SERVIÇO FLORESTAL BRASILEIRO

COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO

RESOLUÇÃO CGDSI Nº 02, DE 14 DE DEZEMBRO DE 2023

Aprova a Política de Segurança da Informação do Serviço Florestal Brasileiro.

Considerando a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

Considerando o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

Considerando a Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação;

Considerando a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC;

Considerando o constante dos autos do processo nº 02209.000418/2023-19;

Considerando as instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

O COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO, instituído pela PORTARIA SFB Nº 184, DE 01 DE DEZEMBRO DE 2023, resolve:

Art. 1º Aprovar a Política de Segurança da Informação - POSIN do Serviço Florestal Brasileiro - SFB com vistas a estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

Art. 2º Esta resolução entra em vigor na data de sua publicação.

GARO BATMANIAN
Diretor-Geral

FERNANDO CASTANHIERA NETO
Diretor de Fomento Florestal - Substituto

FLÁVIA DUARTE NASCIMENTO
Diretora de Planejamento, Orçamento e Administração

RENATO ROSEMBERG
Diretor de Concessão Florestal e Monitoramento

MARCUS VINICIUS DA SILVA
Diretor de Regularização Ambiental Rural

MOSAR RODRIGUES RABELO JUNIOR
Coordenador-Geral de Tecnologia da Informação
Gestor de Segurança da Informação

Documento assinado eletronicamente por **Flávia Duarte Nascimento**, **Diretor(a)**, em 14/12/2023, às 18:31, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Castanheira Neto**, **Diretor(a) Substituto(a)**, em 14/12/2023, às 18:52, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Mosar Rodrigues Rabelo Junior**, **Coordenador(a) - Geral**, em 14/12/2023, às 19:19, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Renato Rosenberg**, **Diretor(a)**, em 15/12/2023, às 10:53, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Garo Joseph Batmanian**, **Diretor(a) Geral**, em 15/12/2023, às 16:21, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 13 de novembro de 2020.

ANEXO I À RESOLUÇÃO CGDSI Nº 02, DE 14 DE DEZEMBRO DE 2023

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SERVIÇO FLORESTAL BRASILEIRO.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2º A Política de Segurança da Informação considera a natureza e a finalidade do SFB e está alinhada ao seu planejamento estratégico para as atividades de Gestão da Informação.

Art. 3º Para os fins do disposto nesta POSIN, conforme o art. 2º do Decreto nº 9.637, de 26 de dezembro de 2018, a Segurança da Informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física e a proteção de dados organizacionais; e

IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 4º Para efeitos de aplicação desta POSIN, são consideradas finalidades a serem garantidas pela Segurança da Informação:

I - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizado nem credenciado;

II - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

III - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizado; e

IV - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Art. 5º As ações de Segurança da Informação serão norteadas pelos seguintes parâmetros :

I - responsabilidade: o dever de cumprir as definições desta Portaria, a legislação e as normas pertinentes à Segurança da Informação vigentes;

II - clareza: as regras e as normas sobre segurança da informação deverão ser elaboradas de forma clara, precisa, concisa e de fácil entendimento

III - privacidade: preservar informação que fira o respeito, a intimidade, a integridade e a honra dos cidadãos não podendo ser divulgadas;

IV - celeridade: as ações de segurança da informação deverão oferecer respostas rápidas a incidentes e falhas;

V - ética: preserva o direito do servidor, colaborador, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação; e

VI - legalidade: deverão ser respeitados os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal e, ainda, consideradas as normas e as políticas organizacionais administrativas, técnicas e operacionais.

CAPÍTULO III

Art. 6º Para cada uma das diretrizes constantes das Seções deste Capítulo poderão ser elaboradas normas internas, metodologias ou procedimentos complementares de segurança da informação.

Art. 7º O uso e o compartilhamento de dados, informações e documentos no âmbito do Serviço Florestal Brasileiro, em todo o seu ciclo de vida, visam à continuidade de seus processos críticos em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

Art. 8º Os recursos coorporativos disponíveis para os usuários deverão ser utilizados estritamente em atividades relacionadas às suas funções institucionais.

Parágrafo único. Os responsáveis pelas unidades organizacionais do SFB poderão autorizar os acessos aos recursos de processamento de informação, conforme normas complementares que serão estabelecidas.

§ 1º É vedado a qualquer agente público do Serviço Florestal Brasileiro o uso desses recursos para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias, ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral, ou causar prejuízos a qualquer pessoa física, ou jurídica, assim como aquelas que atentem contra a moral e a ética, ou que prejudiquem o cidadão, ou a imagem desta entidade, comprometendo a integridade, a confidencialidade, a confiabilidade, a autenticidade, ou a disponibilidade das informações.

Art. 9º O sucesso das ações de segurança da informação está diretamente associado à capacitação científico - tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

Art. 10 Visando alcançar a abrangência definida no art. 3º, toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo Serviço Florestal Brasileiro é considerada ativo de informação e faz parte do seu patrimônio, observados os critérios de confidencialidade, autenticidade, disponibilidade e integridade, além do disposto no art. 16.

Parágrafo único. Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo este seguir rigorosamente o proposto. O desconhecimento desta política por parte do usuário não o isenta das responsabilidades e penalidades previstas, sendo condição *sine qua non* para acesso aos ativos de informação do SFB a adesão formal aos termos desta Política.

