MINISTÉRIO DAS COMUNICAÇÕES
Secretaria-Executiva do Ministério das Comunicações
Subsecretaria de Tecnologia da Informação

RESOLUÇÃO MCOM Nº 51, 28 DE OUTUBRO DE 2026

Aprova a Norma Complementar para o Uso Seguro dos Serviços de Impressão, Cópia e Digitalização.

O SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO, instituído pela Portaria nº 20.054, de 10 de outubro de 2025, representado pelo Gestor de Segurança da Informação, designado por meio da Portaria MCOM nº 308, de 13 de agosto de 2024, no uso das atribuições que lhe confere o art. 17 da Resolução nº 26/2024/MCOM, resolve:

Art. 1º Aprovar a Norma Complementar para o Uso Seguro dos Serviços de Impressão, Cópia e Digitalização, na forma do Anexo I desta Resolução.

Art. 2º Fica revogada a Portaria MCOM nº 5056, de 24 de março de 2022.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

GUSTAVO HENRIQUE DE SOUTO SILVA
Gestor de Segurança da Informação
Presidente do Subcomitê de Segurança da Informação

NORMA COMPLEMENTAR PARA O USO SEGURO DOS SERVIÇOS DE IMPRESSÃO, CÓPIA E DIGITALIZAÇÃO

1. DO OBJETIVO

Art. 1º Esta Norma Complementar estabelece diretrizes, responsabilidades e requisitos para a utilização segura dos serviços de impressão, cópia e digitalização no âmbito do Ministério das Comunicações - MCOM, visando à proteção das informações institucionais durante seu processamento, armazenamento temporário, reprodução, digitalização, manuseio e descarte.

Parágrafo único. Esta Norma tem por finalidade:

I - proteger a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações processadas pelos serviços de impressão, cópia e digitalização;

II - disciplinar a utilização segura dos equipamentos e serviços;

III - reduzir os riscos relacionados ao tratamento físico e digital de documentos;

IV - estabelecer responsabilidades dos usuários e das unidades envolvidas;

V - assegurar a adequada proteção das informações durante todo o ciclo de utilização dos serviços;

VI - promover o uso racional, econômico e sustentável dos recursos disponibilizados; e

VII - estabelecer requisitos mínimos de segurança, sem prejuízo dos procedimentos operacionais e dos controles técnicos aplicáveis.

2. DA ABRANGÊNCIA

Art. 2º Esta Norma aplica-se:

I - aos servidores;

II - aos empregados públicos;

III - aos militares em exercício;

IV - aos estagiários;

V - aos colaboradores;

VI - aos prestadores de serviço;

VII - aos terceiros autorizados; e

VIII - a qualquer usuário autorizado dos equipamentos ou serviços de impressão, cópia ou digitalização no âmbito do MCOM.

3. DAS REFERÊNCIAS NORMATIVAS

Art. 3º Esta Norma observa, entre outros:

I - a Política de Segurança da Informação do MCOM;

II - a Política de Governança do MCOM;

III - a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;

IV - a Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação - LAI;

V - o Decreto nº 12.002, de 22 de abril de 2024;

VI - a Norma Complementar para o Controle de Acesso Lógico;

VII - a Norma Complementar para o Inventário e o Mapeamento de Ativos;

VIII - a Norma Complementar para a Gestão de Riscos de Segurança da Informação;

IX - a Norma Complementar para o Gerenciamento de Vulnerabilidades;

X - a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação; e

XI - os demais normativos institucionais e a legislação aplicável.

