COMPANHIA NACIONAL DE ABASTECIMENTO

RESOLUÇÃO CONSAD N.º 4, DE 31/01/2025

O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA NACIONAL DE ABASTECIMENTO – Consad, no uso das atribuições que lhe são conferidas pelo art. 62, inciso XV do Estatuto Social da Conab, após deliberação tomada em sua 1ª Reunião Ordinária, realizada em 30/01/2025,

R E S O L V E:

1. APROVAR a atualização da Política de Segurança da Informação e Cibernética - NOC 10.010, conforme documento SEI 38643537, anexo.

2. REVOGAR a Resolução Consad N.º 045, de 17/12/2019.

3. Esta Resolução entra em vigor a partir da sua publicação.

JORGE LISANDRO MAIA USSAN
Presidente

Documento assinado eletronicamente por **JORGE LISANDRO MAIA USSAN**, **Conselheiro (a) de Administração - Conab**, em 31/01/2025, às 13:47, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **40377822** e o código CRC **63F4BF9D**.

60.000/054

Criado por regina.reys, versão 3 por regina.reys em 31/01/2025 13:41:34.

Conab	QUADRO COMPARATIVO DO NORMATIVO	Data

Nome da Norma: **Política de Segurança da Informação e Cibernética 10.010**	Unidade: **CGSI**

TEXTO ATUAL	TEXTO PROPOSTO	JUSTIFICATIVA
Removido todo bloco de texto relativo à “IDENTIFICAÇÃO GERAL E SUBSCRIÇÃO” (ver página 1)	Criado novo bloco de texto nomeado: “GENERALIDADES” (ver página 1)	Adequação à NOC 60.304
Movido todo bloco de texto relativo à “CONCEITOS E DEFINIÇÕES” (ver páginas 3 a 5)	Recebido o bloco “CONCEITOS E DEFINIÇÕES” e colado como item I, subitem 2, após as GENERALIDADES (ver páginas 2 a 7)	Adequação à NOC 60.304
4 - Fontes normativas: a) Constituição Federal (CF) – 1988 – artigo 37, § 6º; b) Lei N.º 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências; c) Lei N.º 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País e dá outras providências; d) Lei N.º 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências; e) Lei N.º 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD); f) Decreto N.º 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento; g) Decreto N.º 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição; h) Decreto N.º 10.046 , de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados; i) Decreto N.º 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação,	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 26 de setembro de 2019; k) Instrução Normativa n.º 1, de 27 de maio de 2020; l) Instrução Normativa GSI/PR n.º 3, de 28 de maio de 2021; m) Instrução Normativa GSI/PR 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.	Retirada as citações da legislação por orientação da GEMOR, por meio da NOTA TÉCNICA GEMOR SEI N.º 69/2024, documento SEI nº 38264038.

dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional; j) Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; l) Instrução Normativa Nº 1, de 27 de Maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; m) Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal; n) Instrução Normativa GSI/PR Nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal; o) Norma Complementar N.º 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal; p) Norma Complementar N.º 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal; q) Norma Complementar N.º 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, que estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta; r) Norma Complementar N.º 18/IN01/DSIC/GSIPR, de 10 de abril de 2013, que estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF); s) Norma ABNT NBR ISO/IEC 27001:2013, que fornece os requisitos para o sistema de gestão de segurança da informação nas organizações; t) Norma ABNT ISO/IEC 27002:2020, que fornece os controles de segurança da informação.		