Seção I

Do Tratamento da Informação

Art. 11. Todo ativo de informação criada, adquirido ou custodiado, no âmbito do Serviço Florestal Brasileiro deverá ser protegido contra ameaças segundo as diretrizes descritas nesta POSIN e demais regulamentações em vigor, com o objetivo de minimizar riscos, sem prejuízo da transparência para com o cidadão.

Art. 12. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas deverão ser classificadas segundo o grau de sigilo, criticidade e outros, conforme estabelecido no Decreto nº 7.724, de 16 de maio de 2012, Lei de Acesso à Informação - LAI .

Art. 13. As informações custodiadas pelo Serviço Florestal Brasileiro deverão ser adequadamente protegidas quanto ao acesso e uso, sendo que aquelas consideradas de alta criticidade deverão receber tratamento de acordo com as definições da Gestão de Riscos em Segurança da Informação, previstas no art. 57 desta Portaria.

Art. 14. A manipulação de informações classificadas em qualquer grau de sigilo deverá seguir as normas internas de segurança da informação e o estabelecido no Decreto nº 7.724, de 16 de maio de 2012, quanto a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal.

Art. 15. As informações produzidas ou custodiadas pelo Serviço Florestal Brasileiro deverão ser descartadas conforme o seu nível de classificação, consoante regulamentação.

Art. 16. Deverá ser observado no tratamento dos dados pessoais e ou sensíveis o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.

Parágrafo único. As unidades finalísticas deverão preencher e manter atualizado o Inventário de Dados Pessoais, contendo o registro das operações de tratamento de dados pessoais que realizarem, nos termos do art. 37 da LGPD, e em conformidade com as orientações prestadas pelo Encarregado pelo Tratamento de Dados Pessoais.

Seção II

Da Segurança Física dos Equipamentos

Art. 17. A segurança física dos equipamentos e os mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis deverão ser protegidas contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Art. 18. A área responsável pela segurança organizacional e corporativa do Serviço Florestal Brasileiro deverá implementar perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos.

Art. 19. As áreas seguras serão protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

Art. 20. As áreas seguras controladas pelo Serviço Florestal Brasileiro possuirão procedimentos adequados de proteção, bem como diretrizes que orientem o trabalho no interior dessas áreas, a ser definida em norma interna de segurança da informação.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 21. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, a ser instituída por Portaria específica do dirigente máximo do Serviço Florestal Brasileiro, ficará responsável pela divulgação de práticas e recomendações de Segurança da Informação e pela avaliação das condições de

segurança de rede por meio de verificações de conformidade, com o objetivo de evitar que ocorram incidentes de segurança.

§ 1º A ETIR integrará a Rede Federal de Gestão de Incidentes Cibernéticos, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, do Gabinete de Segurança Institucional da Presidência da República, nos termos do Decreto nº 10.748, de 16 de julho de 2021.

§ 2º A atuação da ETIR será orientada por normas, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR.Gov, sem prejuízo das demais metodologias e padrões conhecidos ou que vierem aprovados pelo Comitê de Governança Digital e Segurança da Informação.

Seção IV

Gestão de Ativos da Informação

Art. 22. Os ativos da informação, sistemas e banco de dados deverão ser protegidos contra indisponibilidade, acessos indevidos, alterações, falhas, perdas, danos, furtos, roubos e interrupções não programadas.

Art. 23. Os ativos de informação deverão ser inventariados e mapeados a fim de produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos de Segurança da Informação, Gestão de Continuidade de Negócios, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas e de auditoria.

Art. 24. O processo de inventário e mapeamento de ativos de informação deve ser dinâmico, periódico e estruturado para manter a Base de Dados de Ativos de Informação atualizada para prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação.

Art. 25. Os ativos de informação fornecidos pelo Serviço Florestal Brasileiro poderão ser analisados, a qualquer tempo, pela área de tecnologia da informação a fim de assegurar o cumprimento das disposições nos art. 8º, art. 11 a 16 e art. 75 desta POSIN.

Seção V

Gestão do Uso dos Recursos de Tecnologia da Informação e Comunicações

Art. 26. Os recursos tecnologia da informação e comunicação deverão ser disponibilizados pela área de tecnologia da informação somente para usuários de informação cadastrados, mediante a utilização de credenciais individuais e intransferíveis, concedidas conforme solicitação da chefia imediata.

Art. 27. Será autorizado o uso de equipamentos pessoais em atividades institucionais somente com a implementação de soluções de segurança da informação com padrões que atendam aos princípios definidos no art. 4º, nesses equipamentos.

Art. 28. Os recursos tecnologia da informação e comunicação disponibilizados deverão ser utilizados exclusivamente para a execução de atividades institucionais.

Art. 29. Toda a informação que trafega pelos ativos de informação poderá ser monitorada de acordo com as necessidades de segurança da informação estabelecidas em norma interna de segurança da informação, conforme diretrizes desta POSIN e respeitada a legislação vigente.

Art. 30. Em caso de desligamento ou impedimento de um agente público ou colaborador que tenha executado atividades no Serviço Florestal Brasileiro, seu superior imediato poderá requisitar a recuperação de informações armazenadas em ativos de informação que estejam sob a guarda da instituição, com a finalidade de continuidade das atividades realizadas pelos mesmos.

