Conab Companhia Nacional de Abastecimento

Política de Segurança da Informação – 10.010

Aprovada em 17/12/2019

Comitê Gestor de Segurança da Informação

IDENTIFICAÇÃO GERAL E SUBSCRIÇÃO

CNPJ (Matriz):	26.461.699/0001-80
Sede:	Brasília /DF
Tipo de estatal:	Empresa pública
Lei de criação:	Lei N.º 8.029/1990
Acionista controlador:	Governo Federal
Tipo de capital:	Fechado
Abrangência:	Nacional
Setor de atuação:	Informações, agricultura e abastecimento
Responsável pela política:	Newton Araújo Silva Júnior presidencia@conab.gov.br (61) 3312-6301
Auditor Interno:	Marcelo Henrique Coelho audin@conab.gov.br (61) 3312-6320
Auditor Independente:	Tanagildo Aguiar Feres aguiarferes@aguiarferes.com.br (16) 3632-3100
Conselheiros de Administração subscritores da Política:	Maximiliano Ferreira Tamer Silvio Farnese Paulo Marcio Mendonça Araújo Antônio Sávio Lins Mendes Fernando Coimbra Júnior Eudes de Gouveia Varela Francisco de Assis Xavier Segundo
Diretores subscritores da Política:	Newton Araújo Silva Júnior Diretor-Presidente Bruno Scalon Cordeiro Diretor-Executivo de Operações e Abastecimento Cláudio Rangel Pinheiro Diretor-Executivo de Gestão de Pessoas Guilherme Soria Bastos Filho Diretor-Executivo de Política Agrícola e Informações José Ferreira da Costa Neto Diretor-Executivo Administrativo, Financeiro e de Fiscalização
Data de divulgação:	26/12/2019

SUMÁRIO

CAPÍTULO I - ESCOPO (Art. 1.º)…….3

CAPÍTULO II - ABRANGÊNCIA (Art. 2.º)……3

CAPÍTULO III - CONCEITOS E DEFINIÇÕES (Art. 3º)……...3

CAPÍTULO IV - DIRETRIZES E ORIENTAÇÕES GERAIS (Art. 4.º)……..5

CAPÍTULO V - DIRETRIZES ESPECÍFICAS (Arts. 5.º ao 34)……...7

Seção I - Gestão de Ativos de TI e Informações (Arts. 5.º ao 8.º)…..……7

Seção II - Segurança Física e do Ambiente de TI (Arts. 9.º ao 17) ……..8

Seção III - Gerenciamento das Operações e Comunicações (Arts. 18 ao 30)……...9

Seção IV - Controle de Acessos (Arts. 31 ao 34)……11

CAPÍTULO VI - RESPONSABILIDADES (Arts. 35 ao 37)……...12

CAPÍTULO VII - SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO (Art. 38)……13

CAPÍTULO VIII - DO DESCUMPRIMENTO DA POLÍTICA (Arts. 39 ao 41)……...14

CAPÍTULO IX - COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI) (Art. 42)……14

CAPÍTULO X - ATUALIZAÇÃO (Art. 43)……...15

CAPÍTULO XI - DIVULGAÇÃO (Art. 44)…….15

CAPÍTULO XII - DISPOSIÇÕES FINAIS (Arts. 45 e 46)……...16

CAPÍTULO XIII - REFERÊNCIAS LEGAIS (Art. 47)……...16

CAPÍTULO I

ESCOPO

Art. 1º Tem por finalidade estabelecer as diretrizes para a segurança da utilização, tratamento, controle e proteção das informações, conhecimentos e dados produzidos, armazenados ou transmitidos, por quaisquer meios, devendo tais diretrizes serem observadas na definição de regras operacionais e procedimentos no âmbito da Companhia Nacional de Abastecimento (Conab).

CAPÍTULO II

ABRANGÊNCIA

Art. 2º Todas as unidades administrativas da Conab, seus dirigentes, empregados e demais agentes públicos ou privados que, oficialmente, executem atividade vinculada à atuação institucional da Companhia.