Inexistente conceito relativo ao item proposto no bloco de “CONCEITOS E DEFINIÇÕES”	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA – 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, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Administradores de Rede – são os Analistas de Tecnologia da Informação (TI) lotados na área de Administração de Rede da Matriz; (ver página 3)	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; (ver página 3)	- Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021. - O nome GEASI foi colocado por extenso, por orientação da GEMOR, por meio da NOTA TÉCNICA GEMOR SEI N.º 69/2024, documento SEI nº 38264038.
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;(ver página 3)	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;(ver página 3)	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Ativos de Tecnologia da Informação (TI) – itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas;	Removido.	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	ATIVO DE REDE – equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores; (ver página 3)	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
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;	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021

Conceito inexistente na Política a ser substituída.	AUTENTICAÇÃO DE MULTIFATORES (MFA) - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
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; (ver página 3)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
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;	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada; (ver página 4)	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;(ver página 4)	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Controle de Acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;(ver página 4)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
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;(ver página 4)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Disponibilidade – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou	DISPONIBILIDADE – propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021

determinado sistema, órgão ou entidade;(ver página 4)	pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;	
Conceito inexistente na Política a ser substituída.	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;(ver página 4)	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	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 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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e pela obrigação do Decreto nº 9.637/2018 que trata da Política Nacional de Segurança da Informação (PNSI) no Poder Executivo Federal.
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; (ver página 4)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
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; (ver página 4)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Gestor da Informação – pessoa responsável pela administração de informações produzidas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades; (ver página 4)	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;	Melhoria de texto com adição de texto para melhoria de alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 com vistas à Conab.
Incidentes de Segurança da Informação – qualquer evento adverso, confirmado ou sob suspeita; (ver página 4)	INCIDENTE CIBERNÉTICO – ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021

	de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;	
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; (ver página 4)	INFORMAÇÃO – dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Integridade – fidedignidade de informações, propriedade que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; (ver página 4)	INTEGRIDADE – propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Conceito inexistente na Política a ser substituída.	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Mídias removíveis – são tipos de dispositivos de memória que podem ser removidos do seu aparelho de leitura, conferindo portabilidade para os dados que carrega; (ver página 4)	MÍDIAS REMOVÍVEIS – são tipos de dispositivos de memória de armazenamento de dados que são portáveis para devido o transporte físico destes;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
Normas Complementares – conjunto de normas que define e regula o uso dos recursos de tecnologia da informação e das informações; (ver página 5)	NORMAS COMPLEMENTARES – conjunto de normas que define e regula o uso dos recursos de tecnologia da informação e das informações no âmbito da Conab;	Melhoria de texto.
Protocolo de Rede – são procedimentos que controlam e regulam a comunicação, conexão e transferência de dados entre sistemas computacionais; (ver página 5)	Remover item.	Não utilização deste conceito na Política.
Sala-cofre – ambiente de TI certificado conforme as normas ABNT NBR 15.247, protegido de desastres; (ver página 5)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.
Sala-segura – ambiente com acesso controlado onde são armazenados os ativos de TI, normalmente situados nas Superintendências Regionais e Unidades Armazenadoras; (ver página 5)	SALA-SEGURA – ambiente com acesso controlado onde são armazenados os ativos de Tecnologia da Informação, normalmente situados nas Superintendências Regionais e Unidades Armazenadoras;	Melhoria de texto.
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; (ver página 5)	SEGURANÇA DA INFORMAÇÃO – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.

Servidor de arquivos – servidor onde são armazenados os arquivos produzidos pelos empregados, independente de sua tecnologia de armazenamento; (ver página 5)	SERVIÇO DE ARMAZENAMENTO DE ARQUIVOS – serviço, disponível por meio da rede computacional da Conab, no qual são armazenados os arquivos digitais produzidos pela Companhia;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.
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; (ver página 5)	Remover item.	Não utilização deste conceito na Política.
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; (ver página 6)	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.
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.	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;	Melhoria de texto.
Conceito inexistente na Política a ser substituída.	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;	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.
Conceito inexistente na Política a ser substituída.	ZERO TRUST– vide confiança zero.	Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e melhorias.
Capítulos I e II suprimidos coma Capítulo I. Incluindo seus artigos. (ver página 3)	CAPÍTULO I – ESCOPO E ABRANGÊNCIA	Alinhamento à IN 01/2020 PR/GSI
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). (ver página 3)	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. (ver página 7)	Melhoria do texto e Alinhamento à IN 01/2020 PR/GSI.
CAPÍTULO II ABRANGÊNCIA	CAPÍTULO I – ESCOPO E ABRANGÊNCIA Art. 2º Esta política se aplica aos agentes públicos que	Melhoria do texto e Alinhamento à IN 01/2020 PR/GSI

