CONSELHO NACIONAL DE TÉCNICOS EM RADIOLOGIA

RESOLUÇÃO CONTER Nº 8, DE 24 DE JULHO DE 2026

(Aprovada ad referendum da Plenária, nos termos do art. 12 e seu § 2º do Regimento Interno)

Institui a Política de Segurança da Informação - PSI no Âmbito do Conselho Nacional de Técnicos em Radiologia - CONTER e dá outras providências.

A Diretoria Executiva do CONSELHO NACIONAL DE TÉCNICOS EM RADIOLOGIA - CONTER, autarquia federal criada pela Lei nº 7.394, de 29 de outubro de 1985, regulamentada pelo Decreto nº 92.790, de 17 de junho de 1986, no uso das atribuições que lhe confere o Regimento Interno, ad referendum do Plenário;

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais ("LGPD"), em especial o Capítulo IV e os Artigos 46 a 51;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação ("PNSI") e determina aos órgãos e às entidades da administração pública federal a instituição de sua própria Política de Segurança da Informação ("PSI");

CONSIDERANDO o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética ("ENSC");

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação, a Lei nº 8.159, de 8 de janeiro de 1991, e a Lei nº 14.129, de 29 de março de 2021;

CONSIDERANDO as Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República, notadamente a IN GSI/PR nº 1, de 27 de maio de 2020, a IN GSI/PR nº 3, de 28 de maio de 2021, a IN GSI/PR nº 5, de 30 de agosto de 2021, e a IN GSI/PR nº 8, de 26 de agosto de 2020, adotadas por esta autarquia como referencial normativo de observância obrigatória; e as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 como referencial técnico;

CONSIDERANDO a necessidade de assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações custodiadas pelo CONTER, bem como a proteção dos dados pessoais de seus profissionais registrados, empregados públicos, membros honoríficos e voluntários, funcionários terceirizados, cidadãos titulares dos dados pessoais por aquele controlados e de pessoas jurídicas prestadores de serviços;

CONSIDERANDO a Portaria CONTER nº 60/2026, que empossou o atual Encarregado pelo Tratamento de Dados Pessoais ("DPO"), e a Portaria CONTER nº 61/2026, que reformulou a Comissão de Privacidade de Proteção de Dados, posteriormente denominada Comissão de Tratamento e Proteção de Dados ("CTPD") pela Portaria 0097/2026;

CONSIDERANDO a decisão da Reunião de Diretoria Executiva do CONTER, AD-REFERENDUM da Plenária, realizada no dia 23 de julho de 2026, concernente à instituição da Política de Segurança da Informação (PSI) no âmbito do CONTER; resolve:

instituir a Política de Segurança da Informação (PSI) no âmbito do CONTER.

TÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

CAPÍTULO I - DO OBJETO E DA FINALIDADE

Art. 1º Fica instituída a Política de Segurança da Informação - PSI ("Política") do Conselho Nacional de Técnicos em Radiologia - CONTER ("Autarquia", "Conselho" ou "Controlador"), com o objetivo de estabelecer princípios, diretrizes, responsabilidades e estrutura de governança destinados à proteção das informações e dos ativos de informação sob custódia da autarquia.

Art. 2º São finalidades da PSI:

I) assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações institucionais, independentemente do meio ou suporte em que se encontrem;

II) proteger os dados pessoais tratados pelo CONTER, em conformidade com a Lei nº 13.709/2018;

III) garantir a continuidade das atividades finalísticas e administrativas da Autarquia;

IV) assegurar a conformidade com o ordenamento jurídico aplicável e com as determinações dos órgãos de controle;

V) promover a cultura de segurança da informação entre todos os que se relacionam com a Autarquia;

VI) subsidiar a tomada de decisão institucional mediante gestão estruturada de riscos de segurança da informação.