CAPÍTULO III

CONCEITOS E DEFINIÇÕES

Art. 3º Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Companhia, com vistas à garantia dos princípios da disponibilidade, integridade, confidencialidade e autenticidade. São conceitos e definições utilizados nesta Política:

I - Administradores de Rede – são os Analistas de Tecnologia da Informação (TI) lotados na área de Administração de Rede da Matriz;

II - Agente público: pessoa que exerce, com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer forma de investidura ou vínculo, mandato, cargo, emprego ou função pública, ainda que transitoriamente;

III - Ativos de Tecnologia da Informação (TI) – itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas;

IV - Autenticação – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação sobre um objeto é verdadeira;

V - Autenticidade – a certeza de que o objeto em análise provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo;

VI - Comitê Gestor de Segurança da Informação (CGSI) – grupo de pessoas com a responsabilidade de assessorar a implementação, tomada de decisão e a condução das ações de segurança da informação;

VII - Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

VIII - 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;

IX - Controle de Acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

X - Data Center – é o local onde são armazenadas, em condições apropriadas de segurança, climatização e limpeza, os ativos que subsidiam as atividades de Tecnologia da Informação da Conab, compreendendo sala-cofre ou sala-segura;

XI - Disponibilidade – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XII - Gestão de Continuidade de Negócios – processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizados, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço em face de rupturas e desafios à operação normal do dia a dia;

XIII - Gestão de Segurança da Informação – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIV - Gestor da Informação – pessoa responsável pela administração de informações produzidas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

XV - Incidentes de Segurança da Informação – qualquer evento adverso, confirmado ou sob suspeita;

XVI - Informação – é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação, seja ela quantitativa ou qualitativa no conhecimento do sistema que a recebe;

XVII - Integridade – fidedignidade de informações, propriedade que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XVIII - Mídias removíveis – são tipos de dispositivos de memória que podem ser removidos do seu aparelho de leitura, conferindo portabilidade para os dados que carrega;

XIX - Normas Complementares – conjunto de normas que define e regula o uso dos recursos de tecnologia da informação e das informações;

XX - Protocolo de Rede – são procedimentos que controlam e regulam a comunicação, conexão e transferência de dados entre sistemas computacionais;

XXI - 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;

XXII - Sala-cofre – ambiente de TI certificado conforme as normas ABNT NBR 15.247, protegido de desastres;

XXIII - Sala-segura – ambiente com acesso controlado onde são armazenados os ativos de TI, normalmente situados nas Superintendências Regionais e Unidades Armazenadoras;

XXIV - Segurança da Informação – proteção sobre as informações de uma determinada instituição ou pessoa. É a proteção da informação contra vários tipos de ameaças, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXV - Serviços de Rede – são um conjunto de facilidades providas por meio de protocolos de rede e *softwares* que, combinados, ofertam ao usuário meios de comunicação, manipulação e armazenamento de dados;

XXVI - Servidor de arquivos – servidor onde são armazenados os arquivos produzidos pelos empregados, independente de sua tecnologia de armazenamento;

XXVII - Sistemas de Informação – são um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informações, com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em organizações;

XXVIII - Usuários – 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.

CAPÍTULO IV

DIRETRIZES E ORIENTAÇÕES GERAIS

Art. 4º São diretrizes gerais da Política de Segurança da Informação:

I - todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos, visando preservar a continuidade do negócio;

II - o gerenciamento dos ativos de informação deverá observar as normas complementares e procedimentos específicos, a fim de garantir sua operação segura e contínua;

III - a periodicidade e critérios serão definidos pela CGSI visando o cumprimento dessa Política, bem como das normas complementares e procedimentos de segurança da informação;

IV - a Conab deve criar e manter registros e procedimentos que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e da rede interna da Companhia;

V - as medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com o valor do ativo protegido;

VI - o Plano de Continuidade de Negócios da Conab deverá abarcar os assuntos relativos à Segurança da Informação;

VII - todos os conselheiros, dirigentes, empregados, estagiários e demais colaboradores da Companhia que sejam usuários dos ativos de informação, sendo eles sigilosos ou não, deverão ter ciência quanto ao correto uso dos dados, informações e conhecimentos produzidos pela Conab;

VIII - os agentes externos, públicos ou particulares, que executem atividade vinculada à atuação institucional e sejam usuários dos ativos de informação, sendo eles sigilosos ou não, deverão ter ciência quanto ao correto uso dos dados, informações e conhecimentos produzidos pela Conab, devendo preencher o “TERMO DE COMPROMISSO E RESPONSABILIDADE” constante de Norma específica, que por sua vez deverá ser assinado pelo gestor responsável pela atividade do referido agente;

