NORMA DE RECURSOS COMPUTACIONAIS 60.213

Sistema de Administração
Subsistema de Administração de Recursos Materiais

SUTIN/GEASI

SUMÁRIO

CAPÍTULO I

GENERALIDADES

1 - Área Gestora desta Norma: Gerência de Administração de Rede e Segurança da Informação (Geasi).

1.1 -Áreas Corresponsáveis: Não se aplica.

2 - Publicidade da Norma: Público.

3 - Finalidade: Regulamentar e estabelecer critérios e procedimentos para o uso dos recursos computacionais no âmbito da Companhia Nacional de Abastecimento (Conab).

4 - Objetivos: Quanto à utilização dos recursos computacionais no âmbito da Conab, são eles:

a) definir as diretrizes necessárias no que tange aos seus critérios de utilização;

b) definir papéis de responsabilidade dos usuários em geral;

c) alinhar conforme a Política de Segurança da Informação (NOC 10.010).

5 - Aplicação: Todas as áreas da Conab que utilizem recursos computacionais.

6 - Competência: Estabelecer regras de utilização dos recursos computacionais da Conab para o público interno e externo.

7 - Alterações da Norma: Revisão Geral

8 - Documento que aprova a Norma: Resolução Direx n.º 024, de 23/11/2020.

9 - Vigência da Norma: Publicada em 25/11/2020.

10 - Fontes normativas:

a) Lei n.º 12.527 de 18/11/2011 (Lei de Acesso à Informação);

b) Lei n.º 12.965 de 23/4/2014 (Marco Civil da Internet);

c) Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);

d) Código Penal, art. 313-A (Inserção de dados falsos em sistemas de informações) e art. 313-B (Modificação ou alteração não autorizada de sistemas de informações);

e) Código de Ética e Integridade da Conab – NOC 10.112;

f) NBR ISO/IEC 27001:2013;

g) Política de Segurança da Informação – NOC 10.010.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

I - Conceitos e Definições

1 - Acesso remoto – é dado através de ferramentas específicas de tecnologia que proveem o acesso de usuários em um computador remoto através da Internet, controlando-o diretamente, independentemente da distância física que separa ambos.

2 - Antivírus – programa ou *software* especificamente desenvolvido para detectar, anular e eliminar vírus de computador.

3 - Armazenamento em nuvem – estratégia de armazenamento de arquivo onde não há necessidade de estar na rede local para acesso aos dados.

4 - *Backbone* – espinha dorsal de uma rede, geralmente uma infraestrutura de alta velocidade que interliga várias redes.

5 - *Backup* – cópia de segurança – em informática refere-se à cópia de dados de um dispositivo para outro com o objetivo de posteriormente os recuperar, caso haja algum problema.

6 - CGSI – Comitê Gestor de Segurança da Informação.

7 - Criptografia – considerada a ciência e a arte de escrever mensagens em forma cifrada ou em código, sendo um dos principais mecanismos de segurança utilizados para proteção contra os riscos associados ao uso de redes compartilhadas.

8 - Criptografado – informação/dado codificado ou cifrado.

9 - Correio Eletrônico (E-*mail*) – sistema que permite compor, enviar e receber mensagens por meio de sistemas eletrônicos de comunicação.

10 - DNS (*Domain Name System)* – consiste num serviço, onde são armazenadas ligações entre endereços IPs e domínios.

11 - e-GOV – sigla que representa o Programa de Governo Eletrônico brasileiro que visa orientar as relações do Governo com os cidadãos, empresas e também entre os órgãos do próprio governo, de forma a aprimorar a qualidade dos serviços prestados, promover a interação com empresas e indústrias e fortalecer a participação cidadã por meio do acesso à informação e a uma administração mais eficiente.

12 - Exfiltração – transferência não autorizada de dados de um sistema de informação.

13 - *Firewall* – dispositivo de rede que regula o tráfego de rede entre redes distintas.

14 - Forense computacional – conjunto de técnicas utilizadas para identificar e coletar evidências digitais. Estas são essenciais para o caso de um Processo Interno de Apuração.

15 - *Hardware* – parte física dos equipamentos de Informática.

Continuação Capítulo II

16 - Interlocutor de Tecnologia da Informação – é o analista, técnico ou assistente de TI alocado nas Superintendências Regionais com a função de dar suporte às atividades e recursos de Tecnologia da Informação.

17 - Internet – rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum, unindo usuários particulares, entidades de pesquisa, órgãos culturais, institutos militares, bibliotecas e empresas de toda envergadura inicial por vezes maiúsc.

18 - Telefonia *IP* – é a utilização de conversação humana usando a Internet ou qualquer outra rede de computadores, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.

19 - IP – Um Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

20 - *LAN* – significa Local Area Network (em português, Rede Local) e é um conjunto de computadores que pertence a uma mesma organização, conectados entre eles por uma rede, numa pequena área geográfica, geralmente através de uma mesma tecnologia (a mais usada é a Ethernet).

21 - LOG – em computação, log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.

22 - *Malware* – termo em inglês que designa toda forma de software construído com intenção maliciosa, com o objetivo de causar dano, alteração, uso pernicioso do equipamento ou roubo de informação.

23 - *Modem* – a palavra Modem vem da junção das palavras: modulador e demodulador. É um dispositivo eletrônico que modula um sinal digital em uma onda analógica, pronta a ser transmitida pela linha telefônica e que demodula o sinal analógico e o reconverte para o formato digital original. Utilizado para conexão à Internet, BBS ou a outro computador.

24 - Notebook (ou Laptop) – computador portátil móvel.

