Conab Companhia Nacional de Abastecimento

Política de Segurança da Informação e Cibernética (Posic) – 10.010

Comitê Gestor de Segurança da Informação (CGSI)

GENERALIDADES

1 - Área Gestora: Comitê Gestor de Segurança da Informação (CGSI).

2 - Publicidade: Público.

3 - Histórico e vigência dos documentos de aprovação:

a) 1.ª versão: Resolução Consad n.º 045, de 17/12/2019 (vigência de 17/12/2019 a 02/02/2025);

b) 2.ª versão: Resolução Consad n.º 04, de 31/01/2025 (vigência a partir de 03/02/2025).

4 - Fontes normativas:

a) Constituição Federal (CF) 1988 – artigo 37, § 6º;

b) Lei n.º 8.159, de 8 de janeiro de 1991;

c) Lei n.º 9.609, de 19 de fevereiro de 1998;

d) Lei n.º 12.527, de 18 de novembro de 2011;

e) Lei n.º 13.709 de 14 de agosto de 2018;

f) Decreto n.º 7.724, de 16 de maio de 2012;

g) Decreto n.º 7.845, de 14 de novembro de 2012;

h) Decreto n.º 9.637, de 26 de dezembro de 2018;

i) Decreto n.º 10.046, de 9 de outubro de 2019;

j) Portaria GSI/PR n.º 93, de 18 de outubro de 2021;

k) Instrução Normativa GSI n.º 1 – Consolidada, de 27 de maio de 2020;

l) Instrução Normativa GSI n.º 3 – Consolidada, de 28 de maio de 2021;

m) Instrução Normativa GSI n.º 5, de 30 de agosto de 2021;

n) Norma Complementar n.º 5/IN01/DSIC/GSIPR, de 14 de agosto de 2009;

o) Norma Complementar n.º 8/IN01/DSIC/GSIPR, de 24 de agosto de 2010;

p) Norma Complementar n.º 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012;

q) Norma Complementar n.º 18/IN01/DSIC/GSIPR, de 10 de abril de 2013;

r) Norma ABNT NBR ISO/IEC 27001:2013;

s) Norma ABNT ISO/IEC 27002:2020;

t) Norma ABNT NBR 15247:2004;

u) Norma ABNT NBR IEC 60529:2017;

v) Norma ABNT NBR 10636-1 de 05/2022;

x) Norma ABNT NBR 17240 de 10/2010;

I - Conceitos e Definições

1 - Administrador de Rede: Pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade. Na Conab, são os Analistas de Tecnologia da Informação, lotados na Gerência de Administração e Segurança de Infraestrutura em Tecnologia da Informação (Geasi).

2 - 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.

3 - Ativo de Rede: Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

4 - 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.

5 - Autenticação: Processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo.

6 - Autenticação de Dois Fatores (2 Factor Authentication): Processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas.

7 - Autenticação de Multifatores (MFA): Utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema.

8 - 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.

9 - Comitê Gestor de Segurança da Informação (CGSI): Grupo de pessoas com a responsabilidade sobre a manutenção desta POSIC, além de assessorar a

implementação, tomada de decisão e a condução das ações de segurança da informação.

10 - Confiança Zero: Modelo de segurança criado em 2010, por John Kindervag, cujo principal conceito é não confiar em qualquer entidade interna ou externa à rede de infraestrutura de tecnologia da informação da organização. Atuando sempre com a suposição de que existam violações de segurança, esse modelo implica alteração na postura, na política e no processo da organização, visando eliminar os problemas de estratégias, com foco apenas no perímetro, por meio da adoção de três princípios básicos:

a) exigência de acesso seguro a todos os recursos, independentemente da origem da solicitação (interna ou externa) ou de quais recursos ela acesse;

b) adoção de um modelo de privilégio mínimo, com a utilização de políticas adaptativas baseadas em risco e proteção de dados, em especial, pelo controle de permissões desnecessárias e usuários inativos;

c) inspeção e registro de todos os eventos, com a aplicação de análises avançadas, para detectar e responder às anomalias em tempo real.