Art. 31. Serão estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os agentes públicos e colaboradores que executem

atividades no Serviço Florestal Brasileiro, de acordo com suas competências funcionais.

Art. 32. Os investimentos em capacitações em segurança da informação deverão ser estabelecidos de forma planejada e contemplados no Plano de Desenvolvimento de Pessoas - PDP do Serviço Florestal Brasileiro, com base na priorização dos riscos a serem tratados, considerando a probabilidade, severidade e relevância deles.

Seção VI

Do Uso do E - mail institucional

Art. 33. A concessão de e-mail institucional no âmbito do Serviço Florestal Brasileiro seguindo os procedimentos definidos em norma interna de segurança da informação, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor.

Art. 34. O serviço de e - mail será oferecido como um recurso institucional para apoiar os seus usuários no cumprimento das atividades institucionais.

Art. 35. O e - mail institucional deverá ser utilizado somente para fins corporativos e relacionados às atividades do agente público ou colaborador, sendo vedado o uso para fins pessoais.

Seção VII

Do Uso e Acesso à Internet

Art. 36. A concessão de acesso à internet no âmbito do Serviço Florestal Brasileiro será limitada às atividades de trabalho do usuário de informação, seguindo os procedimentos definidos em norma interna de segurança da informação do Serviço Florestal Brasileiro, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor.

Parágrafo Único. As solicitações de exceção de acesso deverão ser justificadas pelo usuário de informação e consentidas pela autoridade hierarquicamente superior, cabendo à área de segurança da informação realizar a avaliação dos riscos da exceção para encaminhar à avaliação da aprovação final pelo Gestor de Segurança da Informação.

Art. 37. O uso da internet no Serviço Florestal Brasileiro será monitorado e os acessos serão registrados em dispositivo ou sistema computacional que assegurem ao disposto nesta POSIN.

Art. 38. As publicações oficiais na internet deverão ser autorizadas pela área responsável pelo conteúdo, observado disposto nesta POSIN.

Seção VIII

Do Serviço de Backup

Art. 39. Os procedimentos de **backup** deverão ser fixados por norma interna de segurança da informação do Serviço Florestal Brasileiro, considerando as seguintes diretrizes gerais desta POSIN.

§ 1º O serviço de **backup** deverá ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente.

§ 2º A solução de **backup** deverá ser mantida sempre atualizada, considerando suas diversas características, tais como atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros.

§3º As mídias de **backups** deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas - cofres, objetivando manter a sua segurança e integridade.

§4º A execução de rotinas de **backup** e de recuperação deverá ser rigidamente controlada, documentada e auditada, conforme norma interna de segurança da informação do Serviço Florestal Brasileiro.

Seção IX

Das Redes Sociais

Art. 40. O uso institucional das redes sociais deverá ser norteado por diretrizes, critérios, limitações e responsabilidades, em conformidade com as diretrizes desta POSIN.

Parágrafo único. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações do Serviço Florestal Brasileiro será regida por norma interna de segurança da informação do órgão, em consonância com esta POSIN e com os objetivos estratégicos deste Ministério do Meio Ambiente e Mudança do Clima.

Art. 41. Os perfis institucionais mantidos nas redes sociais deverão ser administrados e custodiados por agentes públicos autorizados pelo Serviço Florestal Brasileiro, tendo suas credenciais de acesso monitoradas pela área de tecnologia da informação a fim de assegurar o disposto nesta POSIN.

Seção X

Da Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Art. 42. As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação deverão observar os padrões, critérios e controles de segurança e seguir o estabelecido na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 e suas atualizações.

Art. 43. O apoio técnico aos processos de planejamento e avaliação da qualidade das soluções de tecnologia da informação poderá ser objeto de contratação, desde que sob supervisão exclusiva de agente público designado pela Coordenação Geral de Tecnologia da Informação do Serviço Florestal Brasileiro.

§ 1º O Termo de Referência ou Projeto Básico para contratação de soluções de tecnologia deverá conter, no que couber ao objeto contratado, requisitos e obrigações de segurança da informação e privacidade, conforme estabelecido no Anexo I - Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 e suas atualizações.

§ 2º Nos editais de licitação e nos contratos de solução de tecnologia da informação com o Serviço Florestal Brasileiro deverá constar cláusula específica sobre a obrigatoriedade de atendimento a esta POSIN, bem como que verse sobre a exigência estabelecida para empresa contratada e prestador de serviços assinarem o Termo de Responsabilidade e o Termo de Confidencialidade, conforme os Anexos II e III desta Portaria.

§ 3º A empresa contratada deverá demonstrar que possui mecanismos que assegurem a segurança das informações do Serviço Florestal Brasileiro por ela acessadas direta ou indiretamente e cumprir o disposto nesta POSIN quando aplicável.

Art. 44. Não poderá ser objeto de contratação a Gestão de Processos de Tecnologia da Informação ou a Gestão de Segurança da Informação, conforme disposto no art. 3º da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 e suas atualizações.

Art. 45. Para o uso, a aquisição ou desenvolvimento e a manutenção de sistemas de informação devem se observar:

I - não será permitido a instalação de quaisquer softwares sem licença de uso;

II - novos sistemas de informação, ou a melhoria dos sistemas existentes, devem obedecer à Metodologia de Desenvolvimento de Softwares do Serviço Florestal Brasileiro ou os guias e metodologias do SISP, bem como devem ser especificados com

requisitos de controle de segurança, e em conformidade com as especificações de requisitos estabelecidos pelas áreas requisitantes do software;

III - o gerenciamento de mudanças deve incluir a garantia de que suas implementações sejam realizadas em horários apropriados, preferencialmente, sem a perturbação dos processos de negócios cabíveis.