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. (ver página 3)	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). (ver página 8)	
Inexistia este capítulo com este tema.	Criado novo capítulo II: “Princípios”	Alinhamento à IN 01/2020 PR/GSI
Criado novos itens para o novo Capítulo II e anexado o artigo 3º para o mesmo.	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.	Alinhamento à IN 01/2020 PR/GSI
CAPÍTULO III CONCEITOS E DEFINIÇÕES (ver páginas 3 a 5)	Renomeado para CAPÍTULO III – DIRETRIZES GERAIS	CONCEITOS E DEFINIÇÕES já consta no prâmbulo da Política, nas páginas 2 a 6, além de alinhamento à IN 01/2020 PR/GSI
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º São diretrizes gerais da Política de Segurança da Informação:	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º São diretrizes gerais desta Posic:	Alinhamento à IN 01/2020 PR/GSI por meio da adição do termo Cibernética, a fim de especificar melhor.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º I - todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos, visando preservar a continuidade do negócio;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º II - o gerenciamento dos ativos de informação deverá observar as normas complementares e procedimentos específicos, a fim de garantir sua operação segura e contínua;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º III - a periodicidade e critérios serão definidos pela CGSI visando o cumprimento dessa Política, bem como das normas	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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	Melhoria de texto.

complementares e procedimentos de segurança da informação;	informação;	
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º V - as medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com o valor do ativo protegido;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º VI - o Plano de Continuidade de Negócios da Conab deverá abarcar os assuntos relativos à Segurança da Informação;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º VI - contemplar a continuidade da segurança da informação no “Plano de Continuidade do Negócio” da Conab;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º VII - dar ciência desta Posic para todos os empregados da Companhia que possuam acesso a sistemas da Conab, além da Norma de Recursos Computacionais;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º 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 (anexo I), devendo também ser assinado, para ciência, pelo gestor responsável pela atividade do referido agente;	Melhoria de texto e de referência ao termo.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º IX - os dirigentes, empregados e colaboradores da Companhia, possuem a responsabilidade pela segurança, integridade e	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º IX - o acesso aos ativos de informação devem ser restritos e controlados, segmentados por papel funcional na Companhia;	Removido todo o conteúdo original deste item, pois o ITEM VII já fala do mesmo tema. No lugar, foi colocada a diretriz de acesso mínimo que consta no item XIII anterior, mas melhorado.

qualidade da informação, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da Conab;		
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º X - todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º X - cabe ao Comitê Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação desta Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos;	Alinhamento à IN 01/2020 PR/GSI
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º XI - os usuários de sistemas informatizados devem manter as informações, produzidas em meio digital, armazenadas em serviço de armazenamento de arquivos fornecido pela Companhia;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º XII - No evento de encerramento de funções, contratos ou acordos de agentes públicos, seus direitos de acesso às informações e aos recursos de processamento da informação devem ser revogados ou ajustados de acordo com a mudança de função, excetuando-se os ativos que, por questões de segurança, não estejam vinculados ao referido sistema;	Melhoria de texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO III – DIRETRIZES GERAIS Art. 4º XIII - a autoridade máxima da Conab é responsável por garantir os recursos necessários para a execução desta Posic no âmbito desta empresa pública;	O conteúdo original do item XIII foi removido, pois já constava no novo item IV. Foi adicionado neste novo item XIII item que inexiste na política a ser substituída, visando alinhamento à IN 01/2020 PR/GSI.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º XIV - a Conab deve nomear Gestor de Segurança da Informação, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em	O item XIV do artigo 4º, original, foi removido por motivo de já existir referência e normativo específico para classificação da informação constante no Artigo 6º, item IV. Novo item XIV em alinhamento ao

