



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação-Geral de Relacionamento, Governança e Projetos
Coordenação de Governança Estratégica em TIC

ATA

1ª REUNIÃO ORDINÁRIA DO COMITÊ DE GOVERNANÇA DIGITAL – CGD/MS Portaria GM/MS Nº 1.001, de 18 de maio de 2021 alterada pela Portaria GM/MS Nº 1708, de 30 de outubro de 2023		
IDENTIFICAÇÃO		TIPO DE DOCUMENTO
DATA	HORÁRIO	REUNIÃO
23.04.2024	11hs	COMITÊ DE GOVERNANÇA DIGITAL - CGD/MS
MEMBROS TITULARES / SUPLENTE		ASSINATURA
Swedenberger do Nascimento Barbosa (SE/MS)		Web Conferência/Teams
Felipe Proenço De Oliveira (SAPS/MS)		Web Conferência/Teams
Ethel Leonor Noia Maciel (SVSA/MS)		Web Conferência/Teams
Carlos Augusto Grabois Gadelha (SECTICS/MS)		Web Conferência/Teams
Adriano Massuda (SAES/MS)		Web Conferência/Teams
Ricardo Weibe Nascimento Costa (SESAI/MS)		Web Conferência/Teams
José Eduardo Bueno (DATASUS/MS)		Web Conferência/Teams
Denise Barros de Sousa Nogueira (CGRGP/DATASUS/MS)		Web Conferência/Teams
Ana Estela Haddad (SEIDIGI/MS)		Web Conferência/Teams
Adriana Macedo Marques (Encarregada/MS)		Web Conferência/Teams
CONVIDADOS		ASSINATURA
Tiago Bahia (DEMAS/MS)		Web Conferência/Teams
Ramon Moreno de Matos Vieira (CGIE/DATASUS/MS)		Web Conferência/Teams
ASSUNTOS ABORDADOS		
<p>1. Abertura da 1ª Reunião Ordinária do CGD/MS.</p> <p>2. Quórum e Lista de Presença: CGRGP/DATASUS/SEIDIGI</p> <p>3. Portaria de Alteração do CGD/MS: 3.1 Competências: Artigo 246. Portaria de Consolidação GM/MS nº1 de 28/09/2017.</p>		<p>4. Critérios para inclusão de Pauta no Comitê:</p> <p>5. Síntese dos itens de TIC em desenvolvimento</p> <p>6. Pedidos de Deliberação 6.1 Fluxo de Notificação Incidentes de Segurança com Dados Pessoais. CGIE/DATASUS/SEIDIGI 6.2. Plano de Dados Abertos do Ministério da Saúde (PDA). DEMAS/SEIDIGI</p> <p>7. Considerações Finais.</p>
DESDOBRAMENTOS		
<p><u>1. Abertura da 1ª Reunião Ordinária do CGD/MS - 2024:</u></p> <p>O Secretário Executivo Swedenberger iniciou a reunião agradecendo a presença dos membros e procedeu à identificação dos representantes das Secretarias.</p> <p>Posteriormente, fez a abertura da reunião evidenciando que o Comitê de Governança Digital do Ministério da Saúde (CGD/MS) possui natureza deliberativa, de caráter permanente e com responsabilidades estratégicas e executivas. O CGD avalia e prioriza as necessidades de informação que serão supridas por soluções de TIC potencialmente aprovadas por esse comitê; aprova proposta de políticas, diretrizes, objetivos e estratégias de TIC e demanda por novas soluções de TIC, no intuito de submissão à Ministra de Estado da Saúde.</p> <p>Em seguida, autorizou a Secretária Ana Estela Haddad em exercício na Secretaria de Informação e Saúde Digital (SEIDIGI) a dar seguimento à Pauta.</p> <p><u>3. Portaria de Alteração do CGD/MS: CGRGP/DATASUS/SEIDIGI:</u></p> <p>3.1 Competências: Artigo 246. Portaria de Consolidação GM/MS nº 1 de 28/09/2017</p> <p>CGRGP: Apresentou a Portaria GM nº1.078, de 30 de outubro de 2023, que altera a portaria de instituição do CGD/MS, de natureza deliberativa com responsabilidades estratégicas de tomada de decisão. Consolida as normas sobre os direitos e deveres dos usuários da saúde e o funcionamento do Sistema Único de Saúde. A portaria estabelece o Comitê de Governança Digital (CGD/MS), com agendas trimestrais, e o Comitê Executivo de Tecnologia da Informação e Comunicação (CETIC/MS), que possui agendas mensais, para discutir algumas demandas de tecnologia dentro das secretarias que são importantes para execução eficiente dentro de cada instância.</p> <p>O CGD/MS trata das pautas priorizadas e é responsável pelos temas de aprovação de políticas, diretrizes, objetivos e estratégias de TI, bem como pela aprovação de demandas de novas soluções de TI.</p> <p>Mencionou as competências do CGD/MS, incluindo a aprovação de propostas, políticas e diretrizes; bem como a aprovação de demandas de novas soluções de TI. Além disso, é responsável por submeter à Ministra propostas de planos relacionados à TIC, como o Plano Diretor de Tecnologia da Informação (PDTIC), o Plano Estratégico de Tecnologia da Informação e Comunicações (PETIC), o Plano de Transformação Digital (PTD) e o Plano de Dados Abertos (PDA). Esses quatro planos específicos requerem execução dentro do CETIC, bem como submissão e autorização pelo CGD/MS.</p> <p><u>4. Critérios para inclusão de Pauta no Comitê:</u></p> <p>CGRGP: Evidenciou a importância de conhecer os critérios para inclusão de pauta ao CGD, para que cada secretaria saiba o que é necessário para essa submissão. Ademais, informou que os critérios foram desenvolvidos em três possibilidades: Proposta de Novos Projetos de TI; Alteração de Definições em Projetos de TI e outras matérias de TI que podem surgir e que são essenciais para o conhecimento de todos, como exemplo citou a questão dos normativos de incidentes e segurança da informação que não é uma pauta específica de um plano ou de um projeto, mas é essencial e precisa que todos tenham conhecimento.</p>		