11 - 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.

12 - Contingência: Descrição de medidas a serem tomadas por uma organização, 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.

13 - 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.

14 - Data Center: É o local físico, normalmente dentro de uma sala-cofre ou sala segura, na qual as informações digitais, por meio de ativos de rede, são armazenadas e processadas, em condições apropriadas de segurança, climatização e limpeza.

15 - 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.

16 - 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*, USB *drives*, HD externo, e cartões de memória.

17 - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): 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 Posic 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.

18 - 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.

19 - 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.

20 - Gestor da Informação: Agente público responsável pela administração das informações produzidas em seu processo de trabalho e/ou sistemas de informação respectivo às suas atividades. Ainda, caso não seja a autoridade competente, responsável por sugerir o nível de classificação dos ativos de informação sob sua responsabilidade e fazer o devido encaminhamento à autoridade competente.

21 - 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.

22 - Informação: Dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

23 - Integridade: Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

24 - Malware: Software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de *malware* estão os vírus, *worms*, *trojans* (ou cavalos de Troia), *spyware*, *adware* e *rootkits.*

25 - Mídias Removíveis: São tipos de dispositivos de memória de armazenamento de dados que são portáveis para devido o transporte físico destes.

26 - Normas Complementares: Conjunto de normas que define e regula o uso dos recursos de tecnologia da informação e das informações no âmbito da Conab.

27 - POSIC: Política de Segurança da Informação e Cibernética.

28 - Recursos Computacionais: São entendidos como computadores, dispositivos móveis, elementos de rede, impressoras, cabeamento, sistemas e *softwares* e demais dispositivos integrantes da rede de comunicação ou nela conectados.

29 - Sala-Cofre: É uma área com alto nível de segurança projetada para armazenar e proteger informações, dados sensíveis, equipamentos críticos ou materiais de valor no ambiente de TI. Normalmente aderente conforme a norma ABNT NBR 15.247.

30 - Sala Segura: Ambiente com acesso controlado onde são armazenados os ativos de Tecnologia da Informação, normalmente situados nas Superintendências Regionais e Unidades Armazenadoras.

31 - Segurança da Informação: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

32 - Serviço de Armazenamento de Arquivos: Serviço, disponível por meio da rede computacional da Conab, no qual são armazenados os arquivos digitais produzidos pela Companhia.

33 - Sistema de Informação: Conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada.

34 - Usuário: Dirigentes, empregados, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da Conab, que poderá ser formalizada por meio da assinatura do Termo de Responsabilidade.

35 - VPN: Virtual Private Network: É uma tecnologia que cria uma conexão segura e criptografada entre um dispositivo (como um computador, *smartphone* ou *tablet*) e uma rede privada, como a internet ou uma rede corporativa.

36 - Zero Trust: Vide confiança zero.

SUMÁRIO

CAPÍTULO I – ESCOPO E ABRANGÊNCIA

Art. 1º Esta Política de Segurança da Informação e Cibernética (Posic) visa estabelecer as diretrizes para segurança da informação, asseguradas por meio da disponibilidade, integridade, confidencialidade e a autenticidade da informação.

Art. 2º Esta política se aplica aos agentes públicos que exercem, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública no âmbito da Companhia Nacional de Abastecimento (Conab).

CAPÍTULO II – PRINCÍPIOS

Art. 3º São princípios desta Posic:

I - alinhamento ao Planejamento Estratégico da Conab;

II - aderência às atuais regulamentações, legislações e normas vigentes no país relacionadas à segurança da Informação;

III - comprometimento na melhoria contínua dos processos e controles da segurança da informação, baseado nas melhores práticas reconhecidas no mercado nacional e internacional.