25 - *NTP* – é um protocolo para sincronização dos relógios dos computadores, ou seja, ele define um jeito para um grupo de computadores conversar entre si e acertar seus relógios, baseados em alguma fonte confiável de tempo, como, por exemplo, os relógios atômicos do Observatório Nacional, que definem a Hora Legal Brasileira.

26 - *Patches* – pacotes de correção/atualização dos produtos disponíveis em diversos sistemas operacionais.

27 - Pendrive – é um dispositivo móvel de memória constituído por dispositivo que armazena dados digitais como documentos, fotos, entre outros.

28 - Portal Conab – sítio web da Conab, onde se encontram os sistemas corporativos.

29 - Pragas digitais – são programas de computador com intuito malicioso, com finalidades de danos, roubo de informações, entre outros.

Continuação Capítulo II

30 - *Proxy* (plural: *proxies*) – serviço que intermedeia o acesso entre um cliente e um servidor.

31 - Recursos computacionais – são os equipamentos de tecnologia da informação, softwares próprios ou de terceiros, arquivos digitais e banco de dados que são direta ou indiretamente administrados, mantidos ou operados pela Superintendência de Tecnologia da Informação (Sutin), por meio das suas gerências subordinadas ou pelos interlocutores de TI das Superintendências Regionais, tais como: computadores pessoais, servidores de rede e terminais de qualquer espécie, incluídos seus equipamentos acessórios, impressoras, redes de computadores e equipamentos de transmissão de dados, bancos de dados ou documentos residentes em disco, fita ou outros meios digitais, *scanners* (equipamentos digitalizadores), sistemas ou softwares desenvolvidos internamente ou por terceiros, entre outros, que possuam similaridade e reconhecimento cabal com a área de TI.

32 - Rede de Dados – possui a função de interligar computadores e/ou conectá-los a outros dispositivos, permitindo que haja a circulação de informações, comandos e recursos entre eles.

33 - Roteadores – são equipamentos usados para fazer a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes um do outro.

34 - *Scanners* – é um equipamento capaz de digitalizar imagens físicas, normalmente documentos ou fotos, em arquivos digitais usáveis por equipamentos informatizados.

35 - Servidor – computador que fornece serviços a uma rede de computadores.

36 - Sigede – Sistema de Gestão de Demandas da Conab.

37 - Site – um site ou sítio eletrônico, é um conjunto de páginas web, isto é, de hipertextos acessíveis geralmente pelo protocolo HTTP ou pelo HTTPS na internet via navegadores de internet.

38 - *SNMP* – Simple Network Management Protocol – é um protocolo de gestão de rede da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede.

39 - *Software* – programa de computador que possui instruções a serem seguidas e/ou executadas para auxiliar em sua instalação.

40 - Spam – mensagem eletrônica não-solicitada enviada em massa.

41 - *Switch* – (plural: switches) é um equipamento que interliga computadores, possibilitando a formação de uma rede local a partir de cabos de rede que se estendem da placa de rede dos computadores até o próprio equipamento.

42 - Usuário – pessoa que utiliza o produto, bem ou serviço.

43 - Vírus – no contexto desta norma, é um programa ou trecho de código projetado para danificar seu computador através da corrupção de arquivos do sistema, utilização de recursos e/ou destruição de dados.

44 - VPN – rede privada virtual, permite realizar um acesso seguro a uma rede remota a partir de uma rede de terceiros.

45 - WAN – uma rede de longa distância ou rede de área alargada é uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente.

Continuação Capítulo II

46 - Web ou www – sistema hipertextual que opera através da internet.

47 - Wiki – termo utilizado para identificar um tipo específico de coleção de documentos em hipertexto ou software colaborativo usado para criá-lo.

48 - *Wireless* – caracteriza qualquer tipo de conexão para transmissão de dados sem a utilização de fios ou cabos.

49 - Worms – é um programa de autorreplicação em redes de computadores, similar a vírus computacional.

CAPÍTULO III

DA UTILIZAÇÃO GERAL DOS RECURSOS COMPUTACIONAIS

I - Regras Normativas Gerais

1 - A utilização dos recursos computacionais e/ou serviços de tecnologia da informação da Conab é norteada por esta Norma.

2 - As regras relacionadas à segurança da informação, dos recursos computacionais e/ou serviços de tecnologia da informação da Conab, estão normatizados na NOC 10.010 (Política de Segurança da Informação) devendo, portanto, esta ser observada prioritariamente.

3 - Todo e qualquer uso dos recursos computacionais deve estar de acordo com obrigações contratuais quando houver, assim como leis e regulamentações vigentes, inclusive perante as delimitações definidas nos contratos de *software* e outras licenças.

4 - Deverá existir, ser mantido e operacional, serviço de registros para auditoria (*log*) para os serviços essenciais e/ou críticos, com guarda dos dados de acordo com a Lei n.º 12.965, de 23/04/2014.

5 - As instruções de funcionamento, bem como as limitações de um serviço devem ser fornecidas aos seus usuários.

6 - Serviços cuja informação é classificada como privativa e/ou confidencial devem fornecer métodos seguros de autenticação e autorização daquela informação.

7 - Deverá ser disponibilizado telefone de contato, acesso a sistema específico para chamado e/ou endereço de e-mail com finalidade de fornecimento de suporte aos usuários dos serviços de TI.

8 - Todo serviço deverá ter um administrador ou contato a ser acionado por meio do Sistema de Gestão de Demandas (Sigede) para os casos de incidentes de segurança ou de outros motivos relacionados ao serviço.

