armazenamento nesses locais é de total responsabilidade do usuário.

O backup dos servidores de aplicações e bancos de dados ocorre diariamente por volta das 21h (horário de Brasília, GMT-3). As imagens mensais dos “Backups FULL” serão armazenadas por tempo indeterminado em fitas LTO.

Todos os e-mails, anexos e arquivos armazenados no diretório em nuvem possuem um serviço de backup a parte. O serviço monitora o volume de alterações nestes documentos e cria versões automaticamente. Todas as versões geradas permanecem armazenadas enquanto o serviço estiver contratado, por prazo indefinido.

6.6. Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

6.7. Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente ou sempre que houver mudança significativa na estrutura tecnológica. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

6.8. Segmentação de Rede

As definições de rede estão especificadas no Manual de Infraestrutura, e devem seguir as seguintes regras para garantia da segurança das informações nela trafegadas:

(i) Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;

(ii) Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;

(iii) Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de TI, que fará a análise, aprovação e execução da configuração.

6.9. Desenvolvimento Seguro

O CONASS mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

7. RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1. Contexto Geral

As respostas aos incidentes de Segurança da Informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, através do direcionamento na utilização dos recursos e procedimentos fundamentais, no intuito de garantir uma resposta efetiva.

7.2. Planejamento Estratégico

Esta atividade compreende identificar, prever e descrever situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já preestabelecidas. Assim, deve constar no planejamento:

(i) A definição de uma equipe de planejamento, suas responsabilidades e papéis predefinidos, para prever situações de sinistro e as possíveis respostas, assim como atuar no monitoramento e na resposta aos incidentes;

(ii) A definição do catálogo dos recursos tecnológicos existentes no parque do CONASS, bem como aqueles necessários para possibilitar uma atuação efetiva na resposta aos incidentes, como por exemplo: cadastro de todos os servidores;

(iii) O detalhamento das ações necessárias na resposta a incidentes, conforme o tipo e criticidade desses, deve abordar o tempo mínimo de resposta e a quem os incidentes devem ser reportados, entre outros.

(iv) Os casos que, em virtude de sua relevância, devem ser previamente autorizados pela alta gestão.

(v) Um Plano de Continuidade do Negócio atualizado, envolvendo os ambientes e processos críticos do CONASS, uma vez que processo de recuperação pode envolver o acionamento de um processo de continuidade do negócio, a fim de restabelecer a operação normal do CONASS;

As novas implementações para o ambiente tecnológico existente deverão ser adequadas a este Regulamento no prazo de 1(um) ano, a partir de sua publicação.

Caso não seja possível a adequação de alguma ferramenta ou componente, a equipe de TI dentro do planejamento deve documentar essa informação, bem como seus motivos, para fins de auditoria interna.

7.3. Identificação

Esta atividade compreende realizar ações para identificação e registro dos sinistros.

(i) Através dos recursos de detecção na rede, no monitoramento dos servidores e recursos de tecnologia ou através de problemas reportados pelos usuários, podem ser identificados alertas de

segurança que configurem incidentes de segurança. Diante disso, o a equipe de TI, com base no planejamento estratégico poderá ser acionada para que o alerta seja analisado e sejam tomadas as devidas providências, tanto no tratamento do incidente, quanto no encaminhamento do problema para os Gestores do CONASS;

(ii) Algumas situações podem ser consideradas na notificação de um evento de Segurança da Informação:

a. Violação da disponibilidade, confidencialidade e integridade da informação;

b. Inconformidade dos Regulamentos e/ou procedimentos;

c. Alterações de sistemas sem controle;

d. Funcionamento indevido de software ou hardware;

e. Violação de acesso lógico.

(iii) Eventos, mesmo que apenas suspeitos, devem ser analisados e validados rapidamente. Uma vez confirmada a ocorrência de um incidente, então a análise do escopo daquele incidente deverá ser executada. Essa análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes;

(iv) Todos os usuários são responsáveis por relatar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da Informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada por e-mail para a equipe de tecnologia;

(v) Nenhum Colaborador deve investigar por conta própria ou tomar ações para se defender de eventual ataque, a não ser que seja instruído pela equipe de TI para uma atuação em nível de minimizar o incidente.

7.4. Resposta

A atividade de resposta a incidentes de segurança da informação compreende reações aos possíveis ataques realizados.