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;	ativos de informação;	Instrução Normativa GSI nº 01, de 27 de maio de 2020.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º XV - a Conab deve nomear o Comitê Gestor de Segurança da Informação, responsável pelo estabelecimento dos controles para avaliaçã o 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;	O item XV do artigo 4º, original, foi removido por motivo de já existir referência e normativo específico para classificação da informação constante no Artigo 6º, item IV. Novo item XV em alinhamento ao DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º XVI -a classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte;	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º XVI - deve haver 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.	O item XVI do artigo 4º, original, foi removido por motivo de já existir referência e normativo específico para classificação da informação constante no Artigo 6º, item IV. Novo item XVI em alinhamento ao INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021, artigo 9º.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º XVII - a Companhia deve promover o cumprimento e operacionalização da classificação da informação conforme seu normativo específico;	O item XVII do artigo 4º, original, foi removido por motivo de já existir referência e normativo específico para classificação da informação constante no Artigo 6º, item IV. Novo item XVII foi adicionado enfatizando sobre a promoção ao cumprimento da norma específica.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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;	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º XIX - o acesso à rede computacional e aos sistemas de informação da Conab deve possuir meios de acesso que visem garantir a autenticidade e confidencialidade do referido acesso;	Melhoria do texto.
CAPÍTULO IV DIRETRIZES E ORIENTAÇÕES GERAIS Art. 4º 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 Informação Art. 6º XX - deve existir mecanismo para o registro e tratamento de incidentes cibernéticos que possam comprometer a segurança operacional da Companhia.	Melhoria do texto.

Inexistente capítulo sobre “Instituição de Etir” na Política a ser substituída.	CAPÍTULO IV – INSTITUIÇÃO DE 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, sem prejuízo das demais metodologias e padrões conhecidos.	Decreto nº 9.637, de 26 de dezembro de 2018, prevê que compete aos órgãos da administração pública federal a instituição e implementação de uma ETIR, nos termos do inciso VII do art. 15. Além disso, a Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, com alterações da Instrução Normativa GSI/PR nº 02, de 24 de julho de 2020.
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.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação 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;	Melhoria de texto e organização do capítulo por subitens do mesmo assunto.
CAPÍTULO V DIRETRIZES ESPECÍFICAS Seção I Gestão de Ativos de TI e Informações 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.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º II - os ativos de informação e associados com os recursos de processamento da informação devem ter um proprietário designado pela Companhia;	Organização em subitem e melhoria de texto.
CAPÍTULO V DIRETRIZES ESPECÍFICAS Seção I Gestão de Ativos de TI e Informações 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.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º III - a regulamentação no estabelecimento de critérios e procedimento para o uso dos recursos computacionais deve seguir a Norma de Recursos Computacionais da Conab;	Organização em subitem e melhoria de texto.

CAPÍTULO V DIRETRIZES ESPECÍFICAS Seção I Gestão de Ativos de TI e Informações 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.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º 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;	Organização em subitem e melhoria/simplificação do texto.
Inexistente subitem/assunto na Política a ser substituída.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º 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;	Organização em subitem e inclusão de normativo específico sobre o tema em questão.
Inexistente subitem/assunto na Política a ser substituída.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º 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;	Organização em subitem e inclusão de normativo específico sobre o tema em questão.
Inexistente subitem/assunto na Política a ser substituída.	CAPÍTULO V – DIRETRIZES ESPECÍFICAS Seção I – Gestão de Ativos de Informação Art. 6º 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)”.	Organização em subitem e inclusão de normativo específico sobre o tema em questão.
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	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	Transformação de artigos em subitens, com melhoria de divisão por tipo de assunto, melhorias de texto, retirada da exigência de certificação em sala-cofre (seguindo determinação do TCU) e adição de diretriz sobre sala-segura.