9 - Todo usuário interno da Companhia, que utiliza recurso computacional, deve possuir uma conta de autenticação a ser utilizada nos serviços.

10 - A área de tecnologia da informação deve manter um catálogo de softwares homologados pela Companhia atualizado e de fácil acesso aos usuários.

II - Regras Gerais aos Usuários

1 - O usuário utilizador de recursos computacionais deve conhecer as instruções, regras e penalidades de funcionamento do serviço que esteja utilizando, devendo ainda:

a) não se passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais, exceto em casos em que o acesso anônimo é explicitamente permitido;

b) responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros;

c) se titular da conta, responder pelo mau uso dos recursos computacionais em qualquer circunstância;

d) responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos e também, se for o caso, às penalidades impostas por outras instâncias (leis municipais, estaduais, distritais e federais);

e) o usuário deve manter seus computadores pessoais com *software*s homologados pela Companhia, inclusive com *patches* e erratas, e antivírus atualizados, conforme orientação da Sutin ou do interlocutor de TI na Superintendência Regional, não podendo o usuário impedir tais correções de segurança;

f) se necessário, os usuários devem procurar a Sutin ou o interlocutor de TI na Superintendência Regional para esclarecimentos.

III - Regra Geral referente à Sutin, que deverá ser observada por suas gerências subordinadas e pelos interlocutores de TI das Superintendências Regionais

1 - É dever dos analistas e técnicos de TI:

a) preservar a integridade e a segurança dos sistemas;

b) manter os registros (logs) de utilização dos serviços entregues, conforme tempo regulamentado em normas da administração pública, em servidor remoto diferente daquele que provê o serviço a ser registrado;

c) fornecer registros de sistema e utilização sempre que solicitado formalmente ou conforme regulamento interno, quando houver;

d) acessar dados dos usuários somente quando for indispensável para manutenção do sistema ou em casos de falhas de segurança, sempre observando os regulamentos vigentes sobre privacidade na administração pública;

e) utilizar o sincronismo de tempo (*ntp) nos* servidores responsáveis por fornecimento de serviço de tecnologia da informação;

f) manter atualizados os sistemas e serviços de tecnologia da informação;

g) manter atualizada tecnologicamente a infraestrutura de tecnologia da informação;

h) informar aos usuários sobre os mecanismos recomendáveis de correção de vulnerabilidades, quando cabível;

i) utilizar sempre das melhores práticas de segurança da informação, especialmente as definidas para a administração pública nos sistemas e serviços de tecnologia da informação entregues à Companhia;

j) garantir a disponibilidade na entrega de serviços aos usuários da Conab e ao público geral, conforme acordo de níveis de serviço definidos pelos gestores de negócio da Companhia;

k) garantir que o armazenamento dos registros de eventos (logs) gerados pelos recursos de tecnologia da informação sejam centralizados sempre que houver viabilidade técnica. Nos casos em que existir limitação técnica o armazenamento dos registros de eventos (logs) deve ser mantido nos sistemas de origem;

l) garantir que os registros de eventos (logs) estejam sempre sincronizados cronologicamente;

m) garantir que os registros de eventos (logs) sejam protegidos e armazenados adequadamente, de acordo com a sua classificação;

n) Garantir a Proteção das Informações dos Registros (logs), de forma que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado;

o) Garantir que os Registros (log) de Administrador e Operador, no qual constam as atividades dos administradores e operadores em sistemas, sejam devidamente registrados;

p) Garantir que os Registros (logs) de Falhas, na qual as falhas ocorridas sejam registradas e analisadas para correção dos problemas encontrados.

IV - Norma Geral de Acesso a Serviços Externos

1 - Define-se como serviços externos aqueles recursos de tecnologia da informação incluindo sítios, aplicações, ferramentas, sistemas, dados, compartilhamentos, fluxos de mídia, mapas, redes sociais, protocolos de comunicação, telefonia, serviços de mensagens, correio eletrônico, nuvem, dentre outros, desde que não sejam fornecidos pela Conab.

2 - Compete à Sutin, bloquear acessos externos que sejam classificados como risco à disponibilidade dos serviços providos pela Companhia, assim como serviços que representem riscos à segurança da tecnologia da informação e que sejam classificados como vetores disseminação de vírus, *malware e* pragas digitais.

3 - Compete ao Comitê Gestor de Segurança da Informação (CGSI) definir o bloqueio de serviços que sejam classificados como risco a segurança da informação, como, por exemplo, serviços que permitam a exfiltração de dados classificados como sigilosos ou confidenciais.

V - Violação das Regras

1 - Consideram-se violação das regras:

a) mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;

b) efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da Conab;

c) utilizar os recursos computacionais da Conab para acesso não autorizado a recursos de terceiros;

d) violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança, interferindo em fechaduras automáticas ou sistemas de alarme;

e) interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto quando autorizado explicitamente pelo superior hierárquico, com prévio conhecimento da área de informática;

f) provocar interferência em serviços de outros usuários ou o bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da Conab;

g) desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e *worms*, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;

h) utilizar os recursos computacionais da Conab para atividades direta ou indiretamente relacionadas à fabricação ou testes de armas nucleares, químicas e biológicas;

i) utilizar os recursos computacionais da Conab para fins comerciais ou políticos, tais como mala direta ou propaganda política;

j) utilizar os recursos computacionais da Conab para ganho indevido;

k) utilizar os recursos computacionais da Conab para intimidar, assediar, difamar ou aborrecer qualquer pessoa;

l) consumir inutilmente os recursos computacionais da Conab de forma intencional.