(i) A partir de uma detecção de um incidente de segurança, é importante controlá-lo antes que uma possível extensão comprometa outros recursos. Como exemplo, tem-se uma infecção por vírus em um computador e que, se não for controlado em tempo, pode comprometer outros computadores da rede;

(ii) A estratégia de resposta ao incidente de segurança da informação a ser adotada deve ser baseada no tipo (ex: vírus, perda de arquivo, incêndio etc.) e na criticidade do incidente (ex: impacta na imagem ou nos negócios do CONASS, compromete várias áreas, entre outros);

(iii) Após a identificação e a confirmação que o incidente se trata de um evento de Segurança da Informação, ou seja, que viole a disponibilidade, a confidencialidade ou a integridade da informação, a resposta deverá ser realizada a partir das seguintes ações:

a. Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema, rastrear a possível causa e servir como evidência em eventuais questionamentos;

b. Verificar se existem planos de ação em que o sinistro identificado esteja previsto, no intuito de seguir o planejamento;

c. Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;

d. Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja permanente ou provisória;

e. Utilizar atividades de recuperação, tais como: a restauração de backups de sistemas, a instalação de patches, a alteração de senhas e a revisão da segurança do perímetro de rede do CONASS.

Quando as consequências do incidente estiverem contidas, é necessário que sejam removidos todos os componentes do incidente, como por exemplo: um código malicioso ou desabilitar contas de usuários violadas.

7.5. Vistoria

A vistoria consiste em ações realizadas após a ocorrência do incidente, como auditorias e análises de vulnerabilidade.

(i) É fundamental assegurar que as atividades envolvidas nas respostas aos incidentes sejam adequadamente registradas para futuras análises. Os registros servirão de banco de conhecimento para resposta em incidentes semelhantes;

(ii) De acordo com o incidente, uma análise mais aprofundada deve ser conduzida para identificar a origem do incidente para que o tratamento das fragilidades e/ou não conformidade encontradas contribuam para a resolução do incidente;

(iii) Periodicamente, a TI deve realizar uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las;

(iv) Após a identificação das possíveis vulnerabilidades, devem ser comunicadas às áreas responsáveis para as devidas tratativas. Após a resolução, deve ser encerrada a ocorrência e registrada as ações realizadas.

8. GESTÃO DE DADOS ANALÍTICOS NO CONASS

Este regulamento também estabelece diretrizes gerais para a gestão de dados analíticos no âmbito do Conselho Nacional de Secretários de Saúde (CONASS), visando promover a qualidade, segurança e eficiência na utilização dos dados para embasar decisões estratégicas no âmbito da saúde pública.

8.1 - Definições:

8.1.1. Dados Pessoais: Informações relacionadas a uma pessoa natural identificada ou identificável, como nome, e-mail, endereço, dados de saúde, entre outros.

8.1.2. Dados Sensíveis: Categoria especial de dados pessoais que requer proteção adicional, incluindo origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

8.1.3. Dados Analíticos: Informações coletadas e processadas para análise e geração de dados estratégicos no contexto do CONASS, incluindo, mas não se limitando a, dados pessoais e sensíveis quando aplicáveis.

8.1.4. Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

8.1.5. Tratamento de Dados: Qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

8.1.6. CONASS: Conselho Nacional de Secretários de Saúde, entidade representativa dos gestores estaduais de saúde do Brasil.

8.2. - Responsabilidades:

8.2.1. CONASS: Responsável por promover a gestão de dados analíticos garantindo recursos adequados, priorizando a qualidade dos dados e definindo estratégias para seu uso eficaz no âmbito do CONASS, em conformidade com a LGPD e demais regulamentações aplicáveis.

8.2.2. Área de Tecnologia da Informação (TI) do CONASS: Encarregada de implementar e manter a infraestrutura tecnológica necessária para a gestão dos dados analíticos, assegurando a segurança, integridade e disponibilidade dos dados, e monitorando o cumprimento dos princípios da LGPD.

8.2.3. Governança de Dados do CONASS: Estabelece políticas, processos e procedimentos para a governança dos dados analíticos, incluindo a definição de metadados, padrões de nomenclatura, classificação, acesso e os direitos dos titulares de dados pessoais.

8.2.4. Gestão de Dados no CONASS: Garante a qualidade dos dados analíticos, incluindo a coleta, transformação, limpeza e validação, bem como a documentação dos processos. Todos os dados

pessoais e sensíveis devem ser tratados de forma a garantir a sua segurança e conformidade com a LGPD.

8.2.5. Análise dos Dados no CONASS: Responsável pela análise, modelagem estatística e mineração de dados, visando extrair informações relevantes para suportar a tomada de decisões no âmbito do CONASS, assegurando que o tratamento dos dados seja realizado de acordo com os princípios da LGPD.

8.3 - Governança de Dados Analíticos:

8.3.1. Identificação e Classificação: Todos os dados analíticos no âmbito do CONASS devem ser identificados e classificados de acordo com sua natureza, fonte, sensibilidade e critérios de uso. Dados pessoais e sensíveis devem ser claramente identificados e receber proteção adequada.

