13134060 08020.008341/2020-59

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

PORTARIA DA SENASP Nº 191, DE 10 DE NOVEMBRO DE 2020

Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

O SECRETÁRIO NACIONAL DE SEGURANÇA PÚBLICA, no uso das atribuições que lhe foram conferidas pela Portaria nº 77, de 17 de janeiro de 2020, publicada no DOU nº 13, Seção 1, Página 70, de 20/01/2020, combinado com o art. 74, VIII, do Regimento Interno da Secretaria Nacional de Segurança Pública, aprovado pela Portaria nº 151, de 26 de setembro de 2018, do Ministro de Estado da Justiça, publicada no DOU nº 200, Seção 1, Páginas 45-51, de 17/10/2018, e tendo em vista o disposto na **Lei 13.709, de 14 de agosto de 2018**; na **Lei nº 13.675, de 11 de junho de 2018**; no **Decreto 9.489, de 30 de agosto de 2018**; e no **Decreto nº 9.876, de 17 de junho de 2019.**

CONSIDERANDO que o Controlador é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, nos termos do artigo 5º, inciso VI da Lei 13.709, de 14 de agosto de 2018;

CONSIDERANDO que na Administração Pública, o Controlador é a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

CONSIDERANDO que Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

CONSIDERANDO que a Secretaria Nacional de Segurança Pública trata dados pessoais e informações no exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem atender aos padrões de integridade, disponibilidade, confidencialidade, confiabilidade, tempestividade dos sistemas informatizados do Governo Federal, interoperabilidade entre os sistemas eletrônicos governamentais e, quando for o caso, com sigilo resguardado;

CONSIDERANDO o descrito no Art. 35, Seção IIII da Lei nº 13.675, de 11 de junho de 2018, que determina que o Sistema Nacional de Informações de Segurança Pública, Prisionais e de Rastreabilidade de Armas e Munições, e sobre Material Genético, Digitais e Drogas (Sinesp) tem por finalidade armazenar, tratar e integrar dados e informações dos integrantes do Sistema Único de Segurança Pública (Susp) para auxiliar na formulação, implementação, execução, acompanhamento e avaliação das políticas relacionadas com:

I - segurança pública e defesa social;

II - sistema prisional e execução penal;

III - rastreabilidade de armas e munições;

IV - banco de dados de perfil genético e digitais;

V - enfrentamento do tráfico de drogas ilícitas.

CONSIDERANDO que o Sinesp tem por objetivos:

I - proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social;

II - disponibilizar estudos, estatísticas, indicadores e outras informações para auxiliar na formulação, implementação, execução, monitoramento e avaliação de políticas públicas;

III - promover a integração das redes e sistemas de dados e informações de segurança pública e defesa social, criminais, do sistema prisional e sobre drogas;

IV - garantir a interoperabilidade dos sistemas de dados e informações, conforme os padrões definidos pelo conselho gestor.

CONSIDERANDO que a integração das informações e dos dados de segurança pública dos órgãos integrantes do Sistema Único de Segurança Pública (Susp) é de responsabilidade do Sinesp, conforme Artigo 10, inciso VI, Seção II da Lei nº 13.675, de 11 de junho de 2018, cabendo a sua padronização e categorização;

CONSIDERANDO que as informações nos sistemas integrantes da plataforma Sinesp, no âmbito da Secretaria Nacional de Segurança Pública, são armazenadas em diferentes formas, veiculadas por meios físicos e eletrônicos, portanto vulneráveis a incidentes de segurança da informação envolvendo a privacidade de dados pessoais como vazamentos, ataques cibernéticos, acessos não autorizados, mau uso, extravio, sequestro de dados etc.;

CONSIDERANDO que a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPDP), compreende um conjunto de ações determinadas pela Lei 13.709, de 14 de agosto de 2018, inclusive especificamente no tocante ao tratamento de dados pessoais pelo poder público, que buscam proteger e preservar a privacidade e proteção de dados pessoais e os ativos de informação, assegurando-lhes disponibilidade, integridade, confidencialidade e autenticidade;

CONSIDERANDO a necessidade de aprimorar a interoperabilidade, eficiência, eficácia e efetividade na elaboração, tramitação, utilização e destinação dos documentos, processos e informações produzidas e recebidas pelos órgãos e entidades pertencentes à Administração Pública;

CONSIDERANDO a vantajosidade de utilizar meios eletrônicos para realização dos processos administrativos com segurança, transparência e economicidade, aumentando a produtividade e celeridade na tramitação de processos, ampliando a sustentabilidade ambiental com o uso da tecnologia da informação e comunicação, propiciando a satisfação do público usuário;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à privacidade e proteção de dados pessoais e informações no âmbito da Administração Pública Federal, às quais a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPDP) deverá estar alinhada;

RESOLVE:

Seção I

Introdução

Art. 1º Instituir a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Secretaria Nacional de Segurança Pública.

§1º. A presente Política Geral de Privacidade e Proteção de Dados Pessoais materializa o desiderato da Secretaria Nacional de Segurança Pública de prestigiar o respeito à proteção de dados pessoais, em consonância com a Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - "LGPD") e com a legislação correlata, especialmente a Lei nº 12.965 de 23 de abril de 2014 (“Lei do Marco Civil da Internet”) e a Lei nº 12.527, 28 de novembro de 2011 (Lei de Acesso à Informação - "LAI").