Art. 46. É responsabilidade dos gestores das unidades e dos gerentes de projetos, a comunicação formal à área de tecnologia da informação, quando da elaboração de iniciativas, ou de projetos que envolvam o desenvolvimento de sistemas, portais, ou de aplicativos de interesse do Serviço Florestal Brasileiro, mesmo que venham a ser desenvolvidos com o uso de recursos externos, ou mesmo quando os serviços forem executados por organizações parceiras, em sites de terceiros.

Seção XI

Do Uso de Computação em Nuvem

Art. 47. A implementação ou contratação de computação em nuvem deverá estar em conformidade com as diretrizes desta POSIN e com a legislação sobre contratação vigente na APF.

§ 1º O uso de recursos de computação em nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação será regido por norma interna de segurança da informação que deverá ser instituída pela unidade responsável pelos ativos de tecnologia e atenderá às determinações desta POSIN.

§ 2º Fica vedado o uso de recurso de computação em nuvem não disponibilizado pelo Serviço Florestal Brasileiro para o armazenamento de ativo de informação institucional.

§ 3º. Cabe ao Gestor de Segurança da Informação, no âmbito de suas atribuições, propor ações de segurança da informação para a implementação de tecnologias de computação em nuvem de forma segura.

Seção XII

Do Uso de Dispositivos Móveis

Art. 48. O uso de dispositivos móveis para acesso aos recursos computacionais do Serviço Florestal Brasileiro deverá ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso.

Parágrafo único. Norma interna de segurança da informação definirá os procedimentos específicos para o uso de dispositivos móveis institucionais, que acessarem aos ativos de informação do Serviço Florestal Brasileiro, conforme diretrizes desta Política de Segurança da Informação.

Seção XIII

Dos Controles de Acesso

Art. 49. O controle de acesso aos sistemas corporativos e o credenciamento de usuário de informações serão definidos em norma interna de segurança da informação do Serviço Florestal Brasileiro.

Art. 50. A autorização, o acesso e o uso dos ativos de informação deverão ser controlados e limitados ao necessário para o cumprimento das atribuições de cada usuário de informação.

Art. 51. A identificação do usuário de informação, qualquer que seja o meio e a forma adotados, deverá ser pessoal e intransferível, permitindo o seu reconhecimento de maneira clara, inequívoca e irrefutável.

Art. 52. Sempre que houver mudança nas atribuições de determinado usuário de informação, os seus privilégios de acesso aos ativos de informação deverão ser imediatamente readequados, devendo ser cancelados em caso de seu desligamento do Serviço Florestal Brasileiro.

Art. 53. A criação e a administração de contas serão realizadas de acordo com os procedimentos especificados em norma interna de segurança da informação do Serviço Florestal Brasileiro para todo e qualquer usuário de informação.

Art. 54. As práticas de segurança deverão contemplar procedimentos de acesso físico as áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

Art. 55. A credencial de acesso concedida a usuários de informação pela área de tecnologia da informação poderá ser revogada, a qualquer tempo, pela área de segurança da informação, em virtude do descumprimento desta POSIN ou das normas e procedimentos específicos dela decorrentes, cabendo recurso ao Gestor de Segurança da Informação.

Seção XIV

Da Gestão de Riscos em Segurança da Informação

Art. 56. A Gestão de Riscos em Segurança da Informação será instituída por norma interna de segurança da informação do Serviço Florestal Brasileiro com vistas a identificar os ativos de informação relevantes e determinar ações de gestão apropriadas.

§ 1º O processo de levantamento de riscos deverá avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com as exigências regulatórias ou legais.

§ 2º A Gestão de Riscos em Segurança da Informação deverá estar alinhada às diretrizes desta POSIN e com a unidade organizacional responsável pela Gestão de Riscos do Serviço Florestal Brasileiro, implementando, no que couber, suas diretrizes e procedimentos.

Art. 57. O Processo de Gestão de Riscos em Segurança da Informação será implementado considerando, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do Serviço Florestal Brasileiro, observadas as diretrizes e normas específicas, no âmbito da Administração Pública Federal, para fomentar sua melhoria contínua.

Seção XV

Da Gestão de Vulnerabilidades Técnicas

Art. 58. A Gestão de Vulnerabilidades Técnicas será implementada com vistas a prevenir a exploração de vulnerabilidades na rede corporativa do Serviço Florestal Brasileiro por meio da aplicação sistemática de ações de identificação, classificação e tratamento de vulnerabilidades, sendo regulamentada por norma interna de segurança da informação do SFB.

Art. 59. O processo de Gestão de Vulnerabilidades deverá assegurar que sejam disponibilizadas à Alta Administração e ao Comitê de Governança Digital e Segurança da Informação, sempre que solicitado, as informações sobre vulnerabilidades referentes aos ativos de rede e de sistemas informatizados geridos pelas áreas de tecnologia da informação, de forma a permitir a eficaz detecção e remediação de vulnerabilidades no menor tempo possível.