IX - os dirigentes, empregados e colaboradores da Companhia, possuem a responsabilidade pela segurança, integridade e qualidade da informação, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da Conab;

X - todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

XI - todos os usuários devem manter as informações produzidas em meio digital, armazenadas em servidor de arquivos, de modo que os dados possam ser objeto de cópia de segurança automática;

XII - quando do desligamento, cessão, afastamento temporário, mudança de responsabilidades e de lotação ou atribuições dentro da organização, faz-se necessária a revogação ou revisão imediata dos direitos de acesso e uso dos ativos de forma automática, por meio de informação obtida diretamente do sistema de gestão de pessoas, excetuando aqueles ativos que, por questões de segurança, não estejam vinculados ao referido sistema;

XIII - todo ativo informacional relacionado à atividade da Companhia deverá ser mantido pelos empregados e demais colaboradores nas dependências e servidores de arquivos da Conab, garantindo o reconhecimento e o esclarecimento da propriedade do acervo pertencente à Companhia;

XIV - as informações custodiadas ou de propriedade da Conab, inclusive nos sistemas de informação, devem ser classificadas quanto aos aspectos de sigilo, sendo garantidas a disponibilidade e a integridade de forma implícita ou explícita, recebendo o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor;

XV - o gestor da informação é responsável por sugerir o nível de classificação das informações sob sua responsabilidade e encaminhá-lo formalmente à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) para que, após análise e classificação pelo agente público competente, possa ser enviado à área de Tecnologia da Informação o tarjamento automático daquelas informações classificadas constantes dos sistemas de informação;

XVI - a classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte;

XVII - todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade da Conab e, a partir dela, conhecer e obedecer as restrições de acesso e divulgação associadas;

XVIII - de forma a promover a gestão e fomentar os aspectos de segurança da informação, a Companhia deve instituir normas complementares que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação;

XIX - o acesso à rede computacional e aos sistemas de informação da Conab depende de autenticação por meio de usuário, senha e outros elementos que possam vir a ser estabelecidos pelo CGSI;

XX - a Conab registrará os acontecimentos não rotineiros que ocorrerem durante ou fora do expediente de serviço, identificando possíveis causas do comprometimento da segurança física dos bens ou da informação.

CAPÍTULO V

DIRETRIZES ESPECÍFICAS

Seção I

Gestão de Ativos de TI e Informações

Art. 5º Responsabilidade pelos Ativos de TI e Informações – alcançar e manter a proteção adequada dos ativos de TI da organização. O inventário físico dos ativos de TI seguirá as definições estabelecidas pela Norma ADMINISTRAÇÃO E CONTROLE DO PATRIMÔNIO – 60.202.

Art. 6º Proprietário dos Ativos de TI – todas as informações e ativos de TI associados com os recursos de processamento da informação devem ter um proprietário designado formalmente pela organização.

Art. 7º Uso aceitável dos Ativos de TI – devem ser identificadas, documentadas e implementadas, regras para que seja permitido o uso de informações e de ativos de TI, conforme estabelecido na Norma RECURSOS COMPUTACIONAIS – 60.213.

Art. 8º Classificação da Informação – assegurar que a informação recebe um nível adequado de proteção, utilizando a Norma CLASSIFICAÇÃO DE INFORMAÇÕES EM GRAU DE SIGILO – 10.303. A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a Companhia. Na classificação da informação deve-se buscar o grau de segurança menos restritivo possível, visando otimizar e agilizar o processo de tratamento e reduzir os custos com sua proteção.

Seção II

Segurança Física e do Ambiente de TI

Art. 9º Áreas Seguras – prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações no ambiente de TI. Para a entrada física nas áreas seguras devem ser utilizados perímetros de segurança e protegidas por controles apropriados de entrada para assegurar que só tenham acesso as pessoas autorizadas. A sala-cofre deve ser certificada atendendo a todos os requisitos da norma ABNT NBR 15.247 e NBR 60.529 com IP mínimo 66. A certificação deverá ser emitida por organismo devidamente acreditado no INMETRO.

Art. 10. Acesso ao *Data Center* – qualquer concessão de acesso será autorizada pelo gestor da área responsável pela Segurança da Tecnologia da Informação da Conab e revisadas mensalmente. Caso tenha a entrada de prestadores de serviços e visitantes no ambiente do *Data Center* deve ser sempre acompanhada por pessoal interno da área de Segurança da Tecnologia da Informação, que se responsabilizará pelas ações do terceiro no ambiente. O sistema de combate a incêndio do *Data Center* deve obedecer aos padrões especificados nas normas da ABNT 9.441.