§2º. Esta Política será administrada pelo Comitê Gestor de Privacidade e Proteção de Dados Pessoais do Sinesp (CGPDP-Sinesp), instituído pela Portaria SENASP Nº 169, de 04 de setembro de 2020.

Seção II
Do Escopo

Art.2º. Esta Política regula a proteção de dados pessoais nas atividades instituída pela Lei 13.675, de 11 de junho de 2018 ao Sinesp e nas suas demais atividades administrativas. Suas disposições regulam o relacionamento da Secretaria Nacional de Segurança Pública com os usuários de seus serviços e demais agentes de tratamento, nos termos da Lei 13.709, de 14 de agosto de 2018, que realizem tratamento de dados pessoais do Sinesp.

§1º. As disposições desta Política se referem a dados pessoais contidos em qualquer suporte físico, seja eletrônico ou não.

Seção III
Do objetivo

Art. 3º. O objetivo desta Política é de definir e divulgar as regras de tratamento de dados pessoais, pela Secretaria Nacional de Segurança Pública, em consonância com a legislação aplicável e com os regulamentos e orientações da Autoridade Nacional de Proteção de Dados (ANPD) e das demais autoridades competentes. Esta Política estabelece diretrizes para a atuação do Comitê Gestor de Privacidade e Proteção de Dados Pessoais do Sinesp (CGPDP-Sinesp), instituído pela Portaria SENASP nº 169, de 04 de setembro de 2020.

Seção IV
Das Referências Legais e Normativas

Art. 4º O tratamento de dados pessoais pela Secretaria Nacional de Segurança Pública é regido pela Lei Federal nº Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, “LGPD”) e pela legislação pertinente (inclusive as leis regedoras do habeas data, da liberdade de acesso à informação, dos direitos de privacidade e de intimidade), assim como por normas técnicas geralmente aceitas (tais como a NBR ABNT ISO/IEC 29100 e NBR ABNT ISO/IEC 27701), por políticas públicas (por exemplo, as de dados abertos e de inclusão digital), pelas boas práticas de governança de dados (como aquelas preconizadas no Guia de Boas Práticas para Implementação na Administração Pública Federal, editado em sintonia com o Decreto Federal nº 10.046/2019) e de segurança da informação.

Seção V
Dos Termos e Definições

Art. 5º. Os termos, expressões e definições utilizados nesta Política serão aqueles conceituados pela Lei Geral de Proteção de Dados, em legislação substituta ou no documento ANEXO I (CONCEITOS E DEFINIÇÕES) nesta Portaria.

Seção VI
Dos Princípios

Art. 6º. A aplicação desta Política será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da Lei 13.709, de 14 de agosto de 2018, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e, responsabilização e prestação de contas.

Seção VII
Do Tratamento de Dados Pessoais

Art. 7º. O tratamento de dados pessoais pela Secretaria Nacional de Segurança Pública é realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Art. 8º. Em atendimento a suas competências legais, a Secretaria Nacional de Segurança Pública poderá, no estrito limite legal, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares. Eventuais atividades que transcendam as finalidades do tratamento do dado pessoal, previstas em lei, estarão sujeitas à obtenção de consentimento dos interessados.

Art. 9º. A Secretaria Nacional de Segurança Pública mantém contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários as operações de tratamento de dados, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível a ser consultada pelos interessados.

Art. 10 Os dados pessoais tratados pela Secretaria Nacional de Segurança Pública são:

I - Protegidos por procedimentos internos, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações;

II - Mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade respectiva ou face a solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de prazos de retenção de dados;

III - Compartilhados somente para o exercício das finalidades e para atendimento de políticas públicas aplicáveis; e

IV - Revistos em periodicidade mínima anual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.

Art. 11. A informação sobre o tratamento de dados pessoais sensíveis ou referentes a crianças ou adolescentes estará disponível em linguagem clara e simples, com concisão, transparência, inteligibilidade e acessibilidade, na forma da lei.

Art. 12. A responsabilidade da Secretaria Nacional de Segurança Pública pelo tratamento de dados pessoais estará atrelada ao dever de se ater ao exercício de sua competência legal, institucional e de empregar boas práticas de governança e de segurança.

Seção VIII
Dos Direitos do Titular

Art. 13. A Secretaria Nacional de Segurança Pública zela para que o Titular do dado pessoal possa usufruir dos direitos assegurados pelos artigos 18 e 19 da LGPD, aos quais a presente Política se reporta, por remissão.

Seção IX

Da Transferência Internacional de Dados

Art. 14. A Secretaria Nacional de Segurança Pública está sujeita ao dever de colaborar para autorização de atividades de cooperação técnica de compartilhamento dos dados observando, dentre outros, os deveres legais inerentes às atividades que implicam a transferência de dados pessoais.

Parágrafo único. Exceto no contexto indicado no ”caput”, a Secretaria Nacional de Segurança Pública não procederá à transferências internacionais de dados pessoais, inclusive para fins de convênios de cooperação administrativa com outros órgãos da administração pública, exceto se prévia e formalmente autorizado pelo Ministério da Justiça e Segurança Pública e mediante consentimento inequívoco pelo Titular respectivo ou anonimização do dado pessoal para execução de políticas públicas definidas em legislação específica ou fins exclusivamente estatísticos.