CAPÍTULO III – DIRETRIZES GERAIS

Art. 4º São diretrizes gerais desta Posic:

I - manter atualizados, quando viável, os mecanismos de controle e proteção utilizados pela Companhia, com vistas à segurança da informação, além de constantemente revisados para melhoria contínua dos processos e/ou ferramentas inerentes aos respectivos mecanismos;

II - observar as normas complementares e/ou específicas relativas ao gerenciamento dos ativos de informação e dos serviços de Tecnologia da Informação (TI) da Companhia;

III - definir, por meio do CGSI, os critérios de aplicação dessa política, assim como a periodicidade de sua revisão e das normas complementares e procedimentos de segurança da informação;

IV - manter pelo tempo mínimo necessário, conforme referenciado por regulamentos federais ou específicos internos, os registros a sistemas informatizados providos pela Conab, incluindo acessos, atividades, exceções e falhas;

V - compatibilizar os valores dos ativos a serem protegidos quando houver investimentos financeiros na aplicação de controles de segurança, a fim de evitar grande discrepância;

VI - contemplar a continuidade da segurança da informação no “Plano de Continuidade do Negócio” da Conab;

VII - dar ciência desta Posic para todos os empregados da Companhia que possuam acesso a sistemas da Conab, além da Norma de Recursos Computacionais;

VIII - dar ciência e fazer cumprir os agentes públicos externos à Conab, como prestadores de serviços, que executem atividade vinculada à atuação institucional e sejam usuários dos ativos de informação, devem conhecer e cumprir esta Política e demais normativos relacionados ao tema, além de preencher e assinar o Termo de Compromisso, Confidencialidade e Responsabilidade, constante na NOC 60.213, devendo também ser assinado, para ciência, pelo gestor responsável pela atividade do referido agente;

IX - garantir que o acesso dos usuários aos ativos de informação seja restrito e controlado, concedendo apenas o mínimo necessário para a execução de suas respectivas funções na Companhia.

X - promover a ampla divulgação desta Política e de suas atualizações, garantindo sua acessibilidade;

XI - definir que os usuários devem armazenar os arquivos digitais de propriedade e interesse da Companhia no serviço de armazenamento de arquivos fornecido pela área de Tecnologia da Informação;

XII - garantir que, nos eventos de encerramento de funções, contratos ou acordos de agentes públicos, os direitos de acesso às informações e aos recursos de processamento da informação sejam revogados ou ajustados conforme a mudança de função, exceto nos casos de ativos que, por razões de segurança, não estejam vinculados ao referido sistema;

XIII - garantir os recursos necessários para a execução desta Posic no âmbito da Conab, sendo a autoridade máxima da Conab a responsável por buscar e disponibilizá-los sempre que necessário;

XIV - nomear o Gestor de Segurança da Informação da Conab, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;

XV - nomear o Comitê Gestor de Segurança da Informação, responsável pelo estabelecimento dos controles para avaliação da Privacidade e Segurança

da Informação da Companhia, com o objetivo de fomentar, a identificação, o monitoramento e a conscientização situacional destes aspectos à Companhia, conforme as melhores práticas e recomendações dos Órgãos governamentais competentes;

XVI - fomentar a criação e execução de um processo contínuo de análise de vulnerabilidades cibernéticas nos sistemas e na infraestrutura de TI da Companhia, com o objetivo de identificar eventuais fraquezas e dar suporte à decisão sobre medidas de mitigação e/ou resolução.

XVII - garantir o cumprimento e operacionalização da classificação da informação conforme normativo específico;

XVIII - instituir, caso necessário, normas complementares que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação;

XIX - garantir disponibilidade, autenticidade e confidencialidade aos meios de acesso à rede computacional e aos sistemas de informação da Conab;

XX - registrar, tratar e executar respostas à incidentes cibernéticos que possam comprometer a segurança operacional da Companhia.

CAPÍTULO IV – INSTITUIÇÃO DE EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR)

Art. 5º Deve ser instituída e implementada uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

I - deverá ser elaborado documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por empregados da Companhia, alocados na Sutin e/ou gerências a ela subordinadas, com capacitação técnica compatível com as atividades da ETIR;

III - a atuação da ETIR será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo Federal, sem prejuízo das demais metodologias e padrões conhecidos.