VI - Distribuição de Informação Imprópria

1 - O usuário ou administrador não pode transmitir, difundir ou disponibilizar a terceiros, informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos e som e/ou imagem, fotografias, gravações, *software* ou qualquer classe de material que de qualquer forma:

a) contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades públicas reconhecidas constitucionalmente, nos tratados internacionais e no ordenamento jurídico como um todo;

b) induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

c) induzam, incitem ou promovam atos, atitudes ou ideias discriminatórias por causa de sexo, raça, religião, crenças, idade ou condição;

d) incorporem, ponham à disposição ou permitam acessar produtos, elementos, mensagens e/ou serviços ilegais, violentos, pornográficos, degradantes ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

e) sejam contrários ao direito de honra, à intimidade pessoal e familiar ou à própria imagem das pessoas;

f) infrinjam as normas sobre segredo das comunicações;

g) constituam publicidade ilícita e enganosa, em geral, que constituam concorrência desleal;

h) incorporem vírus ou outros elementos físicos ou eletrônicos que possam causar dano ou impedir o normal funcionamento da rede, do sistema ou de equipamentos de informática (hardware e *software*) de terceiros ou que possam causar dano aos documentos eletrônicos e arquivos armazenados nestes equipamentos;

i) provoquem, por suas características, dificuldades no normal funcionamento do serviço;

j) permitam a tentativa de acesso ou o acesso às máquinas não autorizadas;

k) permitam a tentativa de quebra ou a quebra de sigilo de códigos alheios, o acesso e modificação de arquivos pertencentes a outros usuários sem a sua autorização.

VII - Penalidades

1 - O descumprimento das disposições constantes nessa Norma caracteriza infração funcional, a ser verificada em Processo Interno de Apuração (PIA), sem prejuízo das responsabilidades penal e civil.

2 - No caso de evidências de uso irregular dos recursos oferecidos, o usuário poderá ter seu acesso bloqueado durante a averiguação.

CAPÍTULO IV

DOS DISPOSITIVOS COMPUTACIONAIS

I - Estação de Trabalho

1 - Define-se como estação de trabalho, o dispositivo fornecido pela companhia para o usuário com o objetivo de tornar possível a execução de suas atribuições.

2 - A estação de trabalho é fornecida ao usuário como um conjunto de *hardware* e *software* sendo, atribuição da Sutin, definir a sua especificação.

3 - É dever da Sutin ou dos interlocutores de TI das Superintendências Regionais, manter atualizadas as estações de trabalho da Conab, sejam elas fixas ou móveis, com as atualizações de segurança e correções de *software*, de forma gerenciada e, se possível, automatizada.

4 - É dever do usuário, desligar sua estação de trabalho ao fim de seu expediente ou quando sua ausência for superior a 2 (duas horas) com objetivo de economia de energia. Salvo contrário, a Sutin ou os interlocutores de TI das Superintendências Regionais poderão programar para que as estações se desliguem automaticamente, considerando os casos de exceção devidamente informados.

5 - Em relação à licenças de uso de *softwares*:

a) apenas é autorizado o uso de *softwares* que possuam licenças legais para utilização na Conab, credenciadas e homologadas pela Sutin;

b) é facultado à Sutin ou aos interlocutores de TI das Superintendências Regionais, desinstalar *softwares* sem a devida licença em nome da Companhia ou que estejam em desacordo com o item anterior.

6 - Em relação ao equipamento ou conjunto deles:

a) o usuário é responsável e deverá zelar pelo pelo bom uso de sua estação de trabalho, seguindo os princípios éticos e morais na sua utilização;

b) no caso de necessidade de mudança de local físico da estação de trabalho, a Sutin ou os interlocutores de TI das Superintendências Regionais deverão ser contatados através do Sigede. Terceiros poderão ser autorizados pela Sutin, pelos interlocutores de TI das Superintendências Regionais ou, na ausência dos anteriores, pelo superior imediato da área envolvida, desde que acompanhados pelo responsável pela autorização;

c) o nome de identificação das estações de trabalho, os *softwares* previamente instalados, as configurações de hardware e de sistema operacional, não devem ser alterados, exceto pela Sutin ou pelos interlocutores de TI das Superintendências Regionais;

d) a utilização de privilégios de administrador de máquina deve ser prioritariamente vedada, exceto pela Sutin ou os casos autorizados por ela;

e) as estações de trabalho conectadas à rede de dados da Conab deverão ser apenas as de propriedade da própria Companhia, exceto as autorizadas pela Sutin;

f) é obrigação do usuário, comunicar à Sutin ou aos interlocutores de TI das Superintendências Regionais, qualquer comportamento que fuja ao padrão normal de funcionamento do equipamento, como, por exemplo, sintomas de vírus;

g) o usuário não possui permissão para desabilitar, nem mesmo temporariamente, os serviços administrativos de sua estação de trabalho, como antivírus, serviços de inventário, de acesso remoto e de atualização de sistema operacional;

h) caso o usuário perceba a ausência destes serviços administrativos, deve comunicar imediatamente à Sutin ou aos interlocutores de TI das Superintendências Regionais, para correção;

i) o usuário deve estar ciente que a execução destes serviços administrativos pode, eventualmente, causar lentidão no equipamento, sendo obrigação da Sutin, estabelecer políticas de execução deles que minimizem o impacto de tal execução.

7 - No caso de estação de trabalho móvel (*notebook, smartphones e tablets*), acrescenta-se:

a) que deve ser considerada a utilização de criptografia no disco de armazenamento interno, conforme seja definido pela Sutin;

b) deverá o computador móvel ser entregue para ser atualizado e verificado se está em conformidade em relação às atualizações de segurança para a Sutin ou para os interlocutores de TI das Superintendências Regionais, com periodicidade frequente conforme for definida pela própria Sutin.