4. DOS CONCEITOS E DAS DEFINIÇÕES

Art. 4º Para fins desta Norma, considera-se:

I - Impressão Segura: modalidade de impressão em que o trabalho permanece retido e somente é liberado após autenticação do usuário autorizado ou utilização de controle de segurança equivalente;

II - Impressão Retida: mecanismo que impede a impressão imediata do documento, mantendo o trabalho temporariamente em fila até sua liberação pelo usuário autorizado;

III - Digitalização: processo de conversão de documento ou informação originalmente em meio físico para formato digital;

IV - Documento Institucional: documento produzido, recebido, armazenado ou utilizado no exercício das atividades institucionais do MCOM, independentemente do suporte em que se encontre;

V - Informação Protegida: informação sujeita a restrição de acesso, sigilo, proteção de dados pessoais ou outro requisito específico de proteção previsto em legislação, regulamentação ou norma institucional;

VI - Multifuncional: equipamento que reúne duas ou mais funcionalidades, tais como impressão, cópia e digitalização;

VII - Fila de Impressão: ambiente lógico no qual os trabalhos de impressão permanecem temporariamente armazenados até seu processamento, cancelamento ou liberação;

VIII - Liberação Segura: procedimento pelo qual o trabalho de impressão somente é executado após ação intencional do usuário autorizado, mediante autenticação ou controle equivalente;

IX - Documento Digitalizado: documento ou representação documental resultante do processo de digitalização; e

X - Registro Operacional: registro gerado pelos sistemas ou equipamentos necessário à administração, segurança, rastreabilidade e acompanhamento dos serviços.

Parágrafo único. Aplicam-se subsidiariamente os conceitos constantes da Política de Segurança da Informação e dos demais normativos institucionais pertinentes.

5. DAS DIRETRIZES GERAIS

Art. 5º A utilização e a administração dos serviços de impressão, cópia e digitalização deverão observar:

I - a proteção da informação;

II - a necessidade de conhecer;

III - o privilégio mínimo;

IV - a rastreabilidade;

V - a disponibilidade;

VI - a economicidade e a sustentabilidade;

VII - a responsabilização do usuário;

VIII - a prevenção da exposição ou divulgação indevida de informações; e

IX - a melhoria contínua dos controles de Segurança da Informação.

Art. 6º Os equipamentos e serviços de impressão, cópia e digitalização destinam-se exclusivamente às atividades institucionais.

6. DA UTILIZAÇÃO DOS SERVIÇOS

Art. 7º Os usuários deverão:

I - conferir previamente o documento e as configurações selecionadas antes da impressão, cópia ou digitalização;

II - assegurar que os documentos impressos ou copiados sejam retirados imediatamente do equipamento após sua liberação;

III - verificar se não permaneceram documentos originais, cópias ou informações no equipamento após sua utilização;

IV - utilizar os serviços exclusivamente por meio dos recursos, equipamentos e mecanismos autorizados pelo MCOM; e

V - adotar os cuidados necessários para impedir o acesso de pessoas não autorizadas às informações processadas.

Art. 8º Na impressão de documentos que contenham informações protegidas, deverão ser utilizados mecanismos de Impressão Segura, Impressão Retida ou outro controle de segurança

equivalente.

§ 1º Quando o recurso de segurança previsto no caput não estiver tecnicamente disponível, deverão ser adotadas medidas compensatórias destinadas a impedir o acesso não autorizado ao documento.

§ 2º As medidas compensatórias e as situações em que deverão ser utilizadas serão disciplinadas em procedimento operacional específico.

§ 3º Quando o risco associado à informação não puder ser adequadamente mitigado por medida compensatória, a impressão deverá ser realizada em equipamento ou ambiente que disponha do controle de segurança necessário.

Art. 9º O usuário permanecerá responsável pelos documentos submetidos aos serviços até sua retirada do equipamento e adoção das medidas necessárias à sua proteção.

Art. 10. É vedado abandonar documentos institucionais ou originais nas bandejas, alimentadores, áreas de saída ou proximidades dos equipamentos.

Parágrafo único. Documento institucional encontrado sem supervisão deverá ser protegido contra acesso indevido e encaminhado ao usuário responsável ou à unidade competente, conforme procedimento institucional.

7. DA DIGITALIZAÇÃO

Art. 11. A digitalização de documentos deverá preservar, conforme aplicável:

I - a autenticidade;

II - a integridade;

III - a legibilidade;

IV - a rastreabilidade; e

V - a adequada proteção da informação.