CAPÍTULO V – DIRETRIZES ESPECÍFICAS

Seção I – Gestão de Ativos de Informação e de TI

Art. 6º Dos Ativos de informação – os elementos relacionados à informação, bem como aos recursos e procedimentos para seu processamento devem ser identificados, criando e mantendo um inventário estruturado destes. São outras diretrizes:

I - o inventário dos ativos de TI deve seguir as definições estabelecidas pela Norma de Administração e Controle do Patrimônio da Conab;

II - os ativos de informação e associados com os recursos de processamento da informação devem ter um proprietário designado pela Companhia;

III - a regulamentação no estabelecimento de critérios e procedimento para o uso dos recursos computacionais deve seguir a Norma de Recursos Computacionais da Conab;

IV - a informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade, deve seguir a Norma de Classificação de Informações em Grau de Sigilo da Conab;

V - as mudanças na infraestrutura, nos serviços e nos ativos de TI devem ser gerenciados de forma controlada, minimizando riscos e impactos negativos nas operações, devendo ser utilizado normativo específico da Companhia para esta finalidade Manual de Gerenciamento de Configuração e de Ativos de Serviço da Conab;

VI - deve ser estabelecida a gestão de dados da Companhia, visando definir e tratar a sensibilidade dos dados, o proprietário dos dados, regras de seu manuseio, de sua privacidade e acessos, dos limites de retenção e descarte de dados, além de seu respectivo inventário, classificação, fluxo e definições de proteção;

VII - as cópias de segurança dos dados digitais, com objetivo de salvaguardar os dados computacionais da Companhia, devem ser regulamentadas por meio de uma Política de Cópia de Segurança de Dados (Backup).

Seção II – Segurança Física do Ambiente de TI

Art. 7º Da Segurança Física às Áreas de TI:

I - as áreas sensíveis de TI da Companhia, como salas-cofre e salas seguras, devem possuir controle de acesso restrito e controlado, com objetivo de assegurar o acesso apenas às pessoas que possuam necessidade do

referido acesso, além de autorizadas por autoridade ou gestor da área responsável pela Segurança de TI;

II - a sala-cofre deve possuir resistência a incêndios conforme requisitos especificados na ABNT NBR 15247, tipo A. Se viável, deve possuir a respectiva certificação, sendo esta emitida por entidade devidamente acreditada pelo INMETRO;

III - a sala-cofre deve possuir IP mínimo 66 em relação ao grau de proteção provida aos invólucros dos equipamentos elétricos, conforme especificações contidas na ABNT NBR 60529. Se viável, deve possuir a respectiva certificação, sendo esta emitida por entidade devidamente acreditada pelo INMETRO;

IV - as salas seguras devem possuir resistência ao fogo, incluindo suas respectivas paredes e/ou divisórias, conforme especificações contidas na ABNT NBR 10636-1. Se viável, deve possuir a respectiva certificação, sendo esta emitida por entidade devidamente acreditada pelo INMETRO;

V - no caso de haver necessidade de entrada de prestadores de serviços e/ou visitantes à sala-cofre, é necessário haver acompanhamento presencial durante todo o período necessário, por pessoal interno da área de Segurança da Tecnologia da Informação da Companhia, a fim de monitorar, instruir e fiscalizar o ambiente e as pessoas ali presentes;

VI - o sistema de detecção e alarme de incêndio do Data Center deve obedecer aos padrões especificados nas normas da ABNT NBR 17240;

VII - a sala-cofre deve possuir controle de proteção física contra incêndios, enchentes, perturbações da ordem pública e outras formas de desastres naturais ou causadas pelo homem;

VIII - os equipamentos sensíveis de TI, como servidores de rede (de processamento) e de armazenamento de dados (*storage*), *switches*, roteadores, devem ser colocados em salas-cofre ou salas-seguras, conforme a importância do ativo, de forma a reduzir os riscos de falhas de segurança quanto ao controle de acesso e de ambiente. Em caso (s) específico (s) de inviabilidade técnica ou financeira, a alocação deve ser em sala técnica para este fim, com acesso restrito e controlado;