Posteriormente, salientou que os itens apresentados foram discutidos nas instâncias do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e no Tribunal de Contas da União (TCU), que formaliza a condução de comitês deliberativos de TI, estabelecendo critérios mínimos para definição de projetos no âmbito da esfera da administração pública federal.

5. Síntese dos itens de TIC em desenvolvimento:

CGRGP: Apresentou a visão geral dos itens tratados no CETIC, nos últimos meses. No contorno das pautas, fora 9 itens de TIC apresentados, sendo um da SVSA, um da SAES, quatro pautas da SE, uma da SECTICS e uma da SEIDIGI. Dentre os projetos apresentados, seis foram submetidos ao CGD: SOMASUS, SISMOB-e, Rebrats Conecta, Logística DLOG, CNIE e Plano de Dados. Atualmente, há três pautas em andamento, que necessitam de uma discussão mais apurada e complementação.

Fez uma breve exposição sobre as duas pautas da reunião. A primeira pauta foi o Fluxo de Notificação de Incidentes de Segurança com Dados Pessoais, que entra dentro do terceiro item dos critérios para submissão de pautas ao comitê, a saber: outros assuntos do CGD para submissão e tem como objetivo definir como o Ministério da Saúde vai lidar com os incidentes de segurança com dados pessoais sensíveis, sejam vindos de ataque cibernético, violação de dados, violação das políticas e padrões de segurança da entidade, dentre outros. A justificativa da formalização do fluxo de incidentes é garantir a conformidade com as regulamentações de proteção de dados LGPD, com a demonstração da transparência e responsabilidade perante os titulares de dados.

6. Pedidos de Deliberação:

6.1 Fluxo de Notificação Incidentes de Segurança com Dados Pessoais. CGIE/DATASUS/SEIDIGI

CGIE: Iniciou a apresentação destacando a relevância do tema no Ministério, haja vista que a guarda, segurança e a disponibilidade dos dados pessoais é um assunto muito importante. Ressaltou que foi criada uma agência nacional de produção de dados, para fiscalização e acompanhamento dessa pauta a nível nacional, e todos os entes devem atender a legislação de proteção de dados.

Apresentou o fluxo notificação de incidentes com dados pessoais. O fluxo começa com a identificação de um possível incidente, que pode ocorrer de diferentes formas, como por cidadãos, pela Equipe de Tratamento de Incidentes de Rede (ETIR) ou pelo canal Fala.BR. A ETIR verifica se o incidente envolve dados pessoais.

Quando um incidente é confirmado, analisa se há informações suficientes. Se for verdadeiro, inicia-se o processo de notificação à encarregada de dados e à Autoridade Nacional de Proteção de Dados (ANPD). Embora não exista um prazo em lei, a ANPD recomenda que a notificação ocorra em dois dias úteis, devido a possibilidade de um vazamento de informações sensíveis.