Seção X
Dos Agentes de Tratamento de Dados Pessoais

Art. 15. A Secretaria Nacional de Segurança Pública é órgão Controlador dos dados pessoais por ela tratados, nos termos das suas competências legal e institucional.

Art. 16. A Secretaria Nacional de Segurança Pública pode, a qualquer tempo, requisitar informações acerca dos dados pessoais confiados a seus fornecedores e prestadores de serviços terceirizados, particularmente no caso de serviços de Tecnologia da Informação e Comunicação (TIC). Os provedores de tais serviços serão considerados Operadores e deverão aderir a esta Política, além de cumprir os deveres legais e contratuais respectivos, dentre os quais se incluirão, mas não se limitarão aos seguintes:

I - Assinar contrato, termo de adesão ou Termo de compromisso, com cláusulas específicas sobre proteção de dados pessoais requeridas pela Secretaria Nacional de Segurança Pública;

II - Apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

III - Manter os registros de tratamento de dados pessoais que realizar, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

IV - Seguir fielmente as diretrizes e instruções transmitidas pela Secretaria Nacional de Segurança Pública;

V - Facultar acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição a Secretaria Nacional de Segurança Pública, ou mediante solicitação das Diretorias afetas a Secretaria Nacional de Segurança Pública;

VI - Permitir a realização de auditorias, incluindo inspeções determinadas pela Secretaria Nacional de Segurança Pública ou de auditor independente por ela autorizado, obrigando-se a disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações legais e estabelecidas;

VII - Auxiliar, em toda providência que estiver ao seu alcance, no atendimento pela Secretaria Nacional de Segurança Pública de obrigações perante Titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII - Comunicar formalmente e de imediato à Secretaria Nacional de Segurança Pública a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo ao Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

IX - Descartar de forma irrecuperável, ou devolver para a Secretaria Nacional de Segurança Pública, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o

encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Art. 17. A Secretaria Nacional de Segurança Pública designou pela Portaria nº 172, de 04 de setembro de 2020, o agente público responsável pela função de Encarregado pelo Tratamento de Dados Pessoais do Sinesp, que atenderá quaisquer contatos, nos termos da lei, no endereço eletrônico encarregado_lgpd.sinesp@mj.gov.br , o qual deverá estar informado no sítio eletrônico e em materiais de divulgação desta Política.

Art. 18. O Encarregado deverá contar com apoio efetivo do Comitê Gestor de Privacidade e Proteção de Dados Pessoais do Sinesp (CGPDP-Sinesp) da Diretoria de Gestão e Integração da Informação (DGI/SENASP), para o adequado desempenho de suas funções.

Art. 19. A Secretaria Nacional de Segurança Pública poderá padronizar modelos de comunicação para utilização pelo Encarregado no atendimento de solicitações ou dúvidas de Titulares de dados pessoais, e demais procedimentos organizacionais, visando a assegurar a celeridade necessária para cumprimento de prazos legais de atendimentos.

Seção XI
Da Segurança e Boas Práticas

Art. 20. A Secretaria Nacional de Segurança Pública deve dispor de uma Política de Segurança da Informação e Comunicações (POSIC) que especifique e determine a adoção de um conjunto de medidas técnicas e administrativas de segurança para a proteção de dados pessoais contra acessos não autorizados e situações acidentais ou incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único. Embora a Secretaria Nacional de Segurança Pública recorra à organização interna e à assessoria externa que seguem padrões e critérios nacionais e internacionais geralmente aceitos, tal precaução não implica em garantia contra a possibilidade de incidentes de segurança ou de violação da proteção de dados pessoais, haja vista, sobretudo, a contínua diversificação dos riscos cibernéticos.

Art. 21. A Secretaria Nacional de Segurança Pública adota boas práticas e governança capazes de inspirar comportamentos adequados e de mitigar os riscos de comprometimento de dados pessoais.

Parágrafo único. As boas práticas adotadas de proteção de dados pessoais e a governança implantada deverão ser objeto de campanhas informativas na esfera interna do Ministério da Justiça e Segurança Pública e seus sítios eletrônicos, visando a disseminação de uma cultura protetiva, com conscientização e sensibilização dos interessados.

Art. 22. O Encarregado pelo Tratamento de Dados Pessoais do Sinesp, através do Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPDP-Sinesp), deverá manter a direção da Diretoria de Gestão e Integração de Informações (DGI/SENASP) a par de aspectos e fatos significativos e de interesse para conhecimento pelas instâncias superiores.

Art. 23. A Política Geral de Privacidade e Proteção de Dados Pessoais deve ser revista em intervalos planejados não superiores a 12 (doze) meses, a partir da data de sua publicação, ou ante a ocorrência de algumas das seguintes condições:

I - Edição ou alteração de leis e/ou regulamentos relevantes;

II - Alteração de diretrizes estratégicas pelo Ministério da Justiça e Segurança Pública;

III - Expiração da data de validade do documento, se aplicável;

IV - Mudanças significativas de tecnologia na organização do Ministério da Justiça e Segurança Pública, como por exemplo a definição de armazenamento em data center localizado no exterior;

V - Análises de risco, em Relatório de Impacto à Proteção de Dados Pessoais, que indique a necessidade de modificação no documento para readequação da organização visando prevenir ou mitigar

riscos relevantes.

