Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 182 - DOU – 19/09/2024 - Seção 1 – p.13

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

PORTARIA CNPQ Nº 1.868, DE 17 DE SETEMBRO DE 2024

O Presidente do CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq, no uso das atribuições que lhe são conferidas pelo Estatuto aprovado pelo Decreto nº 11.229, de 7 de outubro de 2022, e tendo em vista a deliberação da Diretoria Executiva em sua 9ª (nona) reunião, de 17 de julho de 2024, a deliberação do Comitê de Segurança da Informação em sua 2ª (segunda) reunião, de 1º de março de 2024, a Política de Segurança da Informação - PoSIN do CNPq estabelecida pela Portaria CNPq nº 1.019, de 30 de agosto de 2022, e com base na Estratégia de Governo Digital - Decreto nº 10.332 de 28 de abril de 2020, e em conformidade com a legislação aplicável e demais atos normativos pertinentes, e nos termos do processo SEI nº 01300.002032/2024-11, resolve:

Art. 1º Aprova e homologa a Política de Gestão de Controle de Acesso, proposta pelo Comitê de Segurança da Informação - CSI, em complemento às diretrizes estabelecidas pelo Capítulo II, da Política de Segurança da Informação (POSIN) do CNPq e como parte integrante do Programa de Privacidade e Segurança da Informação do CNPq.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Objeto e âmbito de aplicação

Art. 2º A Política de Gestão de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que impliquem em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 3º O controle de acesso será definido e mantido com base em funções, determinando e documentando os direitos de acesso necessários para que cada função seja cumprida com sucesso dentro da organização.

§ 1º A análise de controle de acesso deverá ser realizada anualmente, de modo a validar os privilégios autorizados.

§ 2º O privilégio mínimo deve ser considerado em todas as autorizações de acesso, para que o acesso seja concedido ao mínimo necessário para a realização das atividades pertinentes ao trabalho.

Art. 4º Os controles de autorização, identificação e autenticação devem ser implementados visando minimizar o risco potencial dos sistemas de informação serem acessados ilicitamente e a segurança desses sistemas de informação seja comprometida.

§ 1º Considera-se, portanto, que as credenciais de identificação: crachá de identidade funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

§ 2º Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do CNPq.

Art. 5º Esta Política se aplica a todas as informações, das quais o CNPq seja o agente de tratamento, incluindo o meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento, incluindo especificamente:

I - todos os servidores efetivos ou temporários, estagiários e colaboradores eventuais e contratados das empresas prestadoras de serviços ao CNPq; e

II - todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do CNPq de forma presencial ou remota.

Definições

Art. 6º Para os fins desta Política, considera-se:

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

II - 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, o qual via de regra, requer procedimentos de autenticação;

III - Rede Privada Virtual (ou "Virtual Private Network" - VPN): rede de comunicações privada construída sobre uma rede de comunicações pública ou compartilhada como, por exemplo, a Internet, que cria uma conexão segura e criptografada, considerada como um túnel entre o computador do usuário e um servidor operado pelo serviço VPN, com o objetivo de fornecer a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas;

IV - serviço de diretório: sistema de software que armazena, organiza e fornece acesso a conjunto de atributos sobre recursos e serviços existentes na rede, como por exemplo, usuários, computadores, impressoras, servidores entre outros recursos de rede;

V - autenticação multifator: tecnologia que solicita ao usuário de uma plataforma, um aplicativo ou um sistema a confirmação de sua identidade em dois ou mais momentos, antes de liberar o acesso dele ao sistema;

VI - usuários de recursos de tecnologia da informação: são os servidores ocupantes de cargo efetivo ou cargo em comissão, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no CNPq.

CAPÍTULO II

ACESSO LÓGICO

Art. 7º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso.

Parágrafo único. O acesso deve ser concedido e mantido pelo Serviço de Suporte ao Usuário de TI (SESUT)), vinculado à Coordenação de Infraestrutura de TI (COINT) da Coordenação-Geral de Tecnologia da Informação (CGETI), baseado nas responsabilidades e tarefas de cada usuário.

Art. 8º Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

Art. 9º O acesso remoto deve ser realizado por meio do serviço de Rede Virtual Privada - VPN, que deverá ser solicitado e autorizado seguindo processo formal estabelecido para o acesso a esse serviço.

Parágrafo único. O usuário do serviço de VPN deverá assinar Termo de Responsabilidade específico (Modelo - Anexo II), que estabelece, dentre outros requisitos, a responsabilidade do usuário pela instalação e atualização de antivírus no equipamento que fará o acesso remoto à Rede Local do CNPq.

CAPÍTULO III

CONTA DE ACESSO LÓGICO E SENHA

Login e senha

Art. 10. Para utilização das estações de trabalho do CNPq, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pelo SESUT, mediante solicitação formal pelo titular da unidade do requisitante.

§ 1º O formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet do CNPq.

§ 2º Os privilégios de acesso dos usuários à Rede Local, sistemas e serviços de TI devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 3º Na necessidade de utilização de perfil diferente do disponibilizado, o gestor da unidade do usuário deverá encaminhar solicitação para o SESUT que a examinará, podendo negá-la nos casos em que entender desnecessária.

Art. 11. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo SESUT, quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 12. O padrão adotado para o formato da conta de acesso do usuário (login) é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joao.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, o SESUT realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 13. O padrão adotado para o formato da senha é o definido pelo SESUT, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

Art. 14. A formação da senha de acesso à Rede Local deve seguir as seguintes regras:

I - possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números e as seguintes recomendações:

a) utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

b) não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

c) não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system; e

d) não reutilizar as últimas 5 (cinco) senhas; e

II - o SESUT fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 15. As senhas de acesso serão renovadas a cada 24 (vinte e quatro) meses, devendo o usuário ser informado antecipadamente da necessidade de alteração de sua senha, a fim de que ele próprio possa efetuar a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, seu acesso será bloqueado à Rede Local até que nova senha seja configurada.