8 - Em relação aos dados armazenados no equipamento:

a) os arquivos de interesse da Companhia devem ser armazenados em serviço de armazenamento fornecido pela Sutin. Os arquivos contidos apenas na sua própria estação de trabalho correm risco de serem perdidos por falha aleatória e eventual da própria estação;

b) no caso de estação de trabalho móvel (*notebook, smartphones e tablets*), os dados devem ser mantidos, prioritariamente, em serviço de armazenamento, disponibilizado pela Sutin. Caso haja indisponibilidade deste serviço, deverá, então, haver armazenamento em outro meio como *pendrive* ou similares, até o retorno da conexão com o serviço.

9 - Do acesso a sistemas:

a) o acesso a sistemas informatizados da Companhia se dá através de autorização do gestor do respectivo sistema. Em havendo necessidade de intermediação da área de tecnologia da informação, a fim de se proceder com tal acesso, esta solicitação deve ser através do Sigede;

b) após a autorização do gestor do respectivo sistema, o acesso deve ser concedido exclusivamente aos usuários que possuem necessidade para desempenhar suas funções no referido sistema, considerando, inclusive, o nível de acesso e permissões que deve ser disponibilizado para cada caso;

c) mesmas regras estão sujeitos os empregados cedidos pela Companhia ou que estejam em afastamento temporário.

CAPÍTULO V

AUTENTICAÇÃO E CREDENCIAIS

I - Do Gerenciamento de Contas

1 - O gerenciamento de contas e suas respectivas senhas, constituem o mecanismo básico para a autenticação de usuários dos sistemas computacionais da Conab.

2 - A Sutin é a responsável pela segurança e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle, bem como manter o sigilo das senhas de acesso a esse ambiente.

3 - O usuário é responsável por garantir a confidencialidade de suas credenciais por meio da assinatura de Termo de Ciência e Responsabilidade conforme Anexo I deste regulamento, sendo sua obrigação garantir o seu sigilo, jamais compartilhando com outros empregados da Companhia ou com terceiros.

4 - Cada empregado, terceirizado e estagiário deve possuir uma conta individual, não devendo existir contas compartilhadas por mais de um usuário.

5 - As contas de usuário possuem como nome de usuário a forma utilizada em contas de e-mail, seguindo o formato “nome.sobrenome@conab.gov.br”.

6 - Em caso de homônimo, ou seja, a existência de duas contas com o a mesma formação, o padrão adotado deve seguir as orientações existentes no eping (http://eping.governoeletronico.gov.br/).

7 - Para cada usuário é concedida apenas uma conta, que deverá ser utilizada para acesso aos serviços oferecidos pela Sutin.

8 - Toda conta deverá possuir uma senha de no mínimo oito dígitos alfanuméricos, na qual é obrigatório o uso de caracteres especiais e onde se deve evitar o uso de palavras de dicionário ou caracteres alfanuméricos em sequência.

9 - Uma conta recém-criada receberá uma senha gerada automaticamente, sendo esta considerada temporária até que o usuário faça seu primeiro acesso.

10 - A troca de senha temporária é obrigatória na primeira autenticação.

11 - A senha de usuário deve ser trocada a cada 180 (cento e oitenta) dias pelo próprio usuário, não podendo ser usada nenhuma das três utilizadas anteriormente, devendo conter letra(s), número(s) e símbolo(s), com tamanho mínimo de 8 caracteres. Em 30 (trinta) dias antes do prazo de alteração, o sistema operacional emitirá avisos com a devida solicitação. Caso a referida senha não seja alterada dentro do tempo estipulado, a Sutin poderá, por questões de segurança, desabilitar a conta de rede do respectivo usuário até seu devido restabelecimento de acordo com essa Norma.

12 - Em caso de esquecimento de senha, uma senha temporária poderá ser fornecida após solicitação por meio do Sigede. Neste caso, o superior imediato deverá fazer tal requisição, sendo gerada uma senha temporária que deverá ser entregue exclusivamente ao titular da conta pelo requisitante ou por meio da Sutin, com o apoio dos interlocutores de TI das Superintendências Regionais.

Continuação Capítulo V

II - Papéis e Níveis de Acesso

1 - As contas de usuário dão acesso aos recursos básicos da Rede Conab, além de uma conta de correio eletrônico vinculada.

2 - Diferentes contas podem possuir níveis de acesso distintos a sistemas e serviços, sendo o credenciamento e a definição de tais níveis, de responsabilidade da Sutin, por orientação e definição dos gestores de negócio da Companhia.

3 - A concessão de credenciais ao usuário, com nível administrativo para serviços, recursos e aplicações, deve ser solicitada pelo superior imediato sendo facultado à Sutin, conceder tais credenciais considerando a necessidade.

4 - O gestor do sistema de informação deve conduzir em intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

III - Contas Corporativas

1 - Contas corporativas são utilizadas para tornar a comunicação e a utilização de recursos computacionais impessoais, sendo utilizadas primariamente para o gerenciamento de E-mail.

2 - A criação de uma conta corporativa deve ocorrer por meio do Sigede, indicando o responsável pela sua administração.