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.	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. 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 9441; 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;	
Seção II Segurança Física e do Ambiente de TI 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.	Seção II – Segurança Física do Ambiente de TI Art. 7º 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	Divição do assunto em 3 subtitens provendo melhor detalhamento das diretrizes deste mesmo assunto.

	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;	
Seção II Segurança Física e do Ambiente de TI 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.	Artigo/texto removido.	Tema estabelecido na Seção III da nova Política proposta.
Seção II Segurança Física e do Ambiente de TI Art. 14. Manutenção dos Equipamentos – os equipamentos devem receber manutenção, conforme indicação do fabricante, para assegurar sua disponibilidade e integridade permanente.	Removido artigo.	Inconclusivo, por se tratar de tema com peculiaridade de cada fabricante, de forma a gerar incertezas práticas sobre o que estaríamos assumindo.
Seção II Segurança Física e do Ambiente de TI Art. 14. Manutenção dos Equipamentos – os equipamentos devem receber manutenção, conforme indicação do fabricante, para assegurar sua disponibilidade e integridade permanente.	Removido artigo.	Inconclusivo, por se tratar de tema com peculiaridade de cada fabricante, de forma a gerar incertezas práticas sobre o que estaríamos assumindo.
Seção II Segurança Física e do Ambiente de TI 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.	Seção II – Segurança Física do Ambiente de TI Art. 7º 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;	Melhoria de texto e readequação de posição em subitem do artigo 7º.
Seção II Segurança Física e do Ambiente de TI 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.	Seção II – Segurança Física do Ambiente de TI Art. 7º 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;	Melhoria de texto e readequação de posição em subitem do artigo 7º.

Seção II Segurança Física e do Ambiente de TI 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 II – Segurança Física do Ambiente de TI Art. 7º 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.	Readequação em subitens e melhoria de texto.
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.	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;	Melhoria de texto e organização de posição como subitem do artigo 8º.
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético 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;	Melhoria de texto e organização de posição como subitem do artigo 9º.
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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;	Melhoria de texto e organização de posição como subitem do artigo 9º.
Seção III Gerenciamento das Operações e Comunicações Art. 21. Gerenciamento de Serviços Terceirizados – implementar e manter o nível apropriado de segurança da informação dos	Artigo removido.	Já consta no artigo 4º, subitem VIII da nova Política proposta.

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.		
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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);	Melhoria de texto e organização de posição como subitens do artigo 9º e inclusão da diretriz para DLP.
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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)”;	Simplificação do texto e direcionando maiores detalhes para norma específica sobre o tema.
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 8º Controles Operacionais: 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.	Simplificação e otimização de texto.

Seção III Gerenciamento das Operações e Comunicações 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.	Artigo removido.	Tema já consta em normativo específico e está apontado no artigo 6º da nova Política proposta.
Seção III Gerenciamento das Operações e Comunicações 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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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;	Remoção do artigo 26 por motivo de já estar contemplado, de forma mais ampla, no subitem VI do artigo 9°.
Inexistente subitem/assunto na Política a ser substituída.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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;	Diretriz relacionada ao relativo novo conceito de Zero Trust.
Inexistente subitem/assunto na Política a ser substituída.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica:	Diretriz relacionada ao conceito de autenticação de serviços web por meio do GOV.BR.

	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;	
Inexistente subitem/assunto na Política a ser substituída.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: IX -o serviço de VPN deve possuir autenticação combinada com recurso de MFA (Multi Fator de Autenticação), devendo o acesso de cada usuário possuir acesso apenas ao estritamente necessário ao seu trabalho;	Diretriz relacionada ao conceito de MFA em conexões VPN, a fim de aumentar a segurança.
Seção III Gerenciamento das Operações e Comunicações 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	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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;	Simplificação dos artigos 27, 28 e 29, organização por meio de subitem do artigo 9º.