Art. 16. Os sistemas críticos do CNPq deverão possuir autenticação integrada ao serviço de diretório da Instituição.

Art. 17. Deverá ser habilitada autenticação multifator para:

I - acesso dos usuários e administradores à Rede Local do CNPq;

II - acesso aos sistemas e serviços críticos de TI;

III - acesso aos sistemas internos e externos, em nuvem pública ou privada;

IV - gerenciamento da infraestrutura de TI do CNPq; e

V - acesso à VPN do CNPq.

Art. 18. A CGETI deverá implementar processo automatizado para verificação da saúde operacional das estações de trabalho de usuários em trabalho remoto que acessam o ambiente pela VPN.

CAPÍTULO IV

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 19. A conta de acesso será bloqueada nos seguintes casos:

I - após 5 (cinco) tentativas consecutivas de acesso errado;

II - solicitação do superior imediato do usuário com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pelo CNPq ou descumprimento da Política de Segurança da Informação (POSIN) e normas correlatas em vigência;

IV - após 180 (cento e oitenta) dias consecutivos sem movimentação pelo usuário; e

V - decorridos 90 (noventa) dias após a aposentadoria.

Art. 20. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao SESUT.

Art. 21. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do SESUT.

Art. 22. A CGETI deverá implementar processo automatizado para revogação de acessos, inativação e cancelamento das contas cujos períodos de inatividade atinjam os prazos estabelecidos no art. 19 desta Portaria.

Art. 23. Os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

CAPÍTULO V

MOVIMENTAÇÃO INTERNA

Art. 24. Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede Local devem ser readequados, conforme solicitação do novo superior imediato ao SESUT.

Parágrafo único. Os direitos de acesso antigos devem ser imediatamente cancelados mediante solicitação do antigo superior imediato ao SESUT.

CAPÍTULO VI

CONTA DE ACESSO BIOMÉTRICO

Art. 25. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para obtenção de um acesso, a fim de atender os conceitos da autenticação multifator.

Parágrafo único. O CNPq deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VII

ADMINISTRADORES

Art. 26. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para execução de tarefas específicas na administração de ativos de informação e restritas aos usuários cadastrados.

§ 1º Somente os técnicos da CGETI, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§ 2º Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação da CGETI por meio do SESUT.

§ 3º A CGETI deve implementar a autenticação multifator para todas as contas de administrador.

§ 4º A CGETI deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com este privilégio não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

§ 5º Ao tratar dados pessoais o CNPq deve observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

I - remover os direitos de administrador nos dispositivos finais;

II - remover todos os direitos de acesso root e "admin" aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

III - eliminar privilégios permanentes (privilégios que estão "sempre ativos") sempre que possível;

IV - limitar a associação de uma conta privilegiada ao menor número possível de pessoas; e

V - minimizar o número de direitos para cada conta privilegiada.

Art. 27. Nos casos em que a utilização de login com privilégio de administrador do equipamento local for necessária, o usuário deverá encaminhar solicitação motivada ao SESUT, que poderá negar os casos em que entender desnecessária sua utilização.

§ 1º A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, não podendo ser superior a 30 dias, no entanto poderá ser renovada por solicitação formal do titular da unidade requisitante.

§ 2º Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do CNPq, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos, servidores e a dispositivos de rede.

CAPÍTULO VIII

RESPONSABILIDADES

Art. 28. É de responsabilidade da Coordenação Geral de Gestão de Pessoas (CGGEP) e do SESUT comunicar formalmente o desligamento ou saída do usuário do CNPq para que as permissões de acesso à Rede Local, sistemas e serviços de TI sejam canceladas.

Art. 29. Caberá à CGGEP do CNPq a comunicação imediata ao SESUT sobre desligamentos de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos de TI.

Art. 30. É responsabilidade dos Gestores de contratos de terceirização a comunicação imediata a CGETI sobre desligamentos de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos de TI.

Art. 31. O monitoramento da utilização de serviços de rede e de acesso à Internet é de responsabilidade da CGETI, podendo ainda exercer a função de investigação nos casos de apuração de uso indevido desses recursos.

Parágrafo único. A CGETI poderá bloquear, temporariamente, sem aviso prévio, a estação de trabalho que estiver realizando atividades que coloquem em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do CNPq.

Art. 32. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do CNPq.

§ 1º O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

§ 2º A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo de responsabilidade do usuário titular da conta de acesso os riscos que essa utilização paralela implica.

§ 3º O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 33. O usuário deve informar ao SESUT qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 34. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para o CNPq, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas pelas normas de uso dos mesmos e regras estabelecidas nesta Portaria;

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis; e

VIII - assinar o Termo de Responsabilidade de utilização da respectiva conta de acesso, conforme modelo constante no Anexo I desta Portaria.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 35. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e de outras normas de segurança devem ser obrigatoriamente comunicados pelos usuários ao SESUT.

Art. 36. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a CGETI fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

§ 1º Nos casos em que o responsável pela quebra de segurança for um usuário, a CGETI comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

§ 2º As ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isolada ou cumulativamente.

Art. 37. Processo Administrativo Disciplinar específico será instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Política e pela POSIN.

Art. 38. Os casos de violação ou transgressões omissos nesta Política e nas legislações correlatas serão resolvidos pelo Comitê de Segurança da Informação (CSI) do CNPq.

Art. 39. Esta Portaria entra em vigor 30 (trinta) dias após a data sua publicação.

RICARDO MAGNUS OSÓRIO GALVÃO