IX - os equipamentos contidos na sala-cofre, especificamente os servidores de processamento de sistemas e de armazenamento de dados, devem estar em operação de acordo com recomendações do respectivo fabricante, evitando sua utilização, em ambiente de produção operacional, quando não há mais suporte de peças e serviços disponível ou viável, em cada caso;

X - os equipamentos de TI, de propriedade da Conab, que operam fora de suas dependências, devem possuir requisitos mínimos de segurança cibernética implementados, considerando os riscos envolvidos em cada caso;

XI - antes do descarte de mídias de armazenamento ou de equipamentos de TI que a (s) possua (m), medidas técnicas devem ser utilizadas de forma a garantir que dados sensíveis, ou de propriedade da Companhia, sejam totalmente removidos ou sobrescritos com segurança;

XII - equipamentos de TI e Softwares, de propriedade da Companhia, não devem ser removidos do local sem autorização prévia pelo gestor competente da área de TI;

XIII - a entrada e a saída de insumos e equipamentos de TI das dependências da Companhia, devem ser controladas e autorizadas pelo gestor competente da área de TI.

Seção III – Segurança Lógica e Operacional – Ambiente Cibernético

Art. 8º Controles Operacionais:

I - os procedimentos operacionais, além dos respectivos infográficos (quando importantes para o melhor entendimento), utilizados na infraestrutura e sistemas da área de TI, devem ser documentados, preferencialmente no estilo: “como construído” (*as-built*), mantidos, atualizados e disponíveis para acesso aos usuários, da área de TI, que deles precisem em seus respectivos papéis funcionais;

II - deve haver gerenciamento da segurança das redes computacionais, de forma a prover o monitoramento, a identificação, a prevenção e as ações necessárias para a resolução de eventuais incidentes de segurança de redes.

Art. 9º Controles de Segurança Lógica:

I - os acessos aos sistemas de TI, além dos sistemas de sua infraestrutura, devem ser segregados de acordo com os papéis funcionais e necessidades específicas da área de lotação para cada agente público;

II - deve haver ambientes separados e isolados para os ambientes de operação, desenvolvimento e homologação, com níveis de acesso e controle específicos para cada caso;

III - deve ser implementado sistema atualizado para proteção contra *malwares*, a fim de proteger a integridade dos sistemas computacionais e dados digitais da Companhia;

IV - deve ser implementado e mantido sistema atualizado de prevenção contra a perda de dados digitais da Companhia *(DLP – Data Loss Prevention)*;

V - as cópias de segurança dos dados digitais, com objetivo de salvaguardar os dados computacionais da Companhia, devem ser regulamentadas por meio de uma Política de Cópia de Segurança de Dados (Backup);

VI - de modo geral, os serviços de TI devem ser estabelecidos conforme as melhores práticas de segurança do mercado, buscando garantir a confidencialidade, integridade e a disponibilidade, além de execução de registros (*log*) em cada um destes;

VII - os serviços de TI aos usuários da Companhia, internos e externos, devem ser estabelecidos conforme o conceito de "confiança zero (*Zero Trust*)", por meio de técnicas como autenticação multifatorial (MFA), segmentação de rede, limitação de portas de acesso, limitação do tipo de tráfego esperado, monitoramento contínuo de atividades e políticas de acesso baseadas em identidade e contexto;

VIII - a autenticação nos serviços web da Conab, que estão publicados e acessíveis via internet ao público geral, deve ser feita primariamente por meio de certificados digitais de governo e MFA, combinados por meio da integração com a identidade digital GOV.BR, da Secretaria de Governo Digital (SGD).

Parágrafo único. caso não seja possível ou viável a referida integração combinada de autenticação, dever-se-á utilizar, no mínimo, se viável, o recurso de MFA;

IX - o serviço de VPN deve possuir autenticação combinada com recurso de MFA Multi Fator de Autenticação (MFA), devendo o acesso de cada usuário possuir acesso apenas ao estritamente necessário ao seu trabalho;

X - o monitoramento dos sistemas computacionais da Companhia, incluindo os sistemas de infraestrutura de TI, deve ser de processado com ações visando a proatividade de resolução de eventuais problemas ou incidentes cibernéticos;

XI - os relógios dos sistemas computacionais da Companhia, especialmente os dos sistemas de infraestrutura de TI, quando possível e viável, devem ser sincronizados com relógio de precisão via rede;

XII - a criação, habilitação, desabilitação e remoção de usuários de rede, além da devida lotação na Companhia, deve ser provida por meio sistêmico integrado ao sistema de recursos humanos.