Art. 24. O processo de análise para determinar a adequação, suficiência e eficácia dos documentos da Política Geral de Proteção de Dados Pessoais deve ser formalizado com o registro de diagnósticos e sugestões e das aprovações respectivas.

Art. 25. Independentemente da revisão ou atualização desta Política Geral de Privacidade e Proteção de Dados Pessoais, deverá ser elaborado no mínimo anualmente um Relatório de Impacto de Proteção de Dados Pessoais, identificando vulnerabilidades e respectivos Planos de Ação.

Seção XII
Da Fiscalização

Art. 26. O Comitê Gestor de Privacidade e Proteção de Dados Pessoais do Sinesp (CGPDP-Sinesp), deverá definir, *ad referendum* da Secretaria Nacional de Segurança Pública, os procedimentos e mecanismos de fiscalização do cumprimento desta Política.

Art. 27. A Secretaria Nacional de Segurança Pública cooperará com fiscalizações promovidas por terceiros legitimamente interessados, devendo ser observadas as seguintes condições:

I - Sejam informadas em tempo hábil;

II - Tenham motivação objetiva e razoável;

III - Não afetem a proteção de dados pessoais não abrangidos pelo propósito da fiscalização;

IV - Não causem impacto, dano ou interrupção nos equipamentos ou atividades do Ministério da Justiça e Segurança Pública.

Parágrafo único. A inobservância da presente Política de Proteção de Dados Pessoais acarretará em apuração das responsabilidades internas e externas previstas nas normas e legislações em vigor, podendo haver responsabilização penal, civil e administrativa.

Art. 29. Revogam-se as disposições em contrário.

Art. 30. Esta Portaria entra em vigor nesta data.

CARLOS RENATO MACHADO PAIM

ANEXO I - CONCEITOS E DEFINIÇÕES

Para os fins desta Política Geral de Privacidade e Proteção de Dados Pessoais, considera-se:

1. ACESSO LÓGICO: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

2. ACESSO REMOTO: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

3. ADMINISTRADOR DE SISTEMA: Papel do Sinesp Segurança responsável por criar e dar manutenção na entidade Funcionalidade;

4. ADMINISTRADOR GERAL: Papel do Sinesp Segurança responsável por criar e dar manutenção nas entidades Sistema, Usuário, Administrador de Sistema e Administrador Senasp;

5. ADMINISTRADOR SENASP: Papel do Sinesp Segurança responsável pela gestão dos sistemas do MJ, deverá delegar um gestor para os sistemas. Este papel também é responsável por criar e dar manutenção nas entidades Gestor de sistema, Cadastrador de Estrutura Organizacional e Cadastrador Autorizador;

6. AGENTE RESPONSÁVEL: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

7. AGENTES DE TRATAMENTO: o controlador e o operador;

8. AGENTE PÚBLICO: todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função;

9. AMEAÇA: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

10. ANÁLISE/AVALIAÇÃO DE RISCOS: processo completo de análise e avaliação de riscos;

11. 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;

12. ASSINATURA ELETRÔNICA: código ou registro realizado eletronicamente, por usuário identificado de modo inequívoco, de uso pessoal e intransferível, com vistas a firmar determinado documento com sua assinatura, de modo a comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada. Pode ser: (i) assinatura digital, baseada em certificado digital emitido por autoridade certificadora credenciada na Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil; e (ii) assinatura cadastrada, mediante prévio credenciamento de acesso de usuário, com fornecimento de login e senha.

13. ANTIMALWARE: Ferramenta que procura detectar e, então, anular ou remover os códigos maliciosos de um computador. Os programas antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas *antimalware;*

14. ATAQUE: Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede;

15. ANTIVÍRUS: Tipo de ferramenta *antimalware* desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos. Pode incluir também a funcionalidade de *firewall* pessoal;

16. ATIVIDADES PRECÍPUAS: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Segurança Pública;

17. ATIVIDADES CRÍTICAS: atividades precípuas da Segurança Pública cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, dano à imagem institucional, prejuízo ao Erário, entre outros;

18. ATIVO: qualquer bem, tangível ou intangível, que tenha valor para a organização;

19. ATIVO DE INFORMAÇÃO: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

20. ATIVO DE PROCESSAMENTO: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Segurança Pública; (Não entendi a diferença para o ativo de informação e como isso se aplicaria ao caso do Sinesp) Realmente ficou confuso, mas deveria ter restringido Ativo de informação a parte de software e processamento a hardware. Só que hoje temos um conceito de infraestrutura como software (Nuvem, Hiperconvergência) e que é tanto ativo de informação como de processamento;

21. AUDITORIA: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

22. AUTENTICAÇÃO: declaração de autenticidade de um documento arquivístico, resultante do acréscimo de elemento de verificação ou da afirmação por parte de pessoa investida de autoridade para tal;

23. AUTENTICIDADE: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

24. AUTORIDADE CERTIFICADORA: Entidade responsável por emitir e gerenciar certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc;

25. BANCO DE DADOS (OU BASE DE DADOS): conjunto estruturado de registros de dados ou sistema de armazenamento de dados, que tem como objetivo organizar e guardar as informações, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