CAPÍTULO II - DA ABRANGÊNCIA

Art. 3º A PSI se aplica, no que couber e observadas as respectivas vinculações jurídicas, a:

I) conselheiros federais efetivos e suplentes;

II) empregados públicos do quadro do CONTER, ativos, cedidos ou em exercício provisório;

III) ocupantes de cargos e funções de confiança;

IV) estagiários e aprendizes;

V) fiscais e demais agentes investidos em atribuição fiscalizatória;

VI) conselheiros e empregados de Conselhos Regionais de Técnicos em Radiologia - CRTRs, quando acessarem sistemas, bases de dados ou informações sob custódia do CONTER;

VII) membros das comissões permanentes e transitórias do CONTER;

VIII) prestadores de serviços, empresas contratadas, consultores, e seus prepostos e empregados, quando do acesso a informações ou ativos do CONTER;

IX) quaisquer outras pessoas, físicas ou jurídicas, que, a qualquer título, acessem informações ou ativos de informação da autarquia.

Parágrafo único. A vinculação às disposições desta Política será formalizada mediante assinatura do Termo de Ciência e Responsabilidade constante do Anexo III, no caso dos incisos I a VII, e mediante cláusula contratual específica, no caso dos incisos VII e VIII.

Art. 4º Esta Política abrange todas as informações produzidas, recebidas, armazenadas, transmitidas ou descartadas pelo CONTER, em qualquer suporte, formato ou meio, inclusive as processadas por terceiros em nome da autarquia.

CAPÍTULO III - DAS DEFINIÇÕES

Art. 5º Para os efeitos desta Política, adotam-se as definições constantes do Art. 5º da LGPD, da norma ABNT NBR ISO/IEC 27000 e, complementarmente, as seguintes:

I) ativo de informação: qualquer elemento que produza, processe, transmita, armazene ou descarte informação, incluindo sistemas, equipamentos, mídias, instalações, documentos e pessoas;

II) custodiante da informação: unidade ou agente responsável pela guarda e pela aplicação dos controles de proteção definidos pelo gestor da informação;

III) gestor da informação: titular da unidade organizacional responsável pela informação, a quem compete classificá-la e definir seus requisitos de proteção;

IV) usuário: toda pessoa abrangida pelo Art. 3º desta Política;

V) incidente de segurança da informação: evento ou série de eventos, desejados ou não, que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação;

VI) recursos corporativos: equipamentos, sistemas, redes, contas, licenças e demais meios disponibilizados pelo CONTER para o exercício das atividades institucionais;

VII) norma complementar: ato normativo derivado desta Política, destinado a detalhar tecnicamente eixo específico de segurança da informação.

TÍTULO II

DOS PRINCÍPIOS E DAS DIRETRIZES GERAIS

CAPÍTULO I - DOS PRINCÍPIOS

Art. 6º A segurança da informação no CONTER rege-se pelos seguintes princípios:

I) confidencialidade: a informação deve ser acessível apenas a quem esteja autorizado;

II) integridade: a informação deve ser mantida exata e completa, preservando-se seus atributos originais;

III) disponibilidade: a informação deve estar acessível quando necessária aos agentes autorizados;

IV) autenticidade: deve ser assegurada a fidedignidade da origem e da autoria da informação;

V) legalidade: o tratamento da informação deve observar o ordenamento jurídico vigente;

VI) necessidade e menor privilégio: o acesso à informação deve limitar-se ao mínimo necessário ao desempenho das atribuições do agente;

VII) transparência ativa: as informações de interesse público serão disponibilizadas nos termos da Lei nº 12.527/2011, ressalvadas as hipóteses legais de sigilo;

VIII) responsabilização e prestação de contas: o CONTER deve ser capaz de demonstrar, mediante evidência documental, a adoção de medidas eficazes de segurança da informação e de proteção de dados pessoais, nos termos do Art. 6º, Inciso X, da LGPD;

IX) melhoria contínua: os controles de segurança devem ser periodicamente avaliados e aprimorados;

X) proporcionalidade: os controles adotados devem ser proporcionais ao risco e ao valor da informação protegida.

CAPÍTULO II - DAS DIRETRIZES GERAIS

Art. 7º A informação produzida, custodiada ou processada pelo CONTER constitui ativo institucional, sendo vedado seu uso para finalidade estranha ao interesse público e às atribuições legais da autarquia.

Art. 8º Os recursos corporativos são disponibilizados para fins institucionais, admitido o uso pessoal eventual, desde que não comprometa a segurança da informação, o desempenho dos recursos ou a produtividade, e não configure ilícito.

§ 1º O CONTER poderá monitorar o uso dos recursos corporativos para fins de segurança da informação, auditoria e apuração de irregularidades.