CAPÍTULO VI – RESPONSABILIDADES

Art. 10. São responsabilidades da Diretoria-Executiva da Conab:

I - fornecer os meios necessários e fazer cumprir esta Posic em toda a Companhia;

II - nomear o Gestor de Segurança da Informação, conforme inciso XIV do artigo 4º desta Política, devendo este possuir, obrigatoriamente, o cargo de Superintendente (ou equivalente) ou Diretor;

III - priorizar os recursos necessários para a implementação e gestão desta Posic na Companhia;

IV - acompanhar o CGSI e aprovar as estratégias definidas para a criação, implantação e atualização desta Política;

V - analisar e manifestar-se sobre o CGSI e a Posic, com posterior encaminhamento ao Conselho de Administração, caso necessário;

VI - instituir e nomear a ETIR da Conab, conforme Capítulo IV desta Política, além de apoiar no fornecimento de recursos de pessoal e financeiros, especialmente para melhoria de infraestrutura e treinamentos de aperfeiçoamento técnico, quando necessário.

Art. 11. São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI):

I - assessorar a implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Posic e das normas internas de segurança da informação

IV - avaliar, propor e deliberar, continuamente, sobre alterações desta Política e demais normas internas de Segurança da Informação da Conab;

V - deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade;

VI - avaliar, propor, deliberar e estabelecer os controles, indicadores e respectivos relatórios, para acompanhamento e consciência situacional da implementação da Privacidade e Posic na Companhia;

VII - solicitar à autoridade competente a constituição de grupos de trabalho para tratar de temas e propor soluções específicas de Segurança da Informação;

VIII - propor a adoção de ações de conscientização e capacitação de pessoal, visando difundir os conhecimentos e dar efetividade à Posic;

IX - receber das unidades orgânicas da Conab informações sobre dificuldades relativas à implementação e ao cumprimento desta Política;

X - compartilhar informações sobre novas tecnologias, produtos, ameaças, vulnerabilidades, gerenciamento de risco, políticas de segurança e outras atividades relativas à segurança corporativa com outros órgãos e empresas públicas, de modo a prover a Companhia do conhecimento das práticas mais modernas e adequadas para a proteção de suas informações;

XI - deliberar sobre propostas de medidas destinadas ao desenvolvimento da Segurança da Informação;

XII - comparecer às reuniões do CGSI, quando convocado;

XIII - elaborar relatório, contendo o resultado dos estudos realizados, bem como recomendações para as soluções dos problemas relativos às questões que se destinam ao desenvolvimento da Segurança da Informação;

XIV - as reuniões do CGSI devem ser registradas em Ata específica, assinada por todos os membros presentes e com ciência dos demais integrantes;

XV - avaliar, propor e deliberar sobre normativos, indicadores e demais assuntos relacionados ao estabelecimento e operação do ETIR da Conab.

Art. 12. São responsabilidades do Gestor da Informação:

I - tratar, definir os requisitos de segurança, conceder e revogar acessos e compartilhar, os ativos de informação sob sua responsabilidade, conforme normas específicas.