Destacou a importância da proteção de dados pessoais e a necessidade de notificar a ANPD quando ocorre um incidente relacionado a esses dados.

Após a verificação com a Equipe de Tratamento de Incidente de Rede (ETIR), é realizada uma análise para identificar os responsáveis envolvidos. Os gestores de informação são notificados. Caso seja identificado que o incidente ocorreu por meio de uma invasão e não por compartilhamento ou perda de credencial, a ETIR pode solicitar a retirada do sistema do ar, para impedir que um maior vazamento possa ocorrer, enquanto isso é realizada a análise. Dentro dessa análise, é importante compreender o que ocorreu e manter os gestores do sistema cientes do incidente.

Se for detectado que o sistema foi invadido, pode-se solicitar o bloqueio do acesso para que correções possam ser feitas. Uma nota técnica é elaborada, informando a encarregada de dados sobre o ocorrido. E também é informado aos gestores do sistema e delegacia de crimes cibernéticos.

Após a identificação e tratamento do incidente, caso o sistema tenha sido retirado do ar, é reativado e todos são informados. Caso contrário, é elaborada a nota técnica. Embora não haja um prazo definido em lei, busca-se apresentar uma notificação complementar com análise e ações realizadas ou planejadas para eventuais melhorias dentro do prazo de 30 dias corridos.

SEIDIGI: A Secretária Ana Estela Haddad pediu a palavra e sugeriu realizar uma agenda com maior disponibilidade de horário para viabilizar a apresentação completa sobre o Fluxo de Notificação Incidentes de Segurança com Dados Pessoais.

Salientou que a presente reunião foi convocada devido à necessidade de estabelecer o comitê e garantir a sua regularidade. Solicitou a sensibilidade de todos os secretários para aproveitar da melhor maneira o tempo e o espaço do comitê.

Destacou a importância da construção do Plano de Dados do Ministério, como forma de prevenir os incidentes em diversos níveis, incluindo o nível operacional do sistema. Enfatizou a necessidade de rever o fluxo de processos de trabalho e cuidados com senhas, bem como o estabelecimento de fluxos de documentos nas áreas, a fim de resguardar aquilo que precisa ser protegido com segurança e privacidade.

Complementarmente, informou que uma equipe está trabalhando no processo de segurança de nuvem e na arquitetura de segurança da informação, que será crucial com a RNDS.

Em seguida, passou a palavra para a encarregada de dados do Ministério da Saúde, Adriana Marques.

CGOEX/SEIDIGI: A encarregada de dados se apresentou e contextualizou suas competências instituídas pela LGPD para tratar os dados pessoais sensíveis, como os dados de saúde. Atuando como canal de comunicação entre o MS e os titulares de dados (pessoas, usuários do SUS, os servidores dos ministérios, os funcionários, terceirizados, as pessoas politicamente expostas e a autoridade nacional de proteção de dados).

As atribuições da encarregada incluem receber reclamações e comunicação dos titulares.

Destacou que coordena o subcomitê da LGPD no âmbito do Comitê Gestor de Saúde Digital – CGSD, as atividades de proteção de dados do âmbito do comitê gestor e está revisando o Programa de Governança de Privacidade no Ministério, realizado anteriormente pela AEPD.

Mostrou a estrutura da Assessoria Especial de Proteção de Dados (AEPD) e suas competências. A AEPD foi criada no final do governo anterior, devido a um incidente de segurança, envolvendo uma nuvem (AWS).

A AEPD era composta por 6 pessoas, entre elas:

- Assessor Especial, que era o encarregado
- Substituto do Assessor Especial, que era um Coordenador Geral
- 2 Coordenadores de Assessoria Técnica
- 1 secretário bolsista

Atualmente, essa estrutura da AEPD deixou de existir, e suas competências permanecem.

Foi citado o Programa de Privacidade da Segurança da Informação (PPSI) gerido pelo Datasus. Um programa da Secretaria de Governança Digital (SGD) que lançou a pauta para que todos os ministérios pudessem implementar as ações periodicamente.

Foi destacada a importância do envolvimento das secretarias, visto que são gestoras da maioria dos sistemas do Datasus. Por isso, é necessário sensibilizá-las sobre os prazos exíguos para responder incidentes.

