CAPÍTULO IV - DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 17. O Gestor de Segurança da Informação - GSI será indicado pelo Encarregado e nomeado pela Presidência do CONTER, dentre os empregados públicos da Autarquia e será o responsável pela coordenação da execução desta Política no que tange à segurança da informação.

Art. 18. Compete ao GSI:

I) coordenar o processo de gestão de riscos de segurança da informação;

II) coordenar a ETIR;

III) propor e acompanhar indicadores de segurança da informação;

IV) promover as ações de conscientização e capacitação;

V) manter atualizado o inventário de ativos de informação;

VI) reportar à Presidência e à CTPD as ocorrências relevantes de segurança da informação.

CAPÍTULO V - DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS ("DPO")

Art. 19. O Encarregado pelo Tratamento de Dados Pessoais ("DPO") será designado por ato da Presidência, com publicidade de sua identidade e de seus contatos no sítio eletrônico institucional, nos termos do art. 41, § 1º, da Lei nº 13.709/2018.

Art. 20. Compete ao Encarregado, nos termos do art. 41, § 2º, da Lei nº 13.709, de 2018:

I) receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II) receber comunicações da Autoridade Nacional de Proteção de Dados - ANPD e adotar providências;

III) orientar os agentes e os empregados do CONTER a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

V) supervisionar a elaboração e a manutenção do registro das operações de tratamento de dados pessoais de que trata o art. 37 da Lei nº 13.709/2018;

VI) orientar a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais - RIPD;

VII) atuar como ponto focal do CONTER perante a ANPD;

VIII) supervisionar as atividades do Gestor de Segurança da Informação;

IX) coordenar as atividades da CTPD.

Art. 21. Ao Encarregado são assegurados:

I) autonomia técnica no exercício de suas atribuições, vedada ingerência sobre suas manifestações técnicas;

II) acesso irrestrito às informações, aos dados, sistemas e às unidades da autarquia necessários ao exercício de suas competências;

III) canal de reporte direto à Presidência e à Plenária;

IV) recursos materiais e de pessoal para o desempenho das suas atividades no âmbito da CTPD, bem como para capacitação compatível com a sua função;

V) recursos materiais e de pessoal para capacitação dos membros da CTPD e dos CONTER.

§ 1º A função de Encarregado não poderá ser acumulada com a de responsável pela unidade de Tecnologia da Informação, nem com atribuições que configurem conflito de interesses com o exercício das competências previstas no art. 20.

§ 2º O Encarregado não poderá ser responsabilizado por manifestação técnica emitida no regular exercício de suas atribuições.

CAPÍTULO VI - DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES

Art. 22. Fica instituída a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, com atribuições de prevenção, detecção, análise, contenção, erradicação, recuperação e registro de incidentes de segurança da informação.

§ 1º A ETIR será coordenada pelo GSI e composta por, no mínimo, 2 (dois) integrantes indicados pelo Encarregado e aprovados por Portaria da Presidência, admitida a acumulação com outras atribuições.

§ 2º A ETIR atuará em articulação com o Encarregado sempre que o incidente envolver dados pessoais.

§ 3º O CONTER poderá firmar instrumento de cooperação com equipe de resposta a incidentes de outro órgão ou entidade, ou contratar serviço especializado, para suprir capacidade técnica da ETIR.

CAPÍTULO VII - DOS GESTORES, CUSTODIANTES E USUÁRIOS

Art. 23. Compete aos gestores da informação classificar as informações sob sua responsabilidade, definir os perfis de acesso e revisá-los periodicamente.

Art. 24. Compete aos custodiantes aplicar os controles de proteção definidos pelo gestor da informação e comunicar imediatamente qualquer suspeita de incidente.

Art. 25. Compete aos usuários:

I) utilizar as informações e os recursos corporativos exclusivamente para fins institucionais, ressalvado o disposto no art. 8º;

II) proteger suas credenciais de acesso, vedado o compartilhamento;

III) comunicar imediatamente ao GSI qualquer incidente ou suspeita de incidente de segurança da informação;

IV) manter sigilo sobre as informações classificadas a que tiver acesso, inclusive após o encerramento do vínculo;

V) participar das ações de conscientização e capacitação;

VI) devolver, ao término do vínculo, todos os ativos de informação sob sua posse.