26. BANDA LARGA: Tipo de conexão à rede com capacidade acima daquela conseguida, usualmente, em conexão discada via sistema telefônico. Não há uma definição de métrica de banda larga que seja aceita por todos, mas é comum que conexões em banda larga sejam permanentes e não comutadas, como as conexões discadas. Usualmente, compreende conexões com mais de 100 Kbps, porém esse limite é muito variável de país para país e de serviço para serviço (Fonte: http://www.cetic.br/);

27. BANDA LARGA FIXA: Tipo de conexão banda larga que permite que um computador fique conectado à Internet por longos períodos e com baixa frequência de alteração de endereço IP;

28. BANDA LARGA MÓVEL: Tipo de conexão banda larga. Tecnologia de acesso sem fio, de longa distância, por meio de rede de telefonia móvel, especialmente 3G e 4G (respectivamente a terceira e a quarta geração de padrões de telefonia móvel definidos pelo *International Telecommunication Union* - ITU);

29. BIOMETRIA: uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;

30. BLOQUEIO: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

31. BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso;

32. CADASTRADOR AUTORIZADOR: Papel do Sinesp Segurança responsável pela análise de pré-cadastros destinados para a sua área de interesse e Estrutura Organizacional;

33. CADASTRADOR DE ESTRUTURA ORGANIZACIONAL: Papel do Sinesp Segurança responsável pela criação de estruturas organizacionais de um órgão, departamento ou entidade. Este papel é responsável por criar dar manutenção na entidade Estrutura Organizacional;

34. CADASTRADOR DE INTELIGÊNCIA: Papel do Sinesp Segurança responsável pela criação dos usuários com os perfis de inteligência;

35. CADASTRADOR: Papel do Sinesp Segurança responsável pela criação dos vínculos de usuários em um determinado Sistema Cliente em uma determinada Estrutura Organizacional. Este papel é responsável por criar dar manutenção nas entidades Pessoa e Cadastrador;

36. CERTIFICAÇÃO DE IDENTIDADE: Procedimento de conferência de identidade do manifestante por meio de documento de identificação válido;

37. CICLO DE VIDA DA INFORMAÇÃO: compreende etapas e eventos de produção, recebimento ou alteração, acesso, armazenamento, divulgação, transferência física em redes eletrônicas,

cópia, impressão ou qualquer outra forma de reprodução, destruição e descarte;

38. CIFRAÇÃO: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los;

39. CLASSIFICAÇÃO DA INFORMAÇÃO: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

40. COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS DO SINESP (CGPDP - Sinesp): colegiado consultivo, propositivo e executivo, subordinado a Diretoria de Gestão e Integração de Informações da Senasp, que tem a finalidade de analisar, revisar e aprovar políticas e normas relacionadas à proteção de dados pessoais tratados pelo Sinesp e colaborar com o Subcomitê de Segurança da Informação e Comunicações - SCSIC da Senasp, coordenar a Equipe de Tratamento de Incidentes de Redes Computacionais - ETIR para o desenvolvimento e implantação das políticas e ações do Sinesp na área de Segurança da Informação, Privacidade e Proteção de Dados Pessoais;

41. CONFIDENCIALIDADE: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

42. CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

43. CONTA DE USUÁRIO: Também chamada de "nome de usuário" e "nome de *login*". Corresponde à identificação única de um usuário em um computador ou serviço;

44. CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

45. CONTROLADOR SINESP: pessoa jurídica do órgão ou entidade pública nos termos do art. 37 da Lei nº13.675, de 11 de junho de 2018, representada pela autoridade imbuída de adotar as decisões acerca do tratamento dos dados Sinesp.

46. CONTINUIDADE DE NEGÓCIOS: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

47. CONTINGÊNCIA: descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

48. CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

49. CÓPIA DE SEGURANÇA (BACKUP): é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

50. CORREIO ELETRÔNICO: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

51. CREDENCIAIS OU CONTAS DE ACESSO - permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

52. CRIPTOGRAFIA – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível por meio de procedimentos matemáticos, de forma que possa ser conhecida apenas por seus interlocutores (detentores da "chave secreta");

53. DADO: sequência de símbolos ou valores representados por algum meio, produzidos como resultado de um processo natural ou artificial, e ainda, toda e qualquer representação de fato, situação,

comunicação, notícia, documento, extrato de documento, fotografia, gravação, relato, denúncia, dentre outros, ainda não submetida à metodologia de Produção de Conhecimento;

54. DADO ANONIMIZADO: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

56. DADOS PROCESSADOS: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

57. DADO PÚBLICO: qualquer dado gerado ou sob a guarda governamental que não tenha o seu acesso restrito por legislação específica;

58. DATA CENTER OU CENTRO DE PROCESSAMENTO DE DADOS: ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros equipamentos de TIC;

59. DECIFRAÇÃO: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

60. DISPONIBILIDADE: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada por uma pessoa física ou determinado sistema, órgão ou entidade;

61. DISPOSITIVO MÓVEL: qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, com caráter de mobilidade, como: notebooks, *tablets, smartphones, wearables, tokens* e pendrives;