Art. 11. Proteção Contra Ameaças Externas e do Meio Ambiente – devem ser projetadas e aplicadas proteções físicas contra incêndios, enchentes, perturbações da ordem pública e outras formas de desastres naturais ou causadas pelo homem.

Art. 12. Segurança de Equipamentos – impedir perdas, danos, furto ou comprometimento de ativos de TI e interrupção das atividades da Companhia. Os equipamentos devem ser colocados em local apropriado ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Art. 13. Controle de Acesso Lógico – o acesso lógico será autorizado pela área de Segurança da Tecnologia da Informação no ambiente da Matriz e das Superintendências Regionais.

Art. 14. Manutenção dos Equipamentos – os equipamentos devem receber manutenção, conforme indicação do fabricante, para assegurar sua disponibilidade e integridade permanente.

Art. 15. Segurança de Equipamentos Fora do Local – devem ser tomadas medidas de segurança para equipamentos que operem fora das dependências da Conab, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora dos domínios da Companhia.

Art. 16. Reutilização e Alienação Seguras de Equipamentos – todos os equipamentos que contenham suportes físicos de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.

Art. 17. Remoção de Propriedade – equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia. A entrada e a saída de insumos e equipamentos de TI nas instalações do *Data Center* e salas-seguras devem ser controladas e autorizadas pela gerência responsável pela carga patrimonial dos equipamentos.

Seção III

Gerenciamento das Operações e Comunicações

Art. 18. Procedimentos e Responsabilidades Operacionais – garantir a operação segura e correta dos recursos de processamento da informação. Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

Art. 19. Segregação de Funções – as funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos de TI da Companhia. O acesso ao ambiente de produção deve ser diferente do acesso aos ambientes de desenvolvimento e homologação.

Art. 20. Separação dos Recursos de Desenvolvimento, Teste e de Produção – os recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

Art. 21. Gerenciamento de Serviços Terceirizados – implementar e manter o nível apropriado de segurança da informação dos serviços terceirizados. A contratada deve conhecer e cumprir a Política, diretrizes e práticas de Segurança da Informação estabelecidas pela Companhia, assinando o “TERMO DE CONFIDENCIALIDADE” constante em Norma específica. A Companhia deve possuir o direito de auditar os serviços ou atividades contratadas.

Art. 22. Proteção Contra Códigos Maliciosos e Códigos Móveis – proteger a integridade do *software* e da informação. Implantar controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Art. 23. Cópias de Segurança – manter a integridade e disponibilidade da informação e dos recursos de processamento de informação. As cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente e armazenadas em ambientes seguros, protegidos em meio que previna a ação de desastres naturais ou ações deliberadas, preferencialmente em dois locais diferentes sendo um em ambiente

controlado próximo ao *Data Center* ou sala-segura e outro em ambiente remoto, de modo a mitigar o risco de perda destas informações.

Art. 24. Gerenciamento da Segurança em Redes – garantir a proteção das informações em redes e a proteção da infraestrutura de suporte. As redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito. As características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente ou terceirizados.

Art. 25. Manuseio de Mídias – prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos de TI e interrupções das atividades do negócio. Devem existir procedimentos implementados para o gerenciamento de mídias removíveis. As mídias devem ser descartadas de forma segura e protegida, quando não forem mais necessárias, por meio de procedimentos formais, sendo responsável pelo descarte adequado aquele empregado que o está realizando. Para o manuseio de mídias deve ser observada a Norma RECURSOS COMPUTACIONAIS – 60.213.

Art. 26. Serviços de Comércio Eletrônico – garantir a segurança de serviços de comércio eletrônico ofertado pela Conab e sua utilização segura. As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas. As informações envolvidas em transações *on-line* devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada. A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida para prevenir modificações não autorizadas.

Art. 27. Monitoramento – detectar atividades não autorizadas de processamento da informação. Os registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo definido pelo proprietário da informação ou prazo legal para auxiliar em futuras investigações e monitoramento de controle de acesso. Todos os recursos de tecnologia da informação deverão ser configurados para gerarem registros de eventos (logs), exceto quando houver limitação técnica.