TÍTULO IV

DAS DIRETRIZES ESPECÍFICAS E DAS NORMAS COMPLEMENTARES

Art. 26. As diretrizes específicas de segurança da informação serão detalhadas nas seguintes normas complementares:

I) NC-01 - Classificação e Tratamento da Informação: critérios de classificação quanto ao sigilo e à criticidade, rotulagem, regras de manuseio, transporte, armazenamento e descarte seguro;

II) NC-02 - Gestão de Ativos de Informação: identificação, inventário, atribuição de responsabilidade e ciclo de vida dos ativos;

III) NC-03 - Controle de Acesso e Gestão de Identidades: concessão, alteração, revisão periódica e revogação de acessos, política de senhas, autenticação multifator e gestão de contas privilegiadas;

IV) NC-04 - Gestão de Incidentes de Segurança da Informação: classificação, registro, escalonamento, tratamento, comunicação e lições aprendidas, incluindo o procedimento de comunicação à ANPD e aos titulares nos termos do art. 48 da Lei nº 13.709, de 2018, e da regulamentação da autoridade;

V) NC-05 - Uso Aceitável de Recursos Corporativos: regras de uso de estações de trabalho, dispositivos móveis, correio eletrônico, internet, mídias sociais e trabalho remoto, bem como as hipóteses, os limites e o procedimento de monitoramento de que trata o art. 8º;

VI) NC-06 - Cópias de Segurança, Continuidade e Recuperação: política de backup, testes de restauração, plano de continuidade de negócios e plano de recuperação de desastres;

VII) NC-07 - Segurança da Informação em Contratações e Relações com Terceiros: requisitos de segurança em editais e contratos, cláusulas de confidencialidade, cláusulas de proteção de dados pessoais, avaliação e monitoramento de fornecedores;

VIII) NC-08 - Segurança em Computação em Nuvem: requisitos mínimos aplicáveis à contratação e ao uso de soluções em nuvem, observada a IN GSI/PR nº 3, de 2021;

IX) NC-09 - Segurança Física e do Ambiente: controle de acesso a instalações, proteção de áreas críticas e segurança de equipamentos;

X) NC-10 - Desenvolvimento Seguro e Gestão de Mudanças: requisitos de segurança no desenvolvimento e na manutenção de sistemas e no controle de mudanças;

XI) NC-11 - Conscientização e Capacitação em Segurança da Informação: programa anual, público-alvo, conteúdo mínimo, periodicidade e registro de participação.

§ 1º As normas complementares serão editadas por Portaria da Presidência, mediante proposta da CTPD.

§ 2º A CTPD poderá propor a edição de normas complementares não previstas neste artigo.

TÍTULO V

DA PROTEÇÃO DE DADOS PESSOAIS

Art. 27. O tratamento de dados pessoais no âmbito do CONTER observará os princípios do art. 6º da Lei nº 13.709/2018, e as hipóteses legais de tratamento dos arts. 7º, 11 e 23 da mesma Lei, em especial a execução de políticas públicas e o cumprimento de obrigação legal ou regulatória inerentes às competências da autarquia.

Art. 28. O CONTER manterá registro atualizado das operações de tratamento de dados pessoais que realizar, nos termos do art. 37 da LGPD, sob supervisão do Encarregado.

Parágrafo único. O registro de que trata o caput será revisado, no mínimo, anualmente, e sempre que houver alteração relevante em processo, sistema ou contrato.

Art. 29. Será elaborado Relatório de Impacto à Proteção de Dados Pessoais - RIPD para as operações de tratamento que apresentem alto risco aos direitos e às liberdades dos titulares, especialmente quando envolverem:

I) dados pessoais sensíveis, notadamente dados referentes à saúde e dados biométricos;

II) tratamento em larga escala;

III) monitoramento sistemático de titulares;

IV) decisões automatizadas com efeitos jurídicos;

V) uso de sistemas de inteligência artificial;

VI) novas tecnologias ou usos inovadores de dados pessoais.

Parágrafo único. Considerando a natureza das atividades do CONTER, receberão atenção prioritária os tratamentos relativos a processos ético-disciplinares, dados de saúde coletados em razão de exigências de exercício profissional ou de acessibilidade, dados biométricos utilizados para controle de acesso, controle de frequência ou identificação em processos seletivos, e dados constantes dos registros profissionais.

Art. 30. A proteção de dados pessoais será considerada desde a concepção e por padrão em todos os processos, sistemas e contratações do CONTER.

Art. 31. Os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares serão comunicados à ANPD e aos titulares afetados, na forma e nos prazos da regulamentação vigente, mediante procedimento estabelecido na NC-04.

Art. 32. Os direitos dos titulares previstos no art. 18 da Lei nº 13.709/2018, serão atendidos por canal específico, divulgado no sítio eletrônico institucional, sob responsabilidade do Encarregado.