62. DIRETRIZ: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

63. DOCUMENTO: unidade de registro de informações, qualquer que seja o suporte ou formato;

64. DOCUMENTO DIGITAL: informação registrada, digitalizada, armazenada, sob a forma eletrônica e codificada em dígitos binários, acessível e interpretável por meio de sistema computacional, podendo ser:

65. DOCUMENTO NATO-DIGITAL: documento criado originariamente em meio eletrônico;

66. DOCUMENTO DIGITALIZADO: documento obtido a partir da conversão de um documento-base não digital, gerando uma fiel representação em código digital;

67. DOCUMENTO EXTERNO: documento arquivístico digital não produzido diretamente por sistemas do Sinesp, independentemente de ser nato digital ou digitalizado e de ter sido produzido na instituição ou por ela recebido;

68. DOMÍNIO PÚBLICO: toda informação classificada como sendo de acesso irrestrito ou público;

69. DOWNLOAD (Baixar): copiar arquivos de um servidor (site) na internet para um computador pessoal;

70. ENDOMARKETING: conhecido como marketing voltado para dentro ou marketing interno são conjuntos de ações internas desenvolvidas pela instituição que visa manter os funcionários, servidores e colaboradores, bem informados e integrados, com o objetivo de criar fidelidade, de modo que trabalhem sempre em prol da organização e que atendam melhor seus clientes finais;

71. ENGENHARIA REVERSA: processo utilizado para estudar um programa, código fonte, software, sistema, desmembrando-o minuciosamente através da inversão dos procedimentos utilizados na elaboração;

72. EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e propor respostas às notificações e

atividades relacionadas a incidentes de segurança na rede computacional;

73. ESTRUTURA ORGANIZACIONAL: designação dada à ordenação das partes, hierárquica ou não, de um todo que compõe um órgão ou instituição formalmente constituído e devidamente legitimado a participar do Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas – Sinesp, nos termos da Lei nº 13.675, de 11 de junho de 2018, composta de unidades inferiores e superiores;

74. FIREWALL: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede;

75. FUNCIONALIDADE: Entidade cadastrada no Sinesp Segurança que corresponde a uma funcionalidade específica de um Sistema Cliente que terá o seu acesso controlado pelo Sinesp Segurança;

76. GESTÃO DE CONTINUIDADE: Nos termos da Norma Complementar 06/IN01/DSIC/GSIPR, "a implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação";

77. GESTÃO DE CONTINUIDADE DE NEGÓCIOS: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

78. GESTÃO DE RISCO: Nos termos da Norma Complementar 04/IN01/DSIC/GSIPR, a "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos";

79. GESTÃO DE SEGURANÇA DA INFORMAÇÃO: conjunto de processos, ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação, que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

80. GESTOR DE ESTRUTURA ORGANIZACIONAL: Papel do Sinesp Segurança responsável por gerenciar estruturas organizacionais criadas pelo Cadastrador de EO. Este papel é responsável por criar dar manutenção nas entidades Cadastrador de Estrutura Organizacional, Pessoa e Estrutura Organizacional;

81. GESTOR DE SISTEMA ORGANIZACIONAL: Papel do Sinesp Segurança responsável pela criação de cadastradores e vínculos de usuários em uma determinada Estrutura Organizacional de um determinado sistema. Este gestor substituirá o Gestor de Sistema na Estrutura Organizacional, após a sua criação o Gestor de Sistema não poderá mais criar Cadastradores e vincular usuários. Este papel é responsável por criar dar manutenção nas entidades Cadastrador e Máquina;

82. GESTOR DE SISTEMA: Papel do Sinesp Segurança responsável pela criação de perfis de um determinado sistema e também definirá os cadastradores do sistema. Este papel é responsável por criar e dar manutenção nas entidades Perfil, Cadastrador e Máquina;

83. HARDWARE: É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

84. HTTP (Hyper Text Transfer Protocol) - (Protocolo de Transferência de Hipertexto): é uma linguagem para troca de informação entre servidores e clientes da rede;

85. HTTPS (HyperText Transfer Protocol Secure) – (Protocolo de Transferência de Hipertexto Seguro): é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;;

86. INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS: qualquer evento ou série de eventos adversos, indesejados ou inesperados, confirmado ou sob suspeita, relacionado aos sistemas de computação ou das redes de computadores sob a guarda do Sinesp;

87. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer evento ou série de eventos de segurança da informação e comunicações, não autorizados, indesejados ou inesperados, em situações acidentais ou ilícitas, que possam destruir, perder, alterar, comunicar, transferir ou difundir, acessar de forma não autorizada ou ameaçar a segurança da informação e privacidade dos dados Sinesp;

88. INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, processados ou não, independentemente do suporte em que resida, formato ou meio pela qual seja veiculado, que podem ser utilizados para produção e transmissão de conhecimento;

89. INFORMAÇÃO ATUALIZADA: informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam;

90. INFORMAÇÃO ACUMULADA: aquela que está sob a posse de uma determinada instituição pública, muito embora não necessariamente tenha sido produzida pela Administração;