IV - Contas de Usuários Externos

1 - A criação de contas de acesso de agentes externos, quais sejam, terceirizados, servidores de órgãos de controle e outros prestadores de serviço, deverão ser solicitadas à área de recursos humanos e supervisionadas pelo responsável pelo projeto ou unidade orgânica demandante, a quem compete levar ao conhecimento do agente externo as Políticas de Segurança da Informação (NOC 10.010) da Conab, além desta Norma de Recursos Computacionais (NOC 60.213), garantindo tal ciência por meio da assinatura de “TERMO DE CIÊNCIA E RESPONSABILIDADE”, Anexo I desta Norma, pelos respectivos agentes externos.

2 - Cabe à área de recursos humanos o cadastramento do agente externo em seu sistema, como terceirizado, inclusive apontando tal natureza no cadastramento do e-mail com o subdomínio @ps.conab.gov.br.

3 - O responsável pelo projeto ou unidade orgânica demandante obriga-se a informar à área de recursos humanos, o desligamento do agente externo frente as atividades relacionados à Conab, que por sua vez deverá excluí-lo do cadastro de terceirizados.

V - Infrações Específicas

1 - São consideradas infrações, específicas a este Capítulo:

a) fornecer a senha de acesso a usuários externos;

b) utilizar a senha de outro usuário sem seu consentimento;

c) utilizar os recursos oferecidos pela conta de acesso com fins comerciais não autorizados explicitamente;

d) utilizar a conta de acesso para conseguir acesso não autorizado a recursos ou informações, ou para degradar o desempenho, ou para colocar fora de operação sistemas computacionais locais ou remotos.

CAPÍTULO VI

SERVIÇOS DE COMUNICAÇÃO

I - Do Uso dos Serviços de Comunicação

1 - Para fins desta Norma, serviços de comunicação englobam correio eletrônico, mensagens instantâneas, listas de e-mail, serviços de videochamada e a infraestrutura de telefonia IP providos pela Sutin ou contratados pela Companhia.

2 - Os serviços de comunicação são disponibilizados como ferramenta para comunicação e colaboração, tanto internamente, com o corpo funcional, quanto com o público externo.

3 - Os serviços de comunicação são de uso exclusivo dos empregados, incluindo todos que se vinculem à administração, ainda que de maneira transitória.

4 - Define-se como regras para uso dos serviços de comunicação:

a) a utilização do serviço deve se dar de forma profissional, ética e legal, sendo vedado o uso para fins particulares;

b) é vedado, para fins particulares, o cadastro em serviços de redes sociais ou comércio eletrônico, ferramentas de marketing utilizando o e-mail corporativo da Conab;

c) é proibido o uso do serviço para envio de mensagens em massa (*spam*).

5 - A Conab se reserva o direito de aplicar filtros automatizados, para o bloqueio de mensagens que possuam conteúdos incompatíveis com o interesse da instituição. Tais filtros serão definidos pela Sutin, conforme as melhores práticas do mercado.

6 - No caso de desligamento do empregado, as mensagens armazenadas em sua caixa de correio eletrônico ficarão disponíveis por 15 (quinze) dias após a data de sua rescisão de contrato de trabalho, podendo os conteúdos serem disponibilizados ao empregado ou a seu superior imediato mediante solicitação à Sutin.

7 - Compete à Sutin, monitorar os serviços de comunicação para garantir disponibilidade e segurança do mesmo, mantendo registro de envios e recebimentos de mensagens, respeitando a privacidade legal.

8 - É facultada à Sutin, acesso ao conteúdo de registros de envio e recebimento de mensagens, assim como ao conteúdo dos mesmos, para verificações de segurança como nos casos de incidentes de segurança, detecção de falhas e/ou vulnerabilidades, sendo resguardada a privacidade legal.

9 - Uma vez anonimizados, os registros de envio e recebimento de mensagens, assim como o conteúdo dos mesmos, podem ser utilizados para análises estatísticas e desenvolvimento de serviços.

10 - Sobre listas de discussão por e-mail:

a) a criação de listas de discussão deve se dar por meio do Sigede;

b) o acesso à configuração do servidor de listas e principalmente a seus inscritos deve ser rigorosamente controlado e limitado apenas ao administrador (ou dono) da lista;

c) o administrador do serviço de lista de discussão pode delegar a outras pessoas (usuários que pertençam a Conab) a administração de uma determinada lista. Essa pessoa ficará encarregada da sua manutenção (inclusão/remoção de usuários, moderação, etc.).

CAPÍTULO VII

SERVIÇOS DE ACESSO À INTERNET

I - Da Navegação à Internet aos Usuários em Geral

1 - A navegação na internet é disponibilizada como um serviço com o objetivo de permitir ao corpo funcional a execução de suas atribuições funcionais.

2 - Todos os acessos de navegação na internet serão devidamente registrados para fins legais e de análise estatística, respeitando a privacidade legal.

3 - O acesso à rede disponibilizado aos usuários da Conab deverá ser realizado prioritariamente para os interesses de trabalho, não ficando excluído o uso para outros interesses, desde que:

a) seja feito, preferencialmente, fora do período normal de expediente;

b) não exceda aos limites da ética, do bom senso e da razoabilidade;

c) não contenha, receba ou transmita informações institucionais sigilosas ou protegidas;

d) não contrarie as leis, normas e procedimentos institucionais vigentes;

e) não interfira, prejudique ou desperdice recursos e serviços de rede.

4 - É facultada à Sutin, o acesso aos registros de navegação na internet para verificações de incidentes de segurança como detecção de falhas e/ou vulnerabilidades, resguardada a privacidade legal.

5 - Uma vez anonimizados, os registros de acesso à internet podem ser utilizados para análises estatísticas e desenvolvimento de serviços.

6 - Somente é permitida a navegação na internet utilizando a estrutura de *proxies* fornecida pela Companhia, sendo vedado o uso de serviços externos como *proxies* de terceiros, anonimizadores de tráfego, VPNs e afins.