Art. 28. Trilhas de auditoria – devem ser usadas para determinar se uma violação de política de segurança aconteceu ou se uma atividade suspeita é causa para alarme, possibilitando a localização de um possível incidente de segurança e sua fonte, fornecendo rastreabilidade e evidências necessárias para qualquer ação que pode ser requerida. Os registros de eventos (logs) devem ser periodicamente analisados. A periodicidade e o detalhamento da análise devem ser determinados com base na sua classificação, considerando a criticidade, valor e sensibilidade das informações envolvidas. Os registros de eventos (logs) devem ser mantidos por tempo determinado, de acordo com os requisitos legais, regulamentares, contratuais e a sua classificação.

Art. 29. Monitoramento do Uso do Sistema – devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente de forma regular.

Art. 30. Sincronização dos Relógios – os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com o horário oficial local.

Seção IV

Controle de Acessos

Art. 31. Gerenciamento de Acesso do Usuário – assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação. Todos os usuários da Conab serão criados ou bloqueados com base nos eventos gerados pelo cadastro do empregado no sistema de recursos humanos em execução pela Conab. Todos os usuários devem possuir o menor nível de acesso necessário para o desempenho de suas funções.

Art. 32. Responsabilidades dos Usuários – responsabilidade pelo acesso seguro e adequado aos recursos computacionais disponíveis.

I - Uso de Senhas – os usuários devem ser orientados a seguir boas práticas de segurança na seleção e uso de senhas:

a) as identificações e as senhas são de uso pessoal e intransferível, sendo vedado ao titular compartilhá-las ou fornecê-las a terceiros;

b) quando houver suspeita de vazamento ou uso não autorizado da senha do usuário, a área de Segurança de Tecnologia da Informação deve ser comunicada imediatamente e a senha do usuário afetado deve ser alterada;

c) é proibido aos usuários com perfis de administrador de um recurso de TI utilizar essa característica em benefício próprio ou de terceiros;

II - Equipamento de Usuário sem Monitoramento – os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada:

a) as estações de trabalho somente devem ser utilizadas para execução de atividades de interesse da Conab e com *softwares* homologados e autorizados pela área de Tecnologia da Informação;

b) o usuário não deve alterar as configurações padronizadas pela área de Tecnologia da Informação e não pode, em hipótese alguma, abrir o gabinete das estações de trabalho nem modificar a configuração do *hardware*;

c) o usuário deve informar a área de Suporte Técnico, na Matriz ou nas Superintendências Regionais e Unidades Armazenadoras, quando identificada violação da integridade física do equipamento por ele utilizado.

Art. 33. Controle de Acesso à Rede – prevenir acesso não autorizado aos serviços de rede.

I - Uso dos Serviços de Rede – os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar;

II - Autenticação para Conexão Externa do Usuário – métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos;

III - Identificação de Equipamento em Redes – devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos;

IV - Segregação de Redes – grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes;

V - Controle de Conexão de Rede – para redes compartilhadas, especialmente as que se estendem além dos limites da Conab, a capacidade de usuários para conectar a rede deve ser restrita, de acordo com a política de controle de acesso e os requisitos das aplicações do negócio;

VI - Controle de Roteamento de Redes – deve ser implementado controle de roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.

CAPÍTULO VI

RESPONSABILIDADES

Art. 34. São responsabilidades da Diretoria Executiva da Conab:

I - cumprir e fazer cumprir esta Política de Segurança da Informação;

II - designar o Gestor de Segurança da Informação interno, sendo obrigatoriamente Superintendente (ou equivalente) ou Diretor;

III - priorizar os recursos necessários para a implementação e gestão da Política de Segurança da Informação 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 Política de Segurança da Informação, com posterior encaminhamento ao Conselho de Administração, caso necessário.

Art. 35. São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI):

I - propor a adequação da Política e a criação ou alteração das normas aderentes à Segurança da Informação da Conab;

II - propor normativos e indicadores para acompanhar e avaliar a implementação da Política de Segurança da Informação;

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

IV - propor a adoção de ações de conscientização e capacitação de pessoal, visando difundir os conhecimentos e dar efetividade à Política de Segurança da Informação;

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

VI - 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.

Art. 36. São responsabilidades do Gestor da Informação:

I - tratar a informação;

II - definir os requisitos de segurança para os ativos sob sua responsabilidade;

III - conceder e revogar acessos;

IV - autorizar a divulgação de informações, conforme normas específicas.