91. INFORMAÇÃO CLASSIFICADA: informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada.

92. INFORMAÇÕES CRÍTICAS: são as informações de extrema importância para a sobrevivência da instituição;

93. INFORMAÇÃO DE ACESSO IRRESTRITO OU PÚBLICA: informação sobre a qual não recaia qualquer hipótese de limitação de acesso, ou que seja de amplo conhecimento público em razão de ato de seu titular ou de terceiros. Informação oficialmente liberada pelo Sinesp para o público geral. A divulgação deste tipo de informação não causa problemas ao Sinesp, aos seus usuários e instituições aderentes e integrantes do Sistema Único de Segurança Pública - Susp, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade;

94. INFORMAÇÃO INTERNA: informação liberada exclusivamente para usuários e departamentos específicos das instituições do Susp que fazem uso dos sistemas da Plataforma Sinesp, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização expressa;

95. INFORMAÇÃO SIGILOSA: informação sigilosa em poder dos órgãos e entidades públicas, submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e que possa, ainda, por em risco o curso de investigação ou a integridade física e/ou moral de um cidadão, assim como seus dados pessoais sensíveis. Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais no âmbito da Segurança Pública. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para o Sinesp e/ou seus usuários, bem como aos cidadãos brasileiros ou estrangeiros, portanto seu compartilhamento deve ser restrito e feito de maneira controlada;

96. INFORMAÇÃO PESSOAL: aquela relacionada à pessoa natural identificada ou identificável;

97. INFORMAÇÃO PESSOAL SENSÍVEL: informação pessoal relativa à intimidade, vida privada, honra e imagem cuja divulgação possa ensejar discriminação de seu titular, tais como convicções políticas, religiosas, orientação sexual, identidade de gênero e informações médicas;

98. INTERNET PROTOCOL - IP (PROTOCOLO DE INTERNET): é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

99. INTRANET : rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

100. INTEGRIDADE: propriedade que garante que a salvaguarda da exatidão e completeza da informação e dos métodos de processamento de forma que a informação mantém todas as características originais estabelecidas pelo proprietário;

101. IRRETRATABILIDADE (OU NÃO REPÚDIO): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

102. LOG: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

103. LOGON: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

104. MÁQUINA: Entidade do Sinesp Segurança que representa uma estação de trabalho que terão permissão de acesso para envio de lista de boletins de ocorrência, via xml (web service), para o sistema PPE (Procedimentos Policiais Eletrônicos);

105. MÍDIAS REMOVÍVEIS: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros;

106. NÍVEIS DE ACESSO: forma de controle de acesso na Plataforma Sinesp, classificados quanto ao nível de acesso em: (i) Público: acesso irrestrito e visível a todos os usuários, inclusive pelo público externo; (ii) Restrito - Unidade: acesso limitado aos usuários das Estruturas Organizacionais ou unidades em que o processo esteja aberto ou por onde tramitou; e (iii) Restrito - Usuário: acesso limitado aos usuários que possuem Credencial de Acesso na Plataforma Sinesp, em determinada Estrutura Organizacional ou unidade.

107. OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

108. OPERADOR INTERNO DO SINESP: agentes públicos, no sentido amplo, que realize atividade de tratamento de dados sob responsabilidade do Controlador Sinesp no Ministério da Justiça e Segurança Pública;

109. OPERADOR EXTERNO DO SINESP: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador Sinesp no Ministério da Justiça, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

110. PAPEL: são agrupamentos de funcionalidades pré-definidas pela área de negócios, não editáveis, atribuídos a usuários do Sinesp Segurança;

111. PAPÉIS DO SINESP SEGURANÇA: Organização lógica de um conjunto de funcionalidades do Sinesp Segurança;

112. PERFIL DE ACESSO: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

113. PERFIL DE USUÁRIO: Corresponde ao papel que o usuário exercerá dentro do sistema. Conforme o perfil, pode-se ter acesso a funcionalidades distintas. Ao ser criado um novo usuário é obrigatória a associação do mesmo a algum dos perfis existentes em cada sistema em que este usuário for vinculado;

114. PESSOA: Entidade do Sinesp Segurança que é vinculada como usuário de um ou vários Sistemas Clientes;

115. PLANO DE CONTINGÊNCIA: Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

116. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN): documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

117. PLANO DE GERENCIAMENTO DE INCIDENTES (PGI): plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes;

118. PLANO DE RECUPERAÇÃO DE NEGÓCIOS (PRC): documentação dos procedimentos e informações necessárias para que o Sinesp operacionalize o retorno das atividades críticas à normalidade;

119. PLATAFORMA SINESP (Sistema Nacional de Informações de Segurança Pública, Prisionais e de Rastreabilidade de Armas e Munições, e sobre Material Genético, Digitais e Drogas): conjunto de sistemas e aplicativos independentes desenvolvidos com a finalidade de armazenar, tratar, auditar, proteger e integrar dados e informações para auxiliar na formulação, implementação, execução, acompanhamento e avaliação das políticas relacionadas com segurança pública, sistema prisional e execução penal, bem como o enfrentamento do tráfico de crack e outras drogas ilícitas; (citar o nome completo do Sinesp);

120. POSIC - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

121. PGPPDP - POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: documento aprovado pela autoridade responsável, pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação de Privacidade e Proteção de Dados Pessoais;

122. PRÉ-CADASTRO: solicitação inicial, formulário de sistema, disponibilizado em ambiente de *web*, para preenchimento de informações pessoais, inclusão de documentação comprobatória e aceitação do respectivo termo de compromisso e confidencialidade dos dados obtidos, visando à solicitação de acesso aos sistemas do Sinesp;

123. PRIMARIEDADE: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

124. PROGRAMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;

125. PROTOCOLO: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

126. PROCESSO ADMINISTRATIVO ELETRÔNICO: aquele em que os atos processuais são registrados e disponibilizados, do início ao fim, em meio eletrônico;

127. PROPRIETÁRIO DA INFORMAÇÃO: aquele que produz a informação ou a recebe em nome da instituição;

128. 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.