Art. 33. A disciplina detalhada do tratamento de dados pessoais no CONTER constará de Política de Privacidade e Proteção de Dados Pessoais ("PPDP"), a ser editada como norma complementar a esta Política.

Art. 34. As operações de tratamento de dados pessoais realizadas por operadores contratados serão regidas por instrumento contratual que estabeleça a finalidade, a duração, as medidas de segurança exigidas e as obrigações de reporte de incidentes.

TÍTULO VI

DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 35. O CONTER manterá processo contínuo de gestão de riscos de segurança da informação, compreendendo as etapas de identificação, análise, avaliação, tratamento, monitoramento, análise crítica e comunicação dos riscos.

Art. 36. O processo de gestão de riscos observará a IN GSI/PR nº 5, de 2021, e as normas ABNT NBR ISO/IEC 27005 e ABNT NBR ISO 31000, no que couber.

Art. 37. Será elaborado, no mínimo anualmente, plano de tratamento de riscos de segurança da informação, contendo as ações, os responsáveis e os prazos, submetido à aprovação da CTPD.

Art. 38. Os riscos residuais serão formalmente aceitos pela Presidência, mediante manifestação prévia da CTPD.

TÍTULO VII

DA CONFORMIDADE, DA AUDITORIA E DAS PENALIDADES

CAPÍTULO I - DA CONFORMIDADE E DA AUDITORIA

Art. 39. O cumprimento desta Política e de suas normas complementares será objeto de verificação periódica, no mínimo anual, coordenada pelo GSI.

Art. 40. O CTPD definirá indicadores de segurança da informação, cujos resultados integrarão o relatório anual submetido ao Plenário.

Art. 41. O CONTER manterá evidência documental das medidas adotadas em cumprimento a esta Política, para fins de prestação de contas aos órgãos de controle e à ANPD.

CAPÍTULO II - DAS PENALIDADES

Art. 42. O descumprimento desta Política ou de suas normas complementares sujeitará o infrator às sanções previstas no regime jurídico a que estiver submetido, apuradas mediante procedimento próprio, assegurados o contraditório e a ampla defesa, a saber:

I) aos empregados públicos, as penalidades previstas na Consolidação das Leis do Trabalho e nas normas internas de pessoal do CONTER;

II) aos conselheiros, as penalidades previstas na legislação de regência da autarquia, no Regimento Interno e no Código de Ética aplicável;

III) aos estagiários e aprendizes, as medidas previstas no respectivo termo de compromisso e na legislação específica;

IV) aos prestadores de serviços e contratados, as sanções previstas no instrumento contratual e na Lei nº 14.133, de 1º de abril de 2021;

V) aos demais, as medidas administrativas cabíveis, incluída a suspensão ou revogação do acesso.

§ 1º - Esta Política não cria sanções novas, limitando-se a remeter aos regimes sancionatórios previamente estabelecidos em lei, contrato ou norma interna.

§ 2º - A apuração administrativa não prejudica a responsabilização civil e penal cabível, nem o dever de reparação do dano.

Art. 43. A suspensão cautelar de acesso a sistemas e informações deverá ser feita pelo GSI e imediatamente comunicada ao Encarregado, que recomendará a sua manutenção ou revogação à Presidência, visando a contenção de incidente.

TÍTULO VIII

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 44. Observada as indicações do Encarregado, a Presidência designará, no prazo de 30 (trinta) dias contados da publicação desta Resolução, o Gestor de Segurança da Informação e os integrantes da ETIR.

Art. 45. As normas complementares previstas no art. 26 serão editadas nos seguintes prazos, contados da publicação desta Resolução:

I) 90 (noventa) dias - NC-01, NC-02, NC-03 e NC-04;

II) 180 (cento e oitenta) dias - NC-05, NC-06, NC-07 e NC-11;

III) 270 (duzentos e setenta) dias - NC-08, NC-09 e NC-10.

§ 1º No prazo de 90 (noventa) dias, será editada a Política de Privacidade e Proteção de Dados Pessoais ("PPDP") de que trata o art. 33.

§ 2º No prazo de 120 (cento e vinte) dias, será realizado o inventário de ativos de informação e o registro das operações de tratamento de dados pessoais serão elaborados.

§ 3º No prazo de 180 (cento e oitenta) dias, os contratos vigentes serão revisados, para adequação às disposições desta Política, especialmente quanto às cláusulas de confidencialidade, de segurança da informação e de proteção de dados pessoais.