PORTARIA MCOM Nº 2.805, DE 11 DE JUNHO DE 2021

Aprova a Norma Complementar para Controle de Acesso Lógico do Ministério das Comunicações.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, o Decreto nº 7.845, de 14 de novembro de 2021, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Controle de Acesso Lógico do Ministério das Comunicações.

Art. 2º Esta Portaria entra em vigor:

I – após o termino do apoio operacional prestado pelo Ministério da Ciência, Tecnologia e Inovações, decorrente da Portaria Interministerial nº 3.473, de 10 de setembro de 2020, e alterações posteriores, em relação ao item 2.10.

II – na data da sua publicação, em relação aos demais itens.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA CONTROLE DE ACESSO LÓGICO

OBJETIVO

Esta norma de segurança tem por objetivo definir critérios de segurança para implementação de controle de acesso lógico no âmbito da Rede Corporativa do Ministério das Comunicações - MCOM.

APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA

Norma NBR ISO/IEC 27000 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação;

Norma NBR ISOIEC 17799 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação;

Decreto nº 9.637, de 26 de dezembro de 2018, que Institui a Política Nacional de Segurança da Informação, 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;

Decreto nº 7.845, de 14 de novembro de 2021, 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;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações.

1. **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 - 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;

III - 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;

IV - 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;

V - 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;

VI - 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;

VII - 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;

VIII - 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;

IX - 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;

X - 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;

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

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

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

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

XV - 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;

XVI - usuário: servidores, terceirizados, colaboradores, procuradores, advogados da união, 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 de Termo de Responsabilidade.

2. **PROCEDIMENTOS:**

2.1 O Serviço de Diretórios (acesso à rede de dados) deve ser alimentado por informações disponibilizadas pelas áreas de Gestão de pessoas, de Logística, de Comunicação e de Tecnologia da Informação e Comunicações - TIC do MCOM.

2.2 A área de TIC procederá com a atualização das bases cadastrais do serviço de diretórios na periodicidade do envio das informações.

2.3 O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, estagiários, terceirizados e consultores no âmbito do Ministério, deve observar os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do MCOM 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 MCOM, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

2.4 A área responsável pela gestão de pessoas do MCOM deverá utilizar os canais de atendimento, ou outro canal informado pela área de TIC, para solicitar:

I - o credenciamento de servidores, empregados públicos e estagiários do quadro de pessoal do MCOM na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede;

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

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

2.5 Os responsáveis pela gestão dos contratos de mão de obra terceirizada nas áreas de logística, comunicação e tecnologia da informação e comunicações do MCOM deverão utilizar os canais de atendimento, ou outro canal informado pela área de TIC, para solicitar:

I - o credenciamento de usuários do quadro de terceirizados sob sua gestão na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede;

II - a revogação de credenciais de acesso de terceirizados sob sua gestão; e

III - a desativação de usuários terceirizados sob sua gestão na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico.

2.6 Todos os usuários devem assinar o Termo de Responsabilidade e Confidencialidade, ANEXO I, que deve ser providenciado previamente pela área responsável pela solicitação de credenciamento, ou seja, pelas áreas de Gestão de pessoas, logística, comunicação ou de Tecnologia da Informação e Comunicações do MCOM

2.7 Quanto ao processo de formação das credenciais de acesso, fica estabelecido que o nome do usuário será composto, por padrão, por <primeiro_nome>.<último_sobrenome>, sendo possível acatar sugestão do próprio usuário, desde que seja composta por dois componentes do nome completo, separados por um ponto. Nos casos de indisponibilidade da credencial, serão tentadas outras combinações dos componentes do nome completo, iniciando sempre pelo primeiro nome.

2.8 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 duas senhas utilizadas pelo usuário;

III - terão validade de 180 dias; e

IV - podem ser alteradas sempre que preciso ou quando o usuário achar necessário.

2.9 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 MCOM 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; e

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

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

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

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

2.13 É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado pela ANATEL ou não autorizado pelo MCOM;

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

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

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

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do MCOM, 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 MCOM;

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

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

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

2.14 Cabe à área responsável pela gestão de TIC no âmbito do MCOM definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do MCOM.

2.15 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 MCOM para análise e pronunciamento.

2.16 Identificada irregularidade de mau uso dos recursos de rede poderá ocorrer o bloqueio preventivo do acesso pela área de TIC, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do MCOM, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar.

2.17 O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais, na forma da lei.

ANEXO I
TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Pelo presente instrumento, eu _____, CPF nº _____, documento de identidade nº _____, expedida pelo _____, em _____, e lotado no Ministério das Comunicações - MCOM, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIC do MCOM que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Ministério das Comunicações;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do MCOM;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do MCOM;

V - responder, perante o MCOM, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____de _____de _____

Nome e assinatura do usuário:

Unidade de Lotação:

Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Gestora de Segurança da Informação**, em 11/06/2021, às 11:12 (horário oficial de Brasília), com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **7597535** e o código CRC **51F75613**.

Referência: Processo nº 53115.007158/2021-12 SEI nº 7597535