18907714 08006.000693/2021-25

Ministério da Justiça e Segurança Pública
Secretaria-Executiva

RESOLUÇÃO CGE Nº 18, DE 5 DE AGOSTO DE 2022

O COMITÊ DE GOVERNANÇA ESTRATÉGICA DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso das atribuições que lhe são conferidas pelo art. 1º e pelo Parágrafo único do art. 2º, do Anexo I, da Portaria MJSP nº 2, de 28 de janeiro de 2022, e com base no Art. 53, do Anexo XIII, da mesma Portaria,

RESOLVE:

Art. 1º Aprovar, na forma do anexo a esta Resolução, a Norma de Segurança da Informação e Comunicação para o Teletrabalho, Trabalho Remoto e Acessos Externos no âmbito do Ministério da Justiça e Segurança Pública.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

ANTONIO RAMIREZ LORENZO
SECRETÁRIO-EXECUTIVO

Documento assinado eletronicamente por **ANTONIO RAMIREZ LORENZO**, **Secretário(a)-Executivo(a) do Ministério da Justiça e Segurança Pública**, em 08/08/2022, às 15:10, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **18907714** e o código CRC **A2B6D295**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

ANEXO
NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO PARA O TELETRABALHO, TRABALHO REMOTO E ACESSOS EXTERNOS.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A norma de segurança da informação e comunicação para o teletrabalho, trabalho remoto e acessos externos do Ministério da Justiça e Segurança Pública, complementa a Política de

Segurança da Informação e Comunicação, com a finalidade de definir os requisitos de segurança de teletrabalho, acesso remoto e utilização de dispositivos próprios, com regras para o controle de acesso externo às aplicações, aos serviços de rede e aos sistemas e recursos de tecnologia da informação do Ministério.

Art. 2º Esta norma é aplicável a todos os atores abrangidos pela Política de Segurança da Informação e Comunicação – POSIC do Ministério que façam utilização da sua rede computacional.

Art. 3º As disposições apresentadas nesta norma adotam como terminologia o Glossário de Segurança da Informação do Gabinete de Segurança Institucional - GSI, considerando-se ainda as seguintes definições:

I - teletrabalho: modalidade de trabalho em que o cumprimento da jornada regular pelo participante pode ser realizado fora das dependências físicas do órgão, em regime de execução parcial ou integral, de forma remota e com a utilização de recursos tecnológicos, para a execução de atividades que sejam passíveis de controle e que possuam metas, prazos e entregas previamente definidos e, ainda, que não configurem trabalho externo, dispensado do controle de frequência, nos termos da legislação vigente;

II - trabalho remoto: execução remota das atividades por meio de acesso externo, em caráter excepcional, sem pactuação prévia de atividades, metas, sendo a autorização conferida somente pela chefia imediata; e

III - acesso externo ou acesso remoto: acesso aos recursos de tecnologia da informação e comunicação do Ministério da Justiça e Segurança Pública realizado por meio de equipamentos privados ou de propriedade do órgão que não estejam fisicamente conectados à rede corporativa, podendo se dar no âmbito do teletrabalho, do trabalho remoto ou em qualquer outra circunstância em que o usuário dos serviços de tecnologia da informação e comunicação precise atuar fora das dependências físicas do órgão.

CAPÍTULO II
DAS CONDIÇÕES DE ACESSO

Art. 4º O acesso externo será condicionado ao preenchimento e assinatura de Termo de Ciência e Responsabilidade pelo usuário.

I - dever de manter a infraestrutura necessária para o exercício de suas atribuições, inclusive aquelas relacionadas à segurança da informação;

II - declaração de que está ciente quanto às atribuições e responsabilidades do participante descritas nesta norma e outras obrigações relacionadas à segurança da informação e comunicação no teletrabalho, no trabalho remoto e nos acessos externos;

III - declaração de que não disponibilizará senhas ou acessos a pessoas estranhas ao Ministério da Justiça e Segurança Pública;

IV - vedação à utilização, por terceiros, dos equipamentos de tecnologia da informação e comunicação (TIC) fornecidos pelo Ministério;

V - dever de observar as disposições constantes da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Lei Geral de Acesso à Informação (LAI), no que couber;

VI - obrigação de preservar o sigilo dos dados acessados de forma remota, bem como de manter atualizados os sistemas instalados nos equipamentos de trabalho;

VII - aceitação das regras de conformidade estabelecidas pela área de tecnologia da informação que deverão ser aplicadas aos equipamentos utilizados para se conectar à infraestrutura de rede do Ministério da Justiça e Segurança Pública;

VIII - necessidade de conceder permissão à área de tecnologia da informação e comunicação para instalar ou habilitar agentes de software e outros recursos para monitoramento e

análise remota de segurança da informação e comunicação no equipamento utilizado para se conectar à infraestrutura de rede, respeitado o direito à privacidade;

IX - concordância com a revogação dos acessos e a destruição dos dados de equipamento disponibilizado para o acesso remoto após sua devolução; e

X - obrigação de remover todos os dados, sistemas, softwares, acessos e pastas ou unidades criptografadas armazenados em equipamentos não pertencentes ao Ministério após a descontinuidade do regime de teletrabalho, trabalho remoto, programa de aprendizagem ou ato educativo supervisionado.