129. SISTEMA CLIENTE: São os sistemas que irão se integrar ao Sinesp Segurança, de forma a receber e enviar informações necessárias para prover autenticação, autorização e auditoria;

130. SISTEMAS SINESP: conjunto de ferramentas pertencentes a Plataforma Sinesp composto dos seguintes sistemas: Sinesp Segurança, Sinesp Infoseg, Sinesp Auditoria, Sinesp CAD, Sinesp Cidadão, Rede Sinesp, Sinesp Integração, Sinesp Análise, Sinesp PPE - Procedimento Policiais Eletrônicos (Boletim Nacional de Ocorrência), Sinesp Perícia e sistemas agregados;

131. SINESP SEGURANÇA: Sistema informatizado que foi desenvolvido com o propósito específico de centralizar o controle de acessos e autenticação de usuários nos sistemas gerenciados pelo Ministério da Justiça e Segurança Pública – MJSP;

132. QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

133. RECURSO: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

134. RECURSO CRIPTOGRÁFICO: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

135. RECURSOS COMPUTACIONAIS: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

136. REDE DE COMPUTADORES: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação ou seja, existência de dois ou mais computadores , e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

137. REDE PRIVADA: conjunto de todas as redes locais sob a gestão da instituição;

138. REDE PÚBLICA: rede compartilhada por diversos usuários;

139. REDE HIBRIDA: combinação de duas ou mais redes públicas com redes privadas;

140. REPLICAÇÃO: é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;

141. RISCO: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

142. ROTULAGEM: descrição destinada a informar a qualidade ou características de um documento classificado/categorizado em conformidade com o regulamento definido na Política de Segurança da Informação ou em legislação específica;

143. RÓTULO: informação física ou eletrônica da classificação atribuída à informação;

144. SALA COFRE: é uma sala fortificada que pode ser instalada em uma instituição, provendo um local seguro de invasões e outras ameaças. São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares;

145. SALA SEGURA: sala que proporciona um ambiente seguro no *Datacenter,* oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;

146. SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade, irretratabilidade, confidencialidade e a autenticidade das informações objetivando a proteção contra ameaças para garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

147. SERVIÇO: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade atendida pelo Sinesp;

148. SERVIDOR DE REDE: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

149. SERVIDOR: pessoa legalmente investida em cargo público;

150. SISTEMAS DE INFORMAÇÃO: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

151. SISTEMA DE SEGURANÇA DA INFORMAÇÃO: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

152. SITE: Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

153. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO: todos os serviços, produtos e outros elementos necessários que se integram para o alcance dos resultados pretendidos com a contratação;

154. SOFTWARE: sistema ou componente constituído por um conjunto de programas, procedimentos e documentação desenvolvido para atendimento de necessidades específicas do órgão ou entidade, bem como aqueles previamente desenvolvidos e disponíveis no mercado para utilização na forma em que se encontram ou com modificações;

155. SOFTWARES DE MENSAGERIA: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real;

156. TRATAMENTO DA INFORMAÇÃO: conjunto de ações e toda operação realizada com dados pessoais referentes à coleta, produção, recepção, processamento, classificação, utilização, acesso, reprodução, transporte, transferência, difusão, extração, transmissão, comunicação, distribuição, arquivamento, armazenamento, eliminação, modificação, avaliação, destinação ou controle da informação;

157. TERMO DE RESPONSABILIDADE: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

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

159. TOKEN: dispositivo criptográfico de chave eletrônica, com capacidade de armazenamento de certificado digital devidamente expedido por unidade certificadora credenciada na Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil;

160. TRANSFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

161. TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS: Nos termos da Norma Complementar 05/IN01/DSIC/GSIPR, “é o serviço que consiste em receber, filtrar, classificar e

responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências";

162. TRATAMENTO DA INFORMAÇÃO: toda operação realizada com dados, 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;

163. TRILHAS DE AUDITORIA: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

164. USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador;

165. UNIDADE INFERIOR: unidade alocada abaixo, por vinculo funcional ou não, de estrutura organizacional designada;

166. UNIDADE SUPERIOR: unidade alocada acima, por vinculo funcional ou não, de estrutura organizacional designada;

167. USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

168. USUÁRIO: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do Sinesp, independente do cargo ocupado (prestadores de serviço, consultores, servidores, estagiários e etc), de forma autorizada ou monitorada;

169. VPN (VIRTUAL PRIVATE NETWORK): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito;

170. VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Documento assinado eletronicamente por **CARLOS RENATO MACHADO PAIM**, **Secretário(a) Nacional de Segurança Pública**, em 10/11/2020, às 17:54, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **13134060** e o código CRC **D2A49591**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.