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.		
Seção III Gerenciamento das Operações e Comunicações 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 III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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;	Melhoria de texto e organização de posição como subitens do artigo 9º.
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.	Seção III – Segurança Lógica e Operacional – Ambiente Cibernético Art. 9º Controles de Segurança Lógica: 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.	Simplificação de texto e organização de posição como subitens do artigo 9º. Também, item relacionado ao conceito de Zero Trust contigo no subitem VII do artigo 9º.
Seção IV Controle de Acessos 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; Equipamento de Usuário sem Monitoramento – os usuários devem assegurar que os equipamentos não monitorados tenham	Removido artigo.	Item já é controlado por meio da NOC 60.213 (Norma de Recursos Computacionais). Esta Política já faz esta referência (à NOC) no Artigo 6º, subitem III, da nova Política proposta.

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.		
Seção IV Controle de Acessos 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.	Removido artigo.	Item já é controlado por meio da NOC 60.213 (Norma de Recursos Computacionais). Esta Política já faz esta referência (à NOC) no Artigo 6º, subitem III, da nova Política proposta. Item está também abarcado por meio do artigo 9º da nova Política proposta.
CAPÍTULO VI RESPONSABILIDADES	CAPÍTULO III – RESPONSABILIDADES Art. 10º São responsabilidades da Diretoria Executiva da Conab:	Melhoria do texto com a inclusão “dos meios necessários”, a fim de promover a viabilização prática da Política proposta.

Art. 34. São responsabilidades da Diretoria Executiva da Conab: I- cumprir e fazer cumprir esta Política de Segurança da Informação;	I-fornecer os meios necessários e fazer cumprir esta Posic em toda a Companhia;	
CAPÍTULO VI RESPONSABILIDADES Art. 34. São responsabilidades da Diretoria Executiva da Conab: II - designar o Gestor de Segurança da Informação interno, sendo obrigatoriamente Superintendente (ou equivalente) ou Diretor;	CAPÍTULO III – RESPONSABILIDADES Art. 10º São responsabilidades da Diretoria Executiva da Conab: II - nomear o Gestor de Segurança da Informação, conforme inciso XV do artigo 4º desta Política, devendo este possuir, obrigatoriamente, o cargo deSuperintendente (ou equivalente) ou Diretor;	Melhoria do texto.
CAPÍTULO VI RESPONSABILIDADES Art. 34. São responsabilidades da Diretoria Executiva da Conab: II - designar o Gestor de Segurança da Informação interno, sendo obrigatoriamente Superintendente (ou equivalente) ou Diretor;	CAPÍTULO III – RESPONSABILIDADES Art. 10º São responsabilidades da Diretoria Executiva da Conab: II - nomear o Gestor de Segurança da Informação, conforme inciso XIV do artigo 4º desta Política, devendo este possuir, obrigatoriamente, o cargo deSuperintendente (ou equivalente) ou Diretor;	Melhoria do texto e adição de referência.
CAPÍTULO VI RESPONSABILIDADES Art. 34. São responsabilidades da Diretoria Executiva da Conab: 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.	CAPÍTULO III – RESPONSABILIDADES Art. 10º São responsabilidades da Diretoria Executiva da Conab: III -priorizar os recursos necessários para a implementação e gestão da 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.	Readequação de posição (antes artigo 34 e agora artigo 10º) na nova Política proposta.
(item inexistente referente à ETIR, no capítulo sobre responsabilidades).	CAPÍTULO III – RESPONSABILIDADES Art. 10º São responsabilidades da Diretoria Executiva da Conab: VI -instituir e nomear a ETIR da Conab, conforme Capítulo IV desta Política, além de apoiar no fornecimento de recursos de pessoal e financeiros,	Adição da responsabilidade sobre instituilção de uma ETIR da Conab. Alinhamento à PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 e pela obrigação do Decreto nº 9.637/2018 que trata da Política Nacional de Segurança da Informação (PNSI) no Poder Executivo Federal.