§ 2º O monitoramento previsto no § 1º observará os princípios da legalidade, da finalidade, da necessidade, da proporcionalidade e da prévia cientificação dos usuários, e terá suas hipóteses, seus limites e seu procedimento disciplinados em norma complementar, vedado o acesso ao conteúdo de comunicações de natureza estritamente pessoal fora das hipóteses e do procedimento ali previstos.

Art. 9º Toda informação sob custódia do CONTER será classificada quanto ao grau de sigilo e à criticidade, na forma de norma complementar, observadas a Lei nº 12.527/2011 e a Lei nº 13.709/2018.

Art. 10. A segurança da informação será considerada desde a concepção de processos, sistemas, contratações e projetos, e ao longo de todo o seu ciclo de vida.

Art. 11. Nenhum usuário poderá alegar desconhecimento desta Política ou de suas normas complementares como justificativa para seu descumprimento.

TÍTULO III

DA ESTRUTURA DE GOVERNANÇA

CAPÍTULO I - DA COMPOSIÇÃO DA ESTRUTURA

Art. 12. A estrutura de governança de segurança da informação do CONTER é composta por:

I) a Plenária;

II) a Diretoria Executiva;

III) a Presidência;

IV) a Comissão de Tratamento e Proteção de Dados - CTPD;

V) o Encarregado pelo Tratamento de Dados Pessoais ("DPO");

VI) o Gestor de Segurança da Informação - GSI;

VII) a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

VIII) os gestores e custodiantes da informação;

IX) os usuários.

CAPÍTULO II - DO PLENÁRIO, DA DIRETORIA EXECUTIVA E DA PRESIDÊNCIA

Art. 13. Compete à Plenária aprovar e revisar esta Política, apreciar o relatório anual de segurança da informação e deliberar sobre matérias de segurança da informação que lhe sejam submetidas.

Art. 14. Compete à Presidência, ouvida a Diretoria Executiva:

I) designar os integrantes da Comissão de Tratamento e Proteção de Dados Pessoais, o Encarregado e o Gestor de Segurança da Informação indicado pelo Encarregado;

II) assegurar os recursos orçamentários, humanos e tecnológicos necessários à implementação desta Política;

III) editar as normas complementares derivadas desta Política, mediante proposta da CTPD;

IV) determinar a apuração de descumprimentos, na forma do Título VII.

CAPÍTULO III - DA COMISSÃO DE TRATAMENTO E PROTEÇÃO DE DADOS - CTPD

Art. 15. Fica instituída Comissão de Tratamento e Proteção de Dados Pessoais, órgão colegiado de caráter permanente, deliberativo e consultivo, com a seguinte composição:

I) o Encarregado pelo Tratamento de Dados Pessoais, que a presidirá, sendo preferencialmente um representante da unidade Jurídica;

II) o Gestor de Segurança da Informação, da unidade de Tecnologia da Informação;

III) um representante da unidade de Protocolo;

IV) um representante da unidade de Compras, Licitações e Contratos;

V) um representante da unidade de Arquivo;

VI) um representante da unidade de Gestão de Pessoas;

VII) um representante da unidade Administrativa.

§ 1º Os integrantes e respectivos suplentes serão designados por Portaria da Presidência, com mandato de 2 (dois) anos, permitida a recondução.

§ 2º A participação na CTPD é considerada serviço relevante e enseja remuneração adicional conforme as normas do CONTER.

§ 3º A CTPD reunir-se-á ordinariamente a cada 3 (três) meses e, extraordinariamente, sempre que convocado por sua coordenação ou pela Diretoria Executiva do Conselho.

§ 4º As reuniões da CTPD serão registradas em ata, que constituirá evidência de governança para fins de auditoria.

Art. 16. Compete à Comissão de Tratamento e Proteção de Dados Pessoais:

I) propor à Presidência as normas complementares desta Política e suas revisões;

II) propor ao Plenário a revisão desta Política;

III) deliberar sobre exceções às normas de segurança da informação, mediante análise de risco documentada;

IV) acompanhar a implementação do plano de tratamento de riscos de segurança da informação;

V) analisar os relatórios de incidentes de segurança e determinar medidas corretivas;

VI) aprovar o plano anual de conscientização e capacitação;

VII) elaborar o relatório anual de segurança da informação, a ser submetido ao Plenário;

VIII) deliberar sobre casos omissos desta Política.