Art. 60. O inventário completo e atualizado dos ativos de rede e sistemas informatizados será pré-requisito para o efetivo processo de gestão de vulnerabilidades e deverá identificar, no mínimo, os ativos de hardware, software, serviços em nuvem, o grau de criticidade e o respectivo responsável pela sua gestão.

Seção XVI

Da Gestão de Continuidade de Negócios em Segurança da Informação

Art. 61. O Serviço Florestal Brasileiro deverá manter processo de Gestão de Continuidade de Negócios em Segurança da Informação que forneça estrutura a fim de permitir a continuidade das atividades e, caso sejam interrompidas, assegurar a sua retomada em tempo hábil.

Art. 62. Os ativos de informação de propriedade ou custodiados pelo Serviço Florestal Brasileiro, quando armazenados em meio eletrônico, deverão ser providos de cópia de segurança atualizada e guardada em local seguro, de forma a garantir a continuidade das atividades do órgão.

Art. 63. Deverá ser elaborado um Plano de Continuidade de Negócios em Segurança da Informação que contenha os procedimentos e as informações necessárias para que o Serviço Florestal Brasileiro mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente.

Parágrafo único. O Plano de Continuidade de Negócios em Segurança da Informação - PCN será elaborado pelo Gestor de Segurança da Informação e deverá ser testado e revisado periodicamente, de forma a se manter atualizado para responder às ameaças identificadas.

Seção XVII

Da Auditoria e Conformidade

Art. 64. O Serviço Florestal Brasileiro deverá criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos seus sistemas corporativos e à sua rede interna.

Art. 65. Deverá ser realizada, com periodicidade mínima anual, a verificação de conformidade das práticas de Segurança da Informação aplicadas no Serviço Florestal Brasileiro com esta POSIN, bem como com as normas elaboradas pelo Gabinete de Segurança Institucional da Presidência da República, em vigor.

§ 1º A verificação de conformidade também deverá ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o Serviço Florestal Brasileiro.

§ 2º A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas, simulação de intrusão e testes de invasão.

§ 3º Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade a ser elaborado pelo Gestor de Segurança da Informação.

Art. 66. Os procedimentos e as metodologias utilizados na auditoria e conformidade serão definidos em norma interna de segurança da informação do Serviço Florestal Brasileiro.

Seção XVIII

Do Proprietário da Informação

Art. 67. O dirigente máximo da unidade no Serviço Florestal Brasileiro é denominado gestor da informação, sendo o responsável primário pela sua viabilidade e sobrevivência da mesma.

Art. 68. A Informação é patrimônio do Serviço Florestal Brasileiro e toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo SFB é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

I - Toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelo colaborador e agente público do SFB, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações,

sem prejuízo da autoria, conforme definido em lei e de acordo com a norma de Classificação da Informação;

II - Quando da obtenção de informação de terceiros, o gestor da informação providenciará, junto à concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso da;

III - Na cessão de bases de dados nominais custodiadas ou na informação de propriedade do SFB a terceiros, o gestor da informação em conjunto com o gestor de segurança da informação deverão autorizar e providenciar a documentação formal relativa à autorização de acesso as informações, cabendo ao cessionário:

zelar pelo uso adequado dos dados do SICAR, observando as disposições de propriedade intelectual, bem como os aspectos relacionados à segurança da informação e aos demais dispositivos que visem à evitar o uso e à apropriação indevida dos dados do SICAR por empresa contratada ou terceiros que vierem a ter acesso aos dados

assegurar que os dados sejam tratados para uma finalidade específica de execução de políticas públicas, devidamente previstas em lei, regulamentas ou respaldadas em contratos, convênios ou instrumentos semelhantes, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei no 13.709, 14 de agosto de 2018.

assegurar que as informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas do órgão cessionário, bem como em conformidade com o tratamento de dados pessoais de acordo com as hipóteses legais exigidas na Lei no 13.709 de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.

assegurar que os dados estarão hospedados em local seguro, controlado e auditado pelo cessionário, devendo sendo monitorados e registrados todos os acessos as informações. Caso os dados sejam hospedados em ambiente de nuvem, devem ser observados os requisitos mínimos de segurança da informação previstos na Instrução Normativa GSI/PR no 5 de 30 de agosto de 2021.

adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

comunicar ao SFB e ao titular do dado, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

V - Procedimentos apropriados para garantir a conformidade dos requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e o uso de produtos de softwares proprietários de acordo com a norma de aquisição desenvolvimento e manutenção de sistemas;

VI - Privacidade e a proteção de dados que estejam em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais de acordo com a norma de proteção de dados pessoais.

§ 1º O cessionário responderá pelos danos decorrentes da violação da segurança dos dados, ao deixar de adotar as medidas de segurança previstas no art. 46 da Lei no 13.709, 14 de agosto de 2018 dando causa ao dano.

§ 2º O dirigente máximo da unidade poderá designar um servidor para atuar como proprietário da informação por ato próprio, devendo ser informado ao Comitê de Governança Digital e Segurança da Informação.