Destacou a importância de sensibilizar as secretarias sobre a obrigatoriedade legal de cumprir prazo exíguo, o que exige respostas tempestivas. Além disso, é fundamental realizar o inventário de dados e elaborar o relatório de impacto da proteção de dados dos sistemas e bancos de dados existentes. Esse inventário deve detalhar os dados presentes em cada sistema do MS, incluindo os tipos de dados, especialmente os dados pessoais sensíveis.

O relatório de impacto descreve os efeitos do tratamento dos dados, identificando os riscos associados a esse processo, as medidas administrativas e técnicas de segurança para prevenir invasões e, caso ocorram, as medidas a serem adotadas diante dos riscos envolvidos, a depender da natureza dos dados tratados.

Outras pautas importantes mencionadas foram a normatização do compartilhamento de dados para pesquisa, a política sobre pessoas politicamente expostas e a capacitação e sensibilização sobre proteção de dados no SUS, com ações de capacitação em andamento. Foi ressaltada ainda a importância da governança de dados para embasar políticas públicas.

No que concerne à capacitação, ressaltou como prioridade a sensibilização da cultura organizacional e no âmbito do SUS para a proteção de dados. É fundamental que todos estejam atentos a essa pauta, que deve ser tratada com devido cuidado. Essa é uma ação conjunta com Conselho Nacional de Saúde (CONASS) e o Conselho Nacional de Secretarias Municipais de Saúde (CONASEMS).

Foram citadas diversas ações de capacitação em andamento, como:

- Realização da primeira jornada de proteção de dados, com mais de 4.900 visualizações no canal do Datasus, e planejamento da segunda jornada para o próximo semestre;
- Capacitações específicas para cada departamento da SEIDIGI e demais secretaria;
- Abordagem da questão das credenciais de acesso, com a implementação de capacitação de usuários;
- Destaque para a determinação do Tribunal de Contas da União (TCU) em relação à capacitação das unidades descentralizadas do MS;
- Gestão do conteúdo da intranet em andamento para disponibilizar o material produzindo.

Além do mais, foi ressaltada a importância da governança de dados, que não se limita apenas aos dados pessoais sensíveis, mas também abrange a utilização de dados como ativos fundamentais para embasar políticas públicas e o compartilhamento de informações.

A governança de dados envolve transparência, publicidade e exige a atuação do CGD/MS para alinhar pessoas, processos e tecnologias na gestão da governança no âmbito do Ministério, sendo necessário desenvolver uma Política de Governança de Dados que está sendo tratado no âmbito da Coordenação Geral de Relacionamento, Governança e Projetos (CGRGP).

7. Considerações Finais:

SE: Agradeceu a presença de todas as secretarias e enfatizou a relevância do Comitê de Governança Digital (CGD/MS), para a organização interna da unidade administrativa do governo federal, dada que é fundamental, pois trata de questões relacionadas à vida. Além disso, anunciou que os apresentadores terão mais tempo e oportunidade para abordar os temas levantados em uma próxima reunião.

Também foi destacada a importância dos três pilares da governança de dados: pessoas, processos e tecnologia. Como exemplo, citou os processos instalados para democratizar, organizar e participar ativamente das discussões dentro da lógica de Ministério "único" da Saúde.

Expressou preocupação com a gestão das informações do MS. Diante disso, solicitou a inclusão do tema sobre a gestão da informação do MS como tópico adicional na pauta. Como exemplo de desafio na gestão de informações citou a falta de um sistema de acompanhamento dos insumos estratégicos e medicamentos no Brasil. Considerou preocupante a falta de informação sobre o destino dos medicamentos, sendo necessário ter um sistema que permita monitorar o estoque de cada estado e município para um planejamento orçamentário eficaz, visto que a falta de informação pode acarretar o desabastecimento.

Reforçou a urgência da necessidade dessa informação e a importância de uma conversa mais detalhada no futuro, relacionando o plano de gestão de dados.

Mencionou a relevância das orientações do Tribunal de Contas da União (TCU), sobre o uso da internet e na intranet, reforçando a responsabilidade de cada gestor, dos diferentes níveis do Ministério, de conhecer e seguir as diretrizes.

Enfatizou a importância de que o Sistema Eletrônico de Informações (SEI) seja transparente, e ao mesmo tempo, tenha segurança de dados, de modo que o sistema não se torne uma "peneira" com milhares de pessoas trabalhando com ele. E garantir o seu uso adequado, proporcionando tranquilidade aos gestores para trabalhar, assim como abordar de forma adequada as orientações relacionadas à intranet e internet.