8.3.2. Sobre os Metadados: Deve-se estabelecer um conjunto de metadados padronizados para descrever os dados analíticos, facilitando sua compreensão e reutilização, assegurando a rastreabilidade e a transparência no tratamento dos dados pessoais.

8.3.3. Qualidade de Dados: Devem ser adotadas práticas e procedimentos para garantir a qualidade dos dados analíticos, incluindo auditorias regulares, validação cruzada e controle de erros, assegurando a exatidão, integridade, autenticidade e atualização dos dados.

8.3.4. Acesso e Privacidade: O acesso aos dados analíticos no âmbito do CONASS deve ser restrito apenas a indivíduos autorizados e realizado com base na necessidade de conhecimento, respeitando as leis e regulamentos de privacidade de dados vigentes. Deve-se garantir o anonimato dos dados sempre que possível.

8.3.5. Segurança: Medidas de segurança adequadas devem ser implementadas para proteger os dados analíticos contra acesso não autorizado, uso indevido, vazamento, perda de integridade e quaisquer outras formas de tratamento inadequado.

8.4 - Processos de Gestão dos Dados Analíticos:

8.4.1. Coleta de Dados: Devem ser estabelecidos processos claros e padronizados para a coleta de dados analíticos, incluindo a definição de fontes de dados confiáveis e a documentação de metodologias de coleta. A coleta de dados pessoais deve estar de acordo com os princípios de necessidade, finalidade, adequação e transparência.

8.4.2. Transformação e Limpeza de Dados: Os dados analíticos devem passar por processos de transformação e limpeza para garantir a consistência, integridade e qualidade antes de sua utilização. Dados pessoais devem ser tratados de forma a minimizar a identificação direta dos titulares, aplicando técnicas de anonimização sempre que possível.

8.4.3. Análise e Geração de Dados Estratégicos: Realização de análises estatísticas e outras técnicas pertinentes para a extração de dados e informações relevantes dos dados analíticos, contribuindo

para embasar decisões estratégicas no âmbito do CONASS. A análise de dados pessoais deve ser limitada ao mínimo necessário para atingir as finalidades estabelecidas.

8.4.4. Os resultados das análises e informações derivadas dos dados analíticos devem ser compartilhados de forma adequada, preservando a confidencialidade dos dados pessoais e sensíveis e garantindo que o acesso aos resultados seja feito com base em políticas de acesso definidas e em conformidade com a LGPD.

8.5 - Direitos dos Titulares de Dados

8.5.1. Transparência e Acesso: Os titulares de dados têm o direito de acessar informações sobre o tratamento de seus dados pessoais, incluindo a finalidade do tratamento, a forma e a duração, bem como informações sobre o compartilhamento de dados com terceiros.

8.5.2. Retificação e Atualização: Os titulares têm o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.

8.5.3. Eliminação de Dados: Os titulares têm o direito de solicitar a eliminação dos dados pessoais tratados com o seu consentimento, exceto nos casos em que a manutenção dos dados seja necessária para cumprimento de obrigação legal ou regulatória.

8.5.4. Anonimização e Bloqueio: Os titulares podem solicitar a anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD.

8.5.5. Portabilidade: Os titulares têm o direito de solicitar a portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observadas as regras e procedimentos aplicáveis.

8.5.6. Revogação do Consentimento: O titular pode, a qualquer momento, revogar o consentimento para o tratamento de seus dados pessoais.

8.6 - Medidas de Segurança e Proteção de Dados

8.6.1. Controle de Acesso: O acesso aos dados pessoais deve ser limitado aos colaboradores que necessitem das informações para o desempenho de suas funções, mediante autenticação forte e registros de acesso.

8.6.2. Criptografia e Anonimização: Os dados pessoais devem ser protegidos por mecanismos de criptografia e, sempre que possível, devem ser aplicadas técnicas de anonimização ou pseudonimização.

8.6.3. Auditorias e Monitoramento: Devem ser realizadas auditorias regulares e contínuo monitoramento do tratamento de dados, para garantir a conformidade com as políticas internas e a legislação aplicável.

8.6.4. Gestão de Incidentes de Segurança: Procedimentos específicos para resposta a incidentes envolvendo dados pessoais devem ser estabelecidos, incluindo a notificação aos titulares dos dados e à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável.

8.7 - Disposições Finais

8.7.1. Divulgação e Treinamento: Este regulamento deve ser divulgado e disponibilizado a todos os envolvidos na gestão de dados analíticos no âmbito do CONASS. Todos os colaboradores devem passar por treinamentos periódicos sobre privacidade e proteção de dados.

8.7.2. Revisão Periódica: O regulamento será revisado periodicamente para adequações e aprimoramentos, conforme alterações na legislação ou nas atividades de tratamento de dados do CONASS.