Parágrafo único. Caberá à área de tecnologia da informação e comunicação do Ministério a disponibilização de formulário eletrônico unificado contemplando o Termo de Ciência e Reponsabilidade de que trata o caput deste artigo, que deverá ser assinado por todos os usuários e em prazo a ser definido em regramento específico, a ser editado pelo Secretário-Executivo do Ministério da Justiça e Segurança Pública, sob pena de bloqueio dos acessos.

CAPÍTULO III
DO CONTROLE DE ACESSO

Art. 5º Para os acessos externos, o usuário deverá receber o conjunto mais restritivo possível de permissões.

Art. 6º A área de tecnologia da informação e comunicação avaliará a conformidade do equipamento utilizado para acesso remoto com os padrões de segurança da informação e comunicação necessários para uso corporativo e realizará varreduras e análises com o objetivo de identificar riscos de segurança da informação e comunicação que prejudiquem ou possam prejudicar a infraestrutura de tecnologia da informação e comunicação do Ministério da Justiça e Segurança Pública, realizando o bloqueio do acesso remoto caso identifique alguma não conformidade ou risco de segurança.

§ 1º As varreduras e análises de segurança realizadas deverão ser auditáveis e não poderão coletar informações de cunho pessoal.

§ 2º Em caso de impossibilidade de realização das varreduras e análises de segurança, o acesso remoto será bloqueado até a efetiva verificação, mediante comunicação prévia de quarenta e oito horas.

§ 3º O bloqueio do acesso remoto poderá se dar de forma imediata, por ato fundamentado do responsável pela área de tecnologia da informação e comunicação, prescindindo de comunicação prévia.

Art. 7º O uso e instalação de aplicativos nos equipamentos utilizados para acesso remoto serão previstos em regulamentação específica a ser elaborada e editada pelo responsável pela área de tecnologia da informação e comunicação.

Art. 8º Para os acessos remotos, é obrigatória a utilização de múltiplo fator de autenticação ou outro recurso que ofereça, no mínimo, o mesmo nível de segurança.

Parágrafo único. A Diretoria de Tecnologia da Informação e Comunicação disponibilizará os recursos necessários à segurança nos acessos remotos à infraestrutura de tecnologia da informação e comunicação do Ministério da Justiça e Segurança Pública.

CAPÍTULO IV
DO USO DE EQUIPAMENTOS PESSOAIS

Art. 9º. O licenciamento do sistema operacional e demais programas instalados no equipamento particular é de inteira responsabilidade do usuário, excetuando-se aqueles de uso corporativo que sejam licenciados por usuário, e cujo modelo de licenciamento possibilite o uso em equipamentos pessoais.

Parágrafo único. Poderão, ser fornecidas conforme disponibilidade técnica, as ferramentas corporativas de segurança da informação e comunicação, tal como antivírus ou equivalente para uso em equipamentos pessoais durante sua utilização para acessos remotos.

Art. 10. Nos casos em que a necessidade de acesso remoto decorrer de imposição da administração ou de motivo de saúde, deverá ser disponibilizado equipamento corporativo quando o usuário manifestar discordância em submeter seu equipamento pessoal aos procedimentos descritos nesta norma.

Art. 11. Para o acesso remoto, o usuário deverá providenciar dispositivo capaz de funcionar como autenticador de Múltiplo Fator de Autenticação (MFA) compatível com a tecnologia definida pela área de tecnologia da informação e comunicação, conforme regulamentação específica.

CAPÍTULO V
DAS BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 12. O usuário detentor de processos e documentos obtidos por meio de acesso remoto deverá guardar sigilo a respeito das informações neles contidas, sob pena de responsabilidade, nos termos da legislação em vigor.

Art. 13. Os equipamentos utilizados para acesso remoto devem ser protegidos adequadamente e ter sua segurança mantida regularmente.

Art. 14. São deveres do usuário dos recursos de tecnologia da informação e comunicação do Ministério da Justiça e Segurança Pública, nos termos desta norma:

I - utilizar equipamentos com as últimas atualizações e correções de segurança instaladas;

II - utilizar somente sistema operacional e programas homologados;

III - manter programa antivírus atualizado;

IV -manter o firewall do sistema operacional ativo e corretamente configurado; e

V - providenciar a imediata alteração de sua senha em caso de perda, roubo, descarte ou manutenção do equipamento utilizado para acesso remoto.

CAPÍTULO VI
DO CONTROLE, MONITORAMENTO E AUDITORIA DE RECURSOS TECNOLÓGICOS

Art. 15. Os equipamentos de terceiros ou corporativos utilizados para o trabalho remoto devem atender aos requisitos de conformidade especificados pela área de tecnologia da informação e comunicação, e não poderão remover ou bloquear o funcionamento de mecanismos de segurança que tenham sido instalados.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 16. A Diretoria de Tecnologia da Informação e Comunicação poderá expedir procedimentos operacionais, plano de ação e demais ações necessárias para atendimento desta norma.

Art. 17. Aos acessos remotos aplicam-se as demais normas de segurança da informação e comunicação referentes às atividades desenvolvidas nas dependências do órgão.

Art. 18. Dúvidas, casos omissos, ou situações excepcionais em relação a esta norma serão dirimidos pela Diretoria de Tecnologia da Informação e Comunicação.