Art. 12. Antes do envio ou compartilhamento de documento digitalizado, o usuário deverá:

I - conferir o conteúdo digitalizado;

II - verificar os destinatários;

III - confirmar se os destinatários estão autorizados a acessar a informação;

IV - utilizar exclusivamente destinos, sistemas, contas e serviços autorizados pelo MCOM; e

V - observar as restrições de acesso e proteção aplicáveis ao documento.

Art. 13. A digitalização de documentos que contenham informações protegidas deverá observar a Política de Segurança da Informação, as normas de proteção de dados pessoais e os demais normativos aplicáveis.

Parágrafo único. É vedado encaminhar documentos institucionais digitalizados para contas pessoais, serviços externos não autorizados ou outros destinos incompatíveis com os requisitos de proteção da informação.

8. DA PROTEÇÃO DAS INFORMAÇÕES

Art. 14. Os documentos impressos, copiados ou digitalizados deverão ser protegidos durante todo o seu ciclo de utilização, desde o processamento até sua guarda, encaminhamento, arquivamento ou descarte.

Art. 15. É vedado:

I - deixar documentos que contenham informações protegidas sobre mesas, impressoras, multifuncionais ou outros locais acessíveis a pessoas não autorizadas;

II - descartar documentos institucionais em recipientes ou locais incompatíveis com os requisitos de proteção aplicáveis;

III - digitalizar ou encaminhar documentos para destinatários não autorizados;

IV - compartilhar documentos institucionais sem necessidade funcional ou autorização;

V - utilizar equipamentos particulares ou serviços externos não autorizados para impressão, cópia, digitalização, armazenamento ou encaminhamento de documentos institucionais;

VI - remover documentos, mídias ou componentes que contenham informações institucionais sem autorização; e

VII - utilizar os serviços de forma a contornar controles de Segurança da Informação estabelecidos pelo MCOM.

§ 1º O descarte de documentos institucionais deverá ocorrer de forma compatível com a sensibilidade da informação, de modo a impedir sua recuperação ou acesso indevido.

§ 2º Os procedimentos e meios autorizados para descarte seguro serão definidos em procedimento operacional ou normativo específico.

Art. 16. O tratamento de documentos que contenham dados pessoais deverá observar a legislação de proteção de dados pessoais e os normativos institucionais aplicáveis.

Parágrafo único. O acesso, a impressão, a cópia, a digitalização, o compartilhamento e o descarte de documentos que contenham dados pessoais deverão limitar-se ao necessário para o atendimento da finalidade institucional.

9. DOS EQUIPAMENTOS

Art. 17. Os equipamentos serão disponibilizados conforme critérios administrativos, operacionais e de Segurança da Informação definidos pelas unidades competentes.

Art. 18. A configuração, a manutenção e a administração técnica dos equipamentos e serviços serão disciplinadas por procedimentos operacionais específicos.

§ 1º Os procedimentos deverão contemplar, conforme aplicável:

I - mecanismos de autenticação e liberação segura;

II - proteção das filas de impressão;

III - proteção das informações armazenadas temporariamente nos equipamentos;

IV - atualização e manutenção dos equipamentos;

V - restrição do acesso às funções administrativas;

VI - proteção dos registros operacionais;

VII - medidas de segurança durante manutenção realizada por terceiros; e

VIII - eliminação segura de informações antes da substituição, devolução, transferência, alienação ou descarte de equipamentos ou componentes de armazenamento.

§ 2º A retirada de equipamento ou componente que possa conter informação institucional para manutenção externa deverá observar procedimento que assegure a proteção das informações nele existentes.

§ 3º Esta Norma não disciplina parâmetros técnicos específicos de configuração, manutenção ou administração dos equipamentos, os quais serão definidos pela unidade responsável pela Tecnologia da Informação.

10. DO USO RACIONAL DOS RECURSOS

Art. 19. Os usuários deverão utilizar os recursos de impressão, cópia e digitalização observando critérios de economicidade, eficiência e sustentabilidade.