8.7.3. Cumprimento: A adesão e cumprimento deste regulamento são de responsabilidade de todos os colaboradores envolvidos na gestão e utilização dos dados analíticos no CONASS. O não cumprimento poderá acarretar sanções disciplinares e legais.

9. CONTROLE E REVISÃO

9.1 Informações Gerais	
Título	*Regulamento Interno de Segurança da Informação e Segurança Cibernética*
Versão	FINAL
Status	Finalizado
Aprovadores	n/a
Data da Última Aprovação	n/a
Data da Próxima Revisão Obrigatória	01 (um) ano após a Data da Última Aprovação
Área Responsável pelo Regulamento	TI CONASS
Dispensa do Regulamento	n/a
Palavras-chave para Procura Rápida	Segurança, Informação, Cibernética, Tecnologia, Regulamento, Sigilo, Dados Analíticos, Gestão.

9.2 Histórico de Versões				
Versão	Motivo da Alteração	Data	Revisores	Departamento
V1.0	Versão Preliminar	14/06/2021	Adriano Salgado e Cleomar Dias	TI - CONASS
V1.2	Inclusão do Plano de Gestão de Dados Analíticos	04/05/2023	Adriano Salgado e Felipe Ferré	CONASS
V2.0	Alteração na redação do Plano de Gestão de Dados Analíticos	11/05/2023	Adriano Salgado	TI/CONASS
V2.1	Alteração na redação do Plano de Gestão de Dados Analíticos	25/05/2023	Adriano Salgado	TI – CONASS
Final	Ajuste no item 8, adequação para atender à LGPD	23/09/2024	Adriano Salgado e Cleomar Dias	TI/CONASS

Aprovado por:	Jurandi Frutuoso Silva
Data: 23/09/2024	**Secretário Executivo do CONASS**

10. GLOSSÁRIO

Os termos iniciados com letra maiúscula na Regulamento de Segurança da Informação do CONASS deverão ser interpretados com o significado a seguir:

Antivírus: programa que detecta e elimina vírus de computador.

Backup: cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamento ou para salvaguardar informações.

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

Controle de Acesso: conjunto de restrições ao acesso às informações de um sistema exercido pela equipe de segurança da informação.

Criptografia: arte/ciência de utilizar matemática para tornar a informação segura, criando um grande nível de confiança no meio eletrônico.

Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

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

Download: transferência de arquivo de um computador remoto para outro computador através da rede.

Ferramentas: conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Regulamento de Segurança da Informação das entidades.

Handheld: computadores que cabem na palma da mão (palmtops) e que tem recursos para organização pessoal e comunicação móvel.

Incidente de Segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Junk mail: e-mails não solicitados por usuários não interessados em recebê-los. Log:

registro das transações ou atividades realizadas em sistema de computador.

Nobreak: sistema com baterias, que mantém o computador funcionando por um determinado período.

Peer-to-Peer: rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdo e serviços à rede.

Regulamento de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos sistemas de informação.

Proteção dos Ativos: processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.

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

Senha Fraca ou Óbvia: senha que utiliza caracteres de fácil associação ao seu dono, que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome do usuário, nome de seus familiares, sequências numéricas simples, palavras com significado, dentre outras.

Spam: e-mail não solicitado enviado a grande número de endereços eletrônicos, que geralmente visam fazer propaganda de produtos e serviços.

Vírus: programa construído para causar danos aos softwares do computador.

Cavalo de Tróia (Trojan Horse): programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de hackers.

DECISÃO nº 011/2024 – DO SECRETÁRIO EXECUTIVO DO CONASS

Brasília, 23 de setembro de 2024.

Decide alterar o Regulamento Sobre Gestão de Tecnologia da Informação, instituído pela Resolução nº 014 de 02 de fevereiro de 2014.

O Secretário Executivo do Conselho Nacional de Secretários de Saúde - CONASS, no uso de suas atribuições que lhe confere o Estatuto do CONASS de 1º de novembro de 2023 e o Regimento Interno da Secretaria Executiva do CONASS de 29 novembro de 2023,

DECIDE:

Art. 1º - Alterar o Regulamento de Gestão de Tecnologia da Informação para refletir as atualizações em seu conteúdo e sua nomenclatura. O documento passará a se chamar "Regulamento Interno de Segurança da Informação e Segurança Cibernética".

Art. 2º - Esta Decisão entra em vigor a partir da data de sua assinatura.

JURANDI FRUTUOSO SILVA
Secretário Executivo do CONASS
CPF: 104.643.443-87

Documento assinado digitalmente por JURANDI FRUTUOSO SILVA:10464344387 às 15:10 do dia 24/09/2024, conforme MP n° 2.200-2/2001 de 24/08/2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.