Para mais, propôs ajudar a organizar um processo de alinhamento entre a necessidade da gestão, a obrigação legal, com o objetivo de fazer uma apresentação para a Ministra, em breve.

SEIDIGI: Expressou sua preocupação em realizar tempestivamente a primeira reunião do comitê, visto que foi instituído em outubro de 2023. Salientou que o desafio é imenso, que há muito trabalho pela frente nesse processo que será realizado de forma coletiva.

Destacou a necessidade de que o CGD/MS ocorra para que as pautas sejam apreciadas em tempo oportuno. Exigiu prioridade máxima das áreas envolvidas no que se refere à gestão da informação, principalmente do que é informado à sociedade. Chamou atenção à fragilidade do SEI, haja vista que alguns documentos possuem dados pessoais, dados esses que só devem ser compartilhados, no seu entendimento, mediante pedido judicial.

A Secretária Ana Estela Haddad agradeceu a participação de todos e passou a palavra para a Denise (CGRGP).

CGRGP/DATASUS: Encerrou a reunião agradecendo a todos e destacou a necessidade de apresentar o Plano de Dados Abertos - PDA em uma próxima oportunidade, visto tratar-se de pauta relevante.

ENCAMINHAMENTOS	RESPONSÁVEL	PRAZO
<ol style="list-style-type: none"> 1. Apresentar normativos e fluxo de reporte de incidentes de privacidade e segurança; 2. Priorizar a gestão da informação no MS; 3. Apresentar o Plano de Dados Abertos do Ministério da Saúde (PDA). 	<ol style="list-style-type: none"> 1. CGIE/DATASUS 2. CGIIS/DATASUS 3. DEMAS/SEIDIGI 	<ol style="list-style-type: none"> 1. Próximo CGD/MS 2. Imediato 3. Próximo CGD/MS
SUGESTÃO DE PRÓXIMAS PAUTAS		
<ol style="list-style-type: none"> 1. Agenda das reuniões do CGD/MS. 2. Acompanhamento da evolução sobre a Governança e Gestão de Dados no MS. 3. Deliberação dos itens submetidos pelo CETIC. 		
ELABORADA POR:		
<ul style="list-style-type: none"> • Samara Lopes do Nascimento - CGOV/CGRGP/DATASUS/SEIDIGI/MS 		
REVISADA POR:		
<ul style="list-style-type: none"> • Whesley Fernandes Henrique - CGOV/CGRGP/DATASUS/SEIDIGI/MS • Graziella Cervo Santana - CGOV/CGRGP/DATASUS/SEIDIGI/MS 		
VALIDADA POR:		
<ul style="list-style-type: none"> • Denise Barros de Sousa Nogueira - CGRGP/DATASUS/SEIDIGI/MS 		



Documento assinado eletronicamente por **Carlos Amílcar Salgado, Diretor(a) Departamento de Regulação Assistencial e Controle**, em 18/06/2024, às 11:11, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Swedenberger do Nascimento Barbosa, Secretário(a)-Executivo(a)**, em 19/06/2024, às 10:19, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Felipe Proença de Oliveira, Secretário(a) de Atenção Primária à Saúde**, em 19/06/2024, às 18:09, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Adriana Macedo Marques, Coordenador(a)-Geral de Demandas de Órgãos Externos de Informação e Saúde Digital**, em 20/06/2024, às 17:31, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Ana Estela Haddad, Secretário(a) de Informação e Saúde Digital**, em 21/06/2024, às 16:54, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Leticia de Oliveira Cardoso, Diretor(a) do Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis**, em 21/06/2024, às 16:57, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Ricardo Weibe Nascimento Costa, Secretário(a) de Saúde Indígena**, em 24/06/2024, às 11:40, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Denise Barros de Sousa Nogueira, Coordenador(a)-Geral de Relacionamento, Governança e Projetos**, em 24/06/2024, às 16:53, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



Documento assinado eletronicamente por **Jose Eduardo Bueno de Oliveira, Diretor(a) do Departamento de Informação e Informática do SUS**, em 24/06/2024, às 18:11, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#); e art. 8º, da [Portaria nº 900 de 31 de Março de 2017](#).



A autenticidade deste documento pode ser conferida no site http://sei.saude.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0041353139** e o código CRC **821B3DEC**.