7 - Os acessos a serviços externos que utilizem protocolos encriptados poderão ocorrer de forma interceptada, desde que se garanta a privacidade das informações, sendo o mecanismo de interceptação utilizado apenas quando estritamente necessário. Ainda:

a) quando houver necessidade de análise das informações interceptadas, e estas contiverem dados relativos à privacidade de pessoas naturais, mesmo que para alguma eventual resolução de problemas e diagnóstico de falhas, deve haver, neste caso, formalização e autorização do superior imediato e das pessoas naturais impactadas pela quebra do respectivo sigilo, conforme Lei n.º 13.709/2018.

8 - Deve ser utilizado mecanismo de bloqueio de acesso a endereços que forem considerados impróprios, contendo software malicioso, pornografia ou cujo uso possa comprometer outros serviços da Companhia.

9 - Caso algum *site* seja incorretamente classificado como sendo impróprio, o usuário poderá solicitar a liberação do mesmo via sistema específico exibido na própria página de bloqueio.

Continuação Capítulo VII

10 - Cabe ao Comitê Gestor de Segurança da Informação (CGSI) definir os parâmetros utilizados para controle de acesso a sites na Companhia.

11 - É facultado à Sutin, criar grupos com diferentes níveis de acesso à internet, de acordo com necessidade definida pelo gestor da área e, também, baseando-se nos parâmetros definidos pelo Comitê Gestor de Segurança da Informação (CGSI).

II - Do Uso da Rede

1 - O acesso à rede de dados pelos recursos computacionais dos usuários deve ser disponibilizado através da liberação de endereço MAC previamente cadastrado ou por tecnologia que garanta melhor controle de acesso.

2 - O acesso à Internet se dará, para Matriz da Conab, por meio de rede local (LAN) e para as Superintendências Regionais e Unidades Armazenadoras, por meio de rede local (LAN) interconectada à Matriz por meio de rede de longa distância (WAN).

3 - É vedado aos usuários da rede da Conab:

a) acessar ou tentar acessar a rede por meio de usuário, dispositivo, equipamento ou software não autorizado;

b) fazer uso indevido da rede;

c) interferir na infraestrutura física da rede e seus elementos, exceto aos empregados designados pela Sutin;

d) interceptar ou tentar interceptar a transmissão de dados através da rede;

e) acessar, configurar, instalar ou conectar em ativos de rede, como: *hub, switches, scanners, modem*, roteadores, entre outros, sem o conhecimento e autorização da Sutin;

f) desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores da Conab;

g) conectar, instalar ou utilizar equipamentos de rede sem fio (*wireless*), sem o conhecimento e autorização da Sutin;

h) prospectar, planejar ou contratar serviços de rede, sem o conhecimento, apoio técnico ou autorização da Sutin.

4 - Cabe ao usuário da rede de dados da Conab comunicar a Sutin, qualquer evento alheio ou estranho ao funcionamento normal da rede, por meio do Sigede, fornecendo ou solicitando informações necessárias ao atendimento e registro da ocorrência.

5 - Cabe à Sutin, por meio de suas gerências subordinadas:

a) apoiar tecnicamente a prospecção, planejamento ou contratação de serviços de rede;

b) administrar a rede corporativa da Conab, observando às melhores práticas, normas, leis e padrões recomendados;

c) realizar o monitoramento e resolução de problemas da rede;

d) proteger os serviços e ativos de rede utilizando ferramentas apropriadas, como *firewall*, *proxy*, sistemas de detecção de intrusão, etc;

e) bloquear os serviços desnecessários ou ameaças que possam comprometer o desempenho, integridade ou disponibilidade da rede;

f) manter atualizados os ativos de rede (incluindo *switches*, *hub*s e roteadores);

g) somente fornecer informações de rede, caso exista uma solicitação formal superior ou judicial;

h) limitar ao máximo a divulgação de informações de roteamento, faixa de endereçamento IP, servidores, equipamentos de rede, entre outros, a terceiros;

i) garantir, em níveis mínimos aceitáveis, a disponibilidade, integridade, confidencialidade, autenticidade e a irretratabilidade na utilização da rede da Conab, em conformidade com os recursos disponíveis.

CAPÍTULO VIII

DO CONTROLE DE ACESSO REMOTO

I - Regras Gerais

1 - O acesso remoto à Rede Corporativa da Conab deve ser realizado somente para atender aos interesses da Companhia.

2 - O acesso remoto à Rede Corporativa deve ser feito através de diferentes perfis de acesso, onde o superior imediato definirá o perfil de cada subordinado ou, caso o acesso remoto seja realizado por agente externo, o perfil concedido deverá ser solicitado pela área que motivou o acesso.

3 - O acesso remoto, via VPN, aos recursos da Companhia deve ser concedido como último recurso, apenas disponibilizado caso não seja possível ao usuário realizar suas atividades sem o mesmo.

4 - As ferramentas utilizadas no acesso remoto devem ser previamente homologadas pela Sutin, não sendo permitido o acesso remoto a recursos mantidos dentro da rede corporativa por serviços que dependam da infraestrutura de terceiros. De forma geral, tais ferramentas devem obedecer às seguintes recomendações:

a) utilizar estrutura de credenciais e autenticação já em uso na Companhia;

b) gerar registros de atividades, permitindo identificar não apenas as credenciais que foram utilizadas no acesso, como também quais recursos foram acessados e que ações foram tomadas;

c) utilizar protocolo de rede criptografado;

d) utilizarem estrutura de permissão de uso da base de credenciais da Companhia.