Seção XIX

Da Classificação e Tratamento da Informação

Art. 69. A classificação e o tratamento da informação observarão os seguintes requisitos e critérios:

I - o valor, requisitos legais, sensibilidade e criticidade da informação para o SFB;

II - conjunto apropriado de procedimentos para rotulação e tratamento da informação que será definido e implementado de acordo com o critério de classificação adotado pelo SFB;

Art. 70. Toda informação criada, manuseada, armazenada, transportada ou descartada do SFB será classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita;

Art. 71. A classificação e tratamento de informação serão:

I - norteadas pela legislação específica que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Publica Federal (APF);

II - Implementados e mantidos, em conformidade com a legislação vigente, visando a estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade do Ibama, ao longo do seu ciclo de vida; e

III - realizados de acordo com norma específica de classificação da informação.

Art. 72. As informações sob gestão do SFB terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento de acordo com a norma de classificação da informação;

Seção XX

Da Proteção de Dados Pessoais

Art. 73. Os dados privados, pessoais e ou sensíveis do titular, de crianças e adolescentes deverão ser processados de forma legal, justa e transparente em relação aos seus titulares e observará os seguintes:

I - Devem ser coletados para fins específicos, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses objetivos;

II - Devem estar adequados, relevantes e limitados ao uso necessário e em relação aos fins para os quais são destinados e/ou processados;

III - Quando solicitado pelo titular e/ou quando necessário, os dados devem ser atualizados;

IV - Os dados pessoais devem ser armazenados por períodos mais longos, desde que os dados pessoais sejam processados exclusivamente para arquivamento no interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos sujeitos à implementação das medidas técnicas e organizacionais apropriadas exigidas pela Lei 13.709 – LGPD;

V - Deve-se ter cuidado no tratamento de dados pessoais/privados sensíveis; e VI – As atribuições e responsabilidades do profissional responsável e/ou encarregado (DPO) pela proteção de dados pessoais/privados e informações sensíveis será exercida pelo Gestor de Segurança da Informação.

CAPÍTULO IV

Seção I

Das Competências e Responsabilidades

Art. 74. A estrutura de Gestão de Segurança da Informação no SFB será composta pelo Gestor de Segurança da Informação (GSI) e pelo Comitê de Governança Digital e Segurança da Informação (CGDSI).

Art. 75. O gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargo efetivo, empregados públicos e militares do órgão ou da entidade, com formação ou capacitação técnica compatível conforme as normas estabelecidas pelo Decreto 10.641 de 2 de março de 2021.

Art. 76. O CGDSI deverá realizar reuniões periódicas para acompanhamento das atividades de segurança institucional, avaliação do cumprimento de metas de segurança e a efetiva aplicação dessa POSIN.

Art. 77. O CGDSI poderá criar Grupos de Trabalho para realizar as seguintes atividades:

I - manter contato permanente com o Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República GSI/PR, sob supervisão do Gestor de Segurança da Informação - GSI;

II - realizar vistorias em áreas e instalações, e produzir relatórios quanto à adequação dessas áreas aos requisitos de segurança, apresentando os resultados ao GSI;

Art. 78. São competências do SFB, por meio do seu representante legal, no âmbito da POSIN:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança, por meio da Corregedoria da Instituição;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear gestor de segurança da informação;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Governança Digital e Segurança da Informação - CGDSI ;

VII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o Gabinete de Segurança Institucional da Presidência da Republica (GSI/PR).

Seção II

Do Gestor de Segurança da Informação

Art. 79. O Gestor de Segurança da Informação é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

Art. 80. Ao Gestor de Segurança da Informação compete:

I - planejar, coordenar, supervisionar, executar e controlar a execução das atividades de Tecnologia da Informação em conformidade com as diretrizes desta POSIN;

II - definir estratégias para a implementação desta POSIN e suas normas internas de segurança da informação;

III - supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de Segurança da Informação;

IV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

V - encaminhar os fatos apurados, decorrentes de quebra de segurança, para a aplicação das penalidades previstas no art. 79;

VI - gerenciar a análise de risco;

VII - verificar se os procedimentos de Segurança da Informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos;

VIII - promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os usuários de informação e aos prestadores de serviço;

IX - propor recursos necessários às ações de segurança da informação e das comunicações;

X - acompanhar as atividades da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XI - promover e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

XII - propor normas internas relativas à segurança da informação e comunicações;

XIII - promover a melhoria contínua dos processos de gestão de segurança da informação e propor ajustes corretivos a serem incluídos nas revisões desta POSIN; e

XIV - propor conteúdo sobre segurança da informação, com vistas a facilitar a capacitação e a instrução dos servidores e colaboradores para a utilização de sistemas corporativos e acesso a informações nos níveis físico e lógico, em conformidade com as diretrizes desta POSIN.

Seção III

Das Responsabilidades do Usuário de Informação

Art. 81. O Usuário de Informação é a pessoa física, servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação do Serviço Florestal Brasileiro.

