ANEXO I

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Federais vinculados à Advocacia-Geral da União – AGU, que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico, são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - 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;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, **script**, etc.), sem qualquer intervenção humana no seu uso;

VII - 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;

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

IX - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo

que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

X - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XI - dado: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIII - endereço IP (**Internet Protocol**): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por " . " e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIV - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVI - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVII - estágio supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVIII - ferramenta de gestão de acessos: **software** que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

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

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXIII - **log** ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, **scanners**, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto; e

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo.

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado (s) sistema (s) corporativo (s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral é a base de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e dos sistemas legados, que devem ser alimentadas por informações disponibilizadas pelo INSS. Para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

ITEM	INFORMAÇÃO	CAMPO	DESCRIÇÃO
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

Parágrafo único. A Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Sobre credenciais e perfis de acesso, verifica-se que a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos, a credencial deve ser associada a um perfil de acesso, e o o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

III - as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

§ 1º A área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para solicitar:

I - o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

II - a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

IV - a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.

§ 2º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento "Caixas Individuais-Fundacionais no Governo Federal" (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

§ 3º Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

§ 4º Os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses.

§ 5º Quanto à utilização das credenciais e perfis de acesso, o usuário:

I - deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

II - deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;

III - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

VI - não pode fazer uso das credenciais de acesso de outros usuários;

VII - deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VIII - deve comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do **software** ou de outros ativos da informação;

IX - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;

X - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XI - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

§ 6º O processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

§ 7º O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário.

§ 8º O cadastro de que trata o § 7º deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

§ 9º O credenciamento de estagiários, se dará com a a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

V - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

VIII - os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

IX - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

X - o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

§ 10. O credenciamento de usuários externos, obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

III - a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

a) a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

b) instrumento deve conter cláusulas prevendo:

1. a necessidade e justificativa para acesso à rede corporativa;

2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto; e

3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

c) a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

d) o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

IV - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou **link** eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

V - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

VI - a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

§ 11. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; e

VII - o INSS pode disponibilizar, de forma restrita, às centrais 135, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 12. Nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com a Ouvidoria do Ministério da Economia;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 13. O acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares.

§ 14. O tipo de acesso de que trata o § 12 deverá observar:

I - as parcerias institucionalmente estabelecidas entres esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

§ 15. O bloqueio administrativo se dará da seguinte forma:

I - o responsável pela Corregedoria-Geral do INSS, quando necessário, poderá solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

a) afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

b) indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias; e

c) submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal;

II - as solicitações de que tratam o inciso I deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança;

III - o bloqueio de acessos tratados nas situações do inciso I serão efetivados no âmbito da ferramenta de gestão de acessos nas seguintes situações:

a) usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

b) usuário indiciado nos termos da alínea "c" do inciso I do § 15, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa.

§ 1º Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

§ 2º O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia **Wirelles** (sem fio). Para tanto os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; e

III - as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

§ 3º A área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto.

§ 4º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

§ 5º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

§ 6º A administração da rede corporativa trata da operacionalização da rede do INSS, que é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto e seguem as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se ao monitoramento de serviços de tecnologia contratados pelo Instituto, seguindo as regras desta Norma.

§ 7º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

II - a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma;

III - o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

§ 8º É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

III - a utilização de **softwares** particulares em equipamentos do INSS sem autorização expressa;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

VIII - a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

IX - burlar as regras de acesso a internet configuradas em **proxy** ou ferramenta similar de gerenciamento de conteúdo **web**.

§ 9º Cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria;

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS;

III - armazenamento de registros **logs**:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos **logs** de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no **caput** do art. 8º;

b) o INSS poderá alterar a temporalidade destes dados em norma específica; e

c) os **logs** de acesso devem contemplar minimamente os registros relacionados no Anexo III;

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedora-Geral e PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências-Regionais - SR;

4. gestor de acesso interno: servidor do quadro, lotado na Administração Central, SR, Gerência-Executiva - GEX, Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto;

b) os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto;

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários;

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma;

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma;

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS;

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável;

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS;

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, SR, GEX, APS;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX, APS; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários; e

e) a instalação de sistemas corporativos em equipamentos particulares;

VI - em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no § 2º do art.8º.

Art. 8º Todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze (12) meses, observando o disposto no inciso III do art. 7º.

§ 1º As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento.

§ 2º Identificada irregularidade de mau uso dos recursos de rede poderá ocorrer o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias-Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar.

§ 3º O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

Art. 9º Esta norma deve ser revisada num período máximo de 3 (três) anos.