CAPÍTULO VI RESPONSABILIDADES 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;	CAPÍTULO III – RESPONSABILIDADES Art. 11º 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;	Readequação de texto para alinhamento à IN 01/2020 PR/GSI
CAPÍTULO VI RESPONSABILIDADES Art 35. São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI): 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.	CAPÍTULO III – RESPONSABILIDADES Art. 11º São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI): 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;	Subtitens foram mantidos, mas renumerados no artigo 11 da nova Política proposta.
CAPÍTULO VI	CAPÍTULO III – RESPONSABILIDADES	Adição de subitens visando alinhamento à

RESPONSABILIDADES Art 35. São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI): subitens inexistentes na Política a ser substituída.	Art. 11º São responsabilidades do Comitê Gestor de Segurança da Informação (CGSI): 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.	IN 01/2020 PR/GSI
CAPÍTULO VI RESPONSABILIDADES 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 VI RESPONSABILIDADES Art. 12º 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.	Item foi renumerado e simplicado num único parágrafo.
CAPÍTULO VI RESPONSABILIDADES Artigo inexistente na Política a ser substituída.	CAPÍTULO VI RESPONSABILIDADES Art. 13º 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;	Não havia definições sobre as responsabilidades do Gestor de Segurança da Informação na Política a ser substituída. Foi, portanto, adicionado capítulo visando alinhamento à IN 01/2020 PR/GSI

	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.	
CAPÍTULO VI RESPONSABILIDADES Artigo inexistente na Política a ser substituída.	Art. 14º 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 do órgão ou da entidade; 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.	Não havia definições sobre as responsabilidades da ETIR na Política a ser substituída. Foi, portanto, adicionado capítulo visando alinhamento à IN 01/2020 PR/GSI
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	CAPÍTULO IV – SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO Art. 15º 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	Readequação da numeração na nova Política proposta e melhoria de texto.

correta conduta na utilização das informações da Conab.	conduta na utilização das informações da Conab, realizando capacitação quando necessário.	
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 V – DO CUMPRIMENTO DESTA POLÍTICA Art. 16º 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.	Simplificação com a alteração da nomenclatura (de descumprimento para cumprimento) a fim de enfatizar o dever de cumprimento desta política, mas sem perder a essência sobre apurações de responsabilidade possíveis e adicionando o direito da ampla defesa.
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.	CAPÍTULO VI – COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI) Art. 17º 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.	Readequada a numeração e posicionamento na nova Política proposta.
CAPÍTULO IX COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI) § 1º - Os suplentes de cada membro serão os próprios	CAPÍTULO VI – COMPOSIÇÃO DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO (CGSI) Art. 18º Do funcionamento do CGSI: I-os suplentes institucionais de cada membro serão os próprios	Readequada a numeração e posicionamento na nova Política proposta com transformação de parágrados no artigo 18 com seus subitens.

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.	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 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 VII – DA REVISÃO DESTA POLÍTICA Art. 19º 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.	Readequação da numeração na nova Política proposta e melhoria de texto.
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 VIII – DA PUBLICIDADE E DIVULGAÇÃO Art. 20º Essa Política deve estar pública e disponível nos canais de comunicação internos e externos da Companhia.	Readequação da numeração na nova Política proposta e melhoria de texto.
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 VIII – DISPOSIÇÕES GERAIS Art. 21º O tratamento de dados pessoais que derivar do cumprimento desta Política, deverá acontecer em conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei N.º 13.709 de 14/08/2018. (Texto incluído pela Resolução Consad N.º 014, de 23/07/2021). Art. 22º 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.	
CAPÍTULO XIII REFERÊNCIAS LEGAIS Art. 47. Referências Legais e Normativas:	Capítulo removido.	Capítulo já existente na nova Política proposta, na área de generalidades, página 1, conforme a NOC 60.304 determina.

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.		