Art. 82. Todo usuário de informação deverá respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Art. 83. Ao Usuário de Informação caberá:

I - acessar a rede de dados do Serviço Florestal Brasileiro somente após tomar ciência desta POSIN e das normas internas de Segurança da Informação e assinar o Termo de Responsabilidade (Anexo II);

II - manter sigilo e trocar periodicamente a senha pessoal;

III - não usar a identificação de acesso /**login** e senha de terceiros;

IV - portar crachá de identificação de maneira visível ou uniforme, para os cargos que o exigirem, dentro das instalações do Serviço Florestal Brasileiro;

V - zelar pelos equipamentos disponibilizados para a execução do seu serviço e tratar a informação digital como patrimônio do Serviço Florestal Brasileiro e como recurso que deva ter seu sigilo preservado;

VI - utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do Serviço Florestal Brasileiro exclusivamente para o interesse do serviço;

VII - preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulga - las para pessoas não autorizadas ou que não tenham necessidade de conhece - las;

VIII - não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança ou cujo teor não tenha autorização ou necessidade de conhecer;

IX - não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do Serviço Florestal Brasileiro por terceiros;

X - não utilizar o ambiente computacional do Serviço Florestal Brasileiro para acessar, transmitir, copiar ou reter conteúdo ou arquivos com textos, fotos, filmes ou quaisquer outros registros que possam causar constrangimento a terceiros ou que estejam em desacordo com a moral e a ética públicas e com a legislação vigente;

XI - não transferir qualquer tipo de arquivo que pertença ao Serviço Florestal Brasileiro para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

XII - estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não serão permitidos na rede computacional do Serviço Florestal Brasileiro;

XIII - estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do Serviço Florestal Brasileiro poderá ser auditada;

XIV - estar ciente de que o e - mail é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional do Serviço Florestal Brasileiro deverá obedecer a esse preceito;

XV - ao assinar o Termo de Responsabilidade disponível no Anexo II, o usuário de informação declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta POSIN;

XVI - utilizar as credenciais de acesso (**login** e senha) e os recursos computacionais em conformidade com a POSIN do Serviço Florestal Brasileiro e procedimentos estabelecidos em normas específicas do órgão;

XVII - informar prontamente à Central de Suporte ao Usuário caso tome conhecimento de fato que esteja em desacordo com esta POSIN ou suspeite da veracidade de mensagem ou arquivo recebidos; e

XVIII - no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso.

Seção IV

Das Responsabilidades do Custodiante da Informação

Art. 84. O Custodiante da Informação é o agente público que tem responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelo proprietário da informação.

Art. 85. Ao Custodiante da Informação caberá:

I - cumprir e zelar pela observância integral das diretrizes desta POSIN e demais normas e procedimentos decorrentes;

II - zelar pela disponibilidade, integridade, confidencialidade e autenticidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta POSIN e demais normas e procedimentos decorrentes, mediante assinatura do Termo de Responsabilidade (Anexo II);

III - participar de capacitação, treinamento ou eventos em segurança da informação promovidos pelo GSI/PR;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

V - preservar a classificação do grau de sigilo a documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções;

VI - adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito do Serviço Florestal Brasileiro; e

VII - comunicar imediatamente ao Proprietário da Informação e ao Gestor de Segurança da Informação sobre qualquer incidente que possa comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações ou sobre fato de que tenha conhecimento que esteja em desacordo com esta POSIN.

Seção V

DAS PENALIDADES

Art. 86. O Usuário de Informação responderá pelo prejuízo que vier a ocasionar ao Serviço Florestal Brasileiro em decorrência do descumprimento de uma ou mais regras desta POSIN e pelo uso indevido das suas credenciais de acesso.

Art. 87. A desobediência às regras estabelecidas nesta POSIN, por qualquer pessoa física ou jurídica, no âmbito do Serviço Florestal Brasileiro, implicará ao infrator as penalidades previstas, nos âmbitos civil e penal, quanto à tipificação criminal de delitos informáticos, conforme a Lei nº 12.737, de 30 de novembro de 2012, bem como perante a justiça administrativa, conforme a Lei nº 8.112, de 11 de dezembro de 1990.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 88. Esta POSIN e suas atualizações deverão ser divulgadas amplamente aos usuários de informações do Serviço Florestal Brasileiro.

Parágrafo único. A atualização desta POSIN, bem como todos os instrumentos normativos gerados a partir dela, deverão ser revisados e atualizados sempre que se fizer necessário, não excedendo o período máximo de quatro anos.

Art. 89. Todos os servidores, colaboradores, estagiários e demais agentes públicos ou particulares que executem atividade vinculada à atuação institucional do Serviço Florestal Brasileiro, deverão seguir o estabelecido nesta POSIN e as normas internas de segurança da informação, bem como assinar o Termo de Responsabilidade (Anexo II) quanto ao sigilo do conhecimento dos dados e informações.

Art. 90. Os agentes públicos do Ibama devem reportar à área de Tecnologia da Informação os incidentes em redes computacionais, conforme Norma Complementar no 5 da IN no 1 do Gabinete de Segurança Institucional (GSI) da Presidência da República.

Art. 91. Os casos omissos serão resolvidos pelo Comitê de Governança Digital e Segurança da Informação - CGDSI.

Art. 92. Este documento entra em vigor a partir da data de sua publicação.

ANEXO I

CONCEITOS E DEFINIÇÕES

Os conceitos e as definições utilizados nesta Política de Segurança da Informação estão contidos no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República mediante a Portaria GSI/PF nº 93, de 18 de outubro de 2021, dentre eles:

I - acesso - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

II - agente público - todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação, ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da administração pública federal, direta e indireta.

III - ameaça - conjunto de fatores externos com o potencial de causar dano para um sistema ou organização.

IV - ataque - ação que constitui uma tentativa deliberada e não autorizada para acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro ou indisponível.

V - ativos de informação - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

VI - auditoria - processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições

planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos.