5 - Nos serviços onde é utilizada estrutura de certificados para acesso, o usuário é o responsável pela guarda do certificado, não lhe sendo permitida a transferência do mesmo.

6 - Caso um certificado de acesso remoto seja perdido, extraviado ou divulgado para terceiros, o responsável deve solicitar imediatamente a sua revogação junto à Sutin de modo a evitar uso indevido por terceiros.

7 - O acesso remoto a estações de trabalho é condicionado a liberação do usuário corrente de forma excepcional e justificada, sendo o mesmo limitado a atendimentos de suporte ou trabalho colaborativo.

8 - É facultado a Sutin, por razões críticas de segurança, sem devido aviso prévio, acesso remoto às estações de trabalho para execução de rotinas que sejam consideradas de emergência, como remoção de *malware* ou atualizações de segurança.

9 - O acesso remoto aos servidores deve ser limitado aos analistas da área de tecnologia da informação vinculados à Sutin e aos interlocutores de TI das Superintendências Regionais, estes últimos apenas quando necessitarem de acesso aos servidores existentes exclusivamente na sua respectiva superintendência. Todos estes acessos devem possuir o menor nível de privilégio possível para execução de suas atividades.

CAPÍTULO IX

DOS SERVIÇOS DE ARMAZENAMENTO DE DADOS

I - Dos Serviços de Armazenamento de Arquivos

1 - Reconhecemos os serviços de armazenamento de arquivos como armazenamento em nuvem, compartilhamentos em servidores e outros serviços de armazenamento de arquivos disponibilizados pela Companhia ao usuário.

2 - O acesso a compartilhamentos institucionais deve ser concedido sob solicitação do gestor da área correspondente.

3 - Todos os serviços de armazenamento devem ser concedidos considerando quotas definidas por usuário, no caso de compartilhamentos individuais, ou quotas de unidade orgânica, para os demais compartilhamentos.

4 - O acesso aos serviços de compartilhamento deve utilizar as credenciais de acesso a rede da Companhia.

5 - Deve se estabelecer uma política de arquivamento de forma que apenas arquivos em uso corrente estejam armazenados nos servidores, sendo o material de necessidade histórica ou de uso para auditoria armazenado em meio óptico ou magnético.

6 - Deve-se estabelecer uma janela de recuperação de arquivos, não sendo garantida a recuperação de versões de arquivos ou arquivos removidos há mais de 30 (trinta) dias.

7 - Deve-se estabelecer uma política de conteúdo para os serviços de armazenamento corporativo, garantindo ao administrador permissão de veto nas seguintes condições:

a) não é permitido o armazenamento de arquivos de uso pessoal;

b) não é permitido o armazenamento de conteúdo pornográfico, *malware*, *softwares* piratas ou não licenciados pela Companhia;

c) a Sutin tem permissão de remoção imediata de arquivos que contrariem esta Norma, sendo o usuário responsável passível de medidas administrativas por mau uso.

8 - A Sutin deve possuir acesso aos arquivos em qualquer meio para fins de gerenciamento de espaço de armazenamento e auditoria relacionada a uso irregular dos serviços, respeitando a privacidade legal dos usuários da Companhia.

9 - Deve se estabelecer registro de rastreamento dos serviços de armazenamento de forma a permitir a auditoria do uso dos recursos, prevenir a ação de *malware* e analisar acessos indevidos aos arquivos.

10 - Deve-se dar preferência a serviços que utilizem protocolos criptografados no processo de autenticação e transmissão de arquivos.

11 - Somente é permitido o compartilhamento de arquivos com terceiros (pessoas que não possuem conta na Conab) mediante o uso de senha e com limitação de prazo de acesso.

CAPÍTULO X

FLUXO DO PROCESSO

Não se Aplica.

CAPÍTULO XI

DISPOSIÇÕES GERAIS

I - Alinhamento aos Princípios da Administração Pública

1 - De forma ampla, a utilização do uso dos recursos computacionais desta Companhia, do qual se baseia esta Norma, deve estar aderente e alinhada aos princípios básicos da administração pública, portanto prezando pela ética, legalidade, moralidade, publicidade, eficiência, razoabilidade, proporcionalidade, contraditório e ampla defesa, além da supremacia do interesse público.

CAPÍTULO XII

ANEXOS

I - TERMO DE CIÊNCIA E RESPONSABILIDADE

Conab	**TERMO DE CIÊNCIA E RESPONSABILIDADE**

Declarante:		
Endereço:		
Bairro:		
Cidade:	UF	CEP:
CPF:	Telefone: ( )	
Data Início da prestação do serviço	Data Fim da prestação do serviço	

Declaro que recebi, nesta data, senha de acesso à rede de computadores da Companhia Nacional de Abastecimento (Conab), sendo esta pessoal e intransferível.

Tenho conhecimento que o acesso às informações por meio desta senha é de minha inteira responsabilidade e que qualquer acesso indevido a partir desta autorização (usuário/senha) de acesso, estará sujeita às sanções legais.

Comprometo-me a zelar pelo absoluto sigilo da senha e, também, a solicitar o cancelamento dela, caso ocorra qualquer alteração da representatividade legal que hoje detenho.

Declaro, ainda, ter ciência da Política de Segurança da Informação (NOC 10.010) e da Norma de Recursos Computacionais (NOC 60.213) da Conab.

Local e Data	Assinatura do Usuário

RESPONSÁVEL NA CONAB
Autorizado por (Assinatura e Carimbo)
Este documento deverá ser preenchido, assinado e autorizado, antes de ser encaminhado à Sutin.