Art. 20. Sempre que compatível com a necessidade institucional, deverão ser priorizados:

I - documentos eletrônicos;

II - assinaturas digitais ou eletrônicas admitidas institucionalmente;

III - tramitação eletrônica;

IV - digitalização em substituição à reprodução física desnecessária;

V - impressão frente e verso;

VI - impressão monocromática; e

VII - redução de impressões e cópias desnecessárias.

Parágrafo único. As medidas de economicidade e sustentabilidade não poderão comprometer os requisitos de proteção e Segurança da Informação.

11. DOS REGISTROS OPERACIONAIS

Art. 21. A unidade responsável pela Tecnologia da Informação deverá manter registros operacionais compatíveis com os recursos técnicos disponíveis e necessários à administração, à segurança e à rastreabilidade dos serviços.

§ 1º Os registros deverão contemplar, conforme aplicável e tecnicamente disponível:

I - identificação do equipamento ou serviço utilizado;

II - data e horário da operação;

III - volume de impressão, cópia ou digitalização;

IV - utilização dos equipamentos;

V - consumo de recursos;

VI - disponibilidade do serviço;

VII - utilização das filas de impressão; e

VIII - identificação do usuário, quando necessária à finalidade e tecnicamente disponível.

§ 2º Os registros deverão limitar-se às informações necessárias às finalidades previstas nesta Norma, evitando-se, sempre que possível, o armazenamento do conteúdo dos documentos processados.

§ 3º O acesso aos registros será restrito às pessoas autorizadas, observadas as competências institucionais e a finalidade de sua utilização.

§ 4º Os critérios de retenção, proteção, acesso e descarte dos registros serão definidos em procedimento operacional ou normativo específico.

Art. 22. Os registros operacionais destinam-se à gestão, à segurança e à rastreabilidade dos serviços e não substituem os registros, auditorias ou procedimentos de apuração previstos em normas específicas.

Parágrafo único. Quando necessários à apuração de incidente ou ocorrência, os registros deverão ser preservados e tratados de acordo com os normativos aplicáveis.

12. DAS RESPONSABILIDADES

Do Gestor de Segurança da Informação

Art. 23. Compete ao Gestor de Segurança da Informação:

I - orientar quanto às diretrizes de Segurança da Informação aplicáveis aos serviços;

II - propor a atualização desta Norma;

III - promover a integração desta Norma com os demais normativos de Segurança da Informação;

IV - orientar quanto aos aspectos de Segurança da Informação relacionados aos riscos decorrentes do uso dos serviços; e

V - encaminhar matérias estratégicas ao SINF e ao CGSP, conforme suas competências.

Da unidade responsável pela Tecnologia da Informação

Art. 24. Compete à unidade responsável pela Tecnologia da Informação:

I - administrar tecnicamente os serviços;

II - disponibilizar e manter os equipamentos sob sua responsabilidade;

III - implementar e manter os controles técnicos de Segurança da Informação aplicáveis;

IV - prestar suporte aos usuários;

V - manter a disponibilidade dos serviços, observados os requisitos institucionais;

VI - manter os registros operacionais previstos nesta Norma;

VII - proteger as informações temporariamente armazenadas nos equipamentos e sistemas sob sua administração;

VIII - estabelecer controles para manutenção, substituição, devolução e descarte de equipamentos;

IX - acompanhar, no âmbito de suas atribuições, o acesso técnico de fornecedores e prestadores de serviço; e

X - elaborar e manter atualizados os procedimentos operacionais necessários à execução desta Norma.

Dos gestores das unidades

Art. 25. Compete aos gestores das unidades:

I - orientar os usuários sob sua responsabilidade quanto ao cumprimento desta Norma;

II - comunicar à unidade responsável pela Tecnologia da Informação necessidades específicas relacionadas aos serviços;

III - incentivar o uso racional dos recursos;

IV - comunicar situações que possam representar risco à proteção das informações; e

V - observar e fazer observar as restrições de acesso aplicáveis às informações de sua unidade.