VII - autenticidade - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

VIII - backup - conjunto de procedimentos que permite salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

IX - comitê de governança digital e segurança da informação - grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

X - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

XI - comprometimento - perda de segurança resultante do acesso não autorizado.

XII - confidencialidade - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados.

XIII - controlador - pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

XIV - controle de acesso - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

XV - controle de acesso à informação classificada - realizado por meio de credencial de segurança e da demonstração da necessidade de conhecer.

XVI - cópia de segurança - vide backup.

XVII - credenciamento - processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso, em função de autorização prévia e da necessidade de conhecer.

XVIII - crime cibernético - ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores, utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro.

XIX - criptografia - arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

XX - custódia - consiste na responsabilidade de guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.

XXI - custodiante da informação - qualquer indivíduo ou estrutura de órgão ou entidade da administração pública federal, direta e indireta, que tenha responsabilidade formal

de proteger a informação e aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, comunicadas pelo proprietário da informação.

XXII - dado pessoal - informação relacionada à pessoa natural identificada ou identificável.

XXIII - descarte - eliminação correta de informações, documentos, mídias e acervos digitais.

XXIV - direito de acesso - privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo.

XXV - disponibilidade - propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

XXVI - dispositivos móveis - equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e - books, notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória.

XXVII - documentos classificados - documentos que contenham informação classificada em qualquer grau de sigilo.

XXVIII - ELIMINAÇÃO - exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado.

XXIX - e - mail - sigla de correio eletrônico (electronic mail)

XXX - encarregado - pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

XXXI - equipe de prevenção, tratamento e resposta a incidentes cibernéticos - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede.

XXXII - gestão de continuidade de negócios em segurança da informação - processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

XXXIII - gestão de incidentes cibernéticos: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação do Serviço Florestal Brasileiro.

XXXIV - gestão de riscos em segurança da informação - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

XXXV - gestão de segurança da informação - processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos

institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação.

XXXVI - gestão de vulnerabilidades técnicas: processo que visa prevenir a exploração de vulnerabilidades na rede corporativa do Serviço Florestal Brasileiro por meio da aplicação sistemática de ações de identificação, classificação e tratamento de vulnerabilidades, sendo regulamentada por norma interna de segurança da informação do Serviço Florestal Brasileiro, conforme diretrizes desta Política de Segurança da Informação.

XXXVII - gestor de segurança da informação - responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

XXXVIII - gestor de segurança e credenciamento - responsável pela segurança da informação classificada, em qualquer grau de sigilo, nos órgãos de registro e postos de controle.

XXXIX - guerra cibernética - atos de guerra, utilizando predominantemente elementos de tecnologia da informação em escala suficiente, por um período específico e em alta velocidade, em apoio às operações militares, por meio de ações tomadas exclusivamente no espaço cibernético, com a finalidade de abalar ou de incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter vantagem operacional militar significativa.

XL - incidente cibernético - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema.

XLI - incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XLII - informação - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XLIII - informação classificada em grau de sigilo: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é e que pode ser classificada como ultrassecreta, secreta ou reservada.

XLIV - informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, à vida privada, à honra e à imagem.

XLV - informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado e aquela abrangida pelas demais hipóteses legais de sigilo.

XLVI - integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

XLVII - internet - rede global, composta pela interligação de inúmeras redes, provendo comunicação e informações das mais variadas áreas de conhecimento.

XLVIII - invasão - incidente de segurança no qual o ataque foi bem - sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização.

XLIX - log (registro de auditoria) - registro de eventos relevantes em um dispositivo ou sistema computacional;

L - medidas de segurança - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

LI - níveis de acesso - especificam quanto de cada recurso ou sistema o usuário pode utilizar.

LII - perfil de acesso - conjunto de atributos, de cada usuário, definidos previamente como necessários para credencial de acesso.

LIII - perfil institucional - cadastro do órgão ou entidade da administração pública federal como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação da instituição, com observância de sua correlata atribuição e competência.

LIV - política de segurança da informação - 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. Este termo substituiu o termo Política de Segurança da Informação e Comunicação.

LV - prestador de serviço - pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

LVI - rede de computadores - conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação.

LVII - redes sociais - estruturas sociais digitais, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

LVIII - reduzir risco - forma de tratamento de risco na qual a alta administração decide realizar a atividade adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

LIX - segurança cibernética - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

LX - segurança da informação - ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

LXI - serviços - meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos.

LXII - sistema de informação - conjunto de elementos materiais ou intelectuais colocado à disposição dos usuários em forma de serviços ou bens que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada.

LXIII - termo de compromisso de manutenção de sigilo - termo utilizado para garantir o sigilo de uma informação classificada em grau de sigilo em caráter excepcional, mediante assinatura de pessoa natural não credenciada ou não autorizada por legislação.

LXIV - termo de responsabilidade - termo assinado pelo usuário com a sua concordância em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

LXV - tratamento da informação - conjunto de ações referente à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição,

arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

LXVI - tratamento da informação classificada - conjunto de ações referente à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada, independente do meio, suporte ou formato.

LXVII - trilha de auditoria - registro ou conjunto de registros gravado em arquivos de log ou outro tipo de documento ou mídia que possa indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

LXVIII - 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 entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

LXIX - usuário de informação - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.