Art. 13. São responsabilidades do Gestor de Segurança da Informação:

I - coordenar a elaboração da Posic e das normas internas relacionadas à segurança da informação da Conab, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República e as melhores práticas sobre o assunto no mercado;

II - assessorar a alta administração na implementação da Posic;

III - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

V - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VI - propor recursos necessários às ações de segurança da informação;

VII - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

VIII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

IX - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

X - ser o contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

XI - atuar junto as gerências de tecnologia de informação na definição de padrões e boas práticas na gestão de ativos digitais;

XII - apresentar ao CGSI e a diretoria executiva indicadores, relatórios e ações relacionadas as atividades de gestão de segurança da informação;

XIII - coordenar as ações para a implementação operacional e de infraestrutura para o devido funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Art. 14. São responsabilidades da ETIR:

I - realizar as atividades de prevenção, de tratamento e de resposta a incidentes cibernéticos em seu âmbito de atuação;

II - apoiar a condução de políticas de segurança cibernética e da informação;

III - priorizar a continuidade dos serviços corporativos;

IV - realizar ações voltadas para o fortalecimento da resiliência cibernética da Conab;

V - comunicar ao CTIR Gov a ocorrência de incidentes cibernéticos, de acordo com seu modelo de atuação e com a maior brevidade possível;

VI - manter registro histórico de incidentes cibernéticos e vulnerabilidades que permitam a geração de dados estatísticos.

CAPÍTULO VII – SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 15. As unidades da Conab devem seguir e manter um processo interno, contínuo, com objetivo de divulgação das normas e procedimentos inerentes à segurança da informação, além de conscientizar e sensibilizar seus usuários à correta conduta na utilização das informações da Conab, realizando capacitação quando necessário.

CAPÍTULO VIII – DO CUMPRIMENTO DESTA POLÍTICA

Art. 16. É dever de todos os agentes públicos da Conab, conforme suas respectivas atribuições, cumprir esta Política. O seu descumprimento poderá ensejar a apuração de responsabilidades, com base nos normativos internos e na legislação vigente, garantindo o contraditório e a ampla defesa.

CAPÍTULO IX – COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI)

Art. 17. O Comitê Gestor da Segurança da Informação será composto permanentemente com os titulares das áreas:

I - Gestor de Segurança da Informação;

II - Superintendência de Estratégia e Organização;

III - Superintendência de Marketing e Comunicação;

IV - Superintendência de Gestão de Riscos, Conformidade e Controles Internos;

V - Superintendência de Administração;

VI - Superintendência de Gestão da Oferta;

VII - Superintendência de Gestão da Tecnologia da Informação;

VIII - Superintendência de Operações Comerciais;

IX - Superintendência de Relações do Trabalho; e

X - Encarregado pelo Tratamento de Dados Pessoais.

Art. 18. Do funcionamento do CGSI:

I - os suplentes institucionais de cada membro serão os próprios substitutos dos titulares;

II - caso o Comitê verifique a necessidade da participação de outras áreas, poderá pedir a designação de um novo membro por Portaria ou convidar para participação sem direito a voto;

III - as deliberações do Comitê serão aprovadas por maioria simples dos membros presentes. Em caso de empate, o Gestor de Segurança da Informação terá, além do voto regular, o voto de desempate;

IV - o Comitê estipulará sobre: a periodicidade de suas reuniões, o membro secretário do Comitê, o sistema de votação das pautas e a forma de funcionamento, observada a legislação pertinente ao assunto, por meio de normativo interno.

CAPÍTULO X – DA REVISÃO DESTA POLÍTICA

Art. 19. Esta Política deve ser revisada no período máximo de 2 (dois) anos, caso não ocorram novas legislações, normativos governamentais ou fatos relevantes que exijam uma revisão antes deste tempo. Devendo ser atualizada adequadamente.

CAPÍTULO XI – DA PUBLICIDADE E DIVULGAÇÃO

Art. 20. Essa Política deve estar pública e disponível nos canais de comunicação internos e externos da Companhia.

CAPÍTULO XII – DISPOSIÇÕES GERAIS

Art. 21. O tratamento de dados pessoais que derivar do cumprimento desta Política, deverá acontecer em conformidade à Lei n.º 13.709 de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD). (Texto incluído pela Resolução Consad n.º 014, de 23/07/2021).

Art. 22. Os casos omissos e as dúvidas com relação a esta Política serão submetidos ao Comitê Gestor de Segurança da Informação, que avaliará a necessidade de encaminhar à Diretoria-Executiva para deliberação.