Dos usuários

Art. 26. Compete aos usuários:

I - utilizar corretamente os equipamentos e serviços;

II - preservar a confidencialidade, a integridade, autenticidade e a disponibilidade das informações sob sua responsabilidade;

III - retirar imediatamente os documentos impressos ou copiados;

IV - verificar a retirada de documentos originais dos equipamentos;

V - conferir os destinatários e destinos utilizados nas digitalizações;

VI - utilizar os mecanismos de segurança disponibilizados;

VII - comunicar falhas, ocorrências ou situações que possam comprometer a Segurança da Informação; e

VIII - observar esta Norma e os demais normativos institucionais aplicáveis.

13. DA INTEGRAÇÃO COM OUTROS NORMATIVOS

Art. 27. Aplicam-se subsidiariamente aos serviços disciplinados nesta Norma:

I - a Norma Complementar para o Controle de Acesso Lógico;

II - a Norma Complementar para o Inventário e o Mapeamento de Ativos;

III - a Norma Complementar para a Gestão de Riscos de Segurança da Informação;

IV - a Norma Complementar para o Gerenciamento de Vulnerabilidades;

V - a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação;

VI - a Política de Segurança da Informação; e

VII - os demais normativos institucionais relacionados à proteção da informação e dos dados pessoais.

Parágrafo único. As normas referidas neste artigo permanecem responsáveis pelos respectivos processos e controles, não havendo transferência ou duplicidade de competências em razão desta Norma.

14. DA CONFORMIDADE

Art. 28. O descumprimento desta Norma deverá ser comunicado ao Gestor de Segurança da Informação e, conforme a natureza da ocorrência, às demais instâncias competentes para avaliação e adoção das providências cabíveis.

Parágrafo único. O descumprimento poderá sujeitar o responsável às medidas administrativas, contratuais ou legais cabíveis, observados o devido processo e a legislação aplicável.

Art. 29. As ocorrências que caracterizem ou possam caracterizar incidente de Segurança da Informação deverão ser comunicadas e tratadas conforme a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação.

15. DAS DISPOSIÇÕES FINAIS

Art. 30. Os procedimentos operacionais necessários à execução desta Norma serão elaborados e mantidos atualizados pela unidade responsável pela Tecnologia da Informação, observadas as competências das demais unidades.

Parágrafo único. Os procedimentos deverão disciplinar, quando aplicável:

I - a utilização de Impressão Segura, Impressão Retida e Liberação Segura;

II - as medidas compensatórias previstas no art. 8º;

III - os destinos autorizados para digitalização;

IV - o descarte seguro de documentos;

V - a geração, proteção, retenção e descarte de registros operacionais;

VI - a proteção das informações armazenadas temporariamente nos equipamentos;

VII - os controles aplicáveis à manutenção realizada por terceiros; e

VIII - os procedimentos de substituição, devolução, transferência, alienação e descarte de equipamentos e componentes.

Art. 31. Os casos omissos serão resolvidos pelo Gestor de Segurança da Informação, observadas as competências das unidades envolvidas, podendo ser submetidos ao Subcomitê de Segurança da Informação ou ao CGSP, conforme sua relevância.

Art. 32. Esta Norma deverá ser revisada periodicamente ou sempre que houver alteração relevante:

I - da legislação ou regulamentação aplicável;

II - da Política de Segurança da Informação;

III - da tecnologia utilizada na prestação dos serviços;

IV - dos riscos relacionados aos serviços; ou

V - da estrutura organizacional ou das competências das unidades envolvidas.

Parágrafo único. A revisão da Norma deverá considerar os incidentes, os riscos, os resultados de avaliações e as necessidades de melhoria identificados durante sua aplicação.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Tecnologia da Informação**, em 29/10/2026, às 17:22, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015 .

A autenticidade deste documento pode ser conferida no site https://sei.mcom.gov.br/sei/verifica, informando o código verificador **13600336** e o código CRC **E3183A45**.

Anexos

Não Possui.