CAPÍTULO VII

SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 37. Todas as unidades da Conab deverão manter um processo permanente de divulgação de suas normas e procedimentos para capacitar, conscientizar e sensibilizar seus usuários à correta conduta na utilização das informações da Conab.

CAPÍTULO VIII

DO DESCUMPRIMENTO DA POLÍTICA

Art. 38. O não cumprimento das diretrizes desta Politica poderá ensejar na apuração de responsabilidade com base nos normativos internos e legislação em vigor.

Art. 39. O descumprimento das disposições constantes nesta Política e nas Normas Operacionais sobre Segurança da Informação caracteriza infração funcional, a ser verificada em processo administrativo, sem prejuízo das responsabilidades penal e civil.

Art. 40. A autoridade competente obedecerá, dentre outros, aos princípios da legalidade, motivação, razoabilidade, proporcionalidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência.

CAPÍTULO IX

COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI)

Art. 41. O Comitê Gestor da Segurança da Informação será composto permanentemente com os titulares das áreas:

I - Gestor de Segurança da Informação;

II - Chefe de Gabinete;

III - Procuradoria-Geral;

IV - Superintendência de Acompanhamento das Regionais;

V - Superintendência de Administração;

VI - Superintendência de Armazenagem;

VII - Superintendência de Estratégia e Organização;

VIII - Superintendência de Gestão da Oferta;

IX - Superintendência de Gestão da Tecnologia da Informação;

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

XI - Superintendência de Informações do Agronegócio;

XII - Superintendência de Marketing e Comunicação;

XIII - Superintendência de Operações Comerciais; e

XIV - Superintendência de Relações do Trabalho.

§ 1º - Os suplentes de cada membro serão os próprios substitutos dos titulares.

§ 2º - 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.

§ 3º - 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.

§ 4º - O Comitê estipulará a periodicidade das reuniões ordinárias e extraordinárias, 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

ATUALIZAÇÃO

Art. 42. Essa Política deve ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

CAPÍTULO XI

DIVULGAÇÃO

Art. 43. Após a publicação desta Política, ela estará disponível permanentemente nos canais de comunicação interno e externo da Conab a todos os usuários.

CAPÍTULO XII

DISPOSIÇÕES GERAIS

Art. 44. O tratamento de dados pessoais que derivar do cumprimento deste instrumento, deverá acontecer em conformidade à Lei Geral de Proteção de Dados Pessoais, Lei Nº 13.709/2018. (Texto incluído pela Resolução Consad n° 14, de 23/7/2021).

Art. 45. 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.

Art. 46. Esta Política entra em vigor, conforme as alterações aprovadas:

I - Resolução Conad N.º 045, de 17/12/2019.

CAPÍTULO XIII

REFERÊNCIAS LEGAIS

Art. 47. Referências Legais e Normativas:

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

II - Lei N.º 8.159, de 8 de janeiro de 1991; Lei N.º 9.609, de 19 de fevereiro de 1998; Lei N.º 9.609, de 19 de fevereiro de 1998; Lei N.º 12.527, de 18 de novembro de 2011; Lei N.º 13.709 de 14 de agosto de 2018;

III - Decreto N.º 7.845, de 14 de novembro de 2012; Decreto N.º 7.724, de 16 de maio de 2012; Decreto N.º 8.789, de 29 de junho de 2016; Decreto N.º 9.637, de 26 de dezembro de 2018;

IV - Decreto-Lei N.º 5.452, de 1.º de maio de 1943;

V - Instrução Normativa N.º 01 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008;

VI - Norma ABNT ISO/IEC 27002:2005, de 31 agosto de 2005; Norma ABNT ISO/IEC 27001:2006, de 31 de março de 2006;

VII - Norma Complementar N.º 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008;
Norma Complementar N.º 03/IN01/DSIC/GSIPR, de 30 de junho de 2009;
Norma Complementar N.º 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009;
Norma Complementar N.º 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009;
Norma Complementar N.º 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009;
Norma Complementar N.º 07/IN01/DSIC/GSIPR, de 06 de maio de 2010;
Norma Complementar N.º 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010;
Norma Complementar N.º 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012;
Norma Complementar N.º 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012;
Norma Complementar N.º 18/IN01/DSIC/GSIPR, de 09 de abril de 2013.