POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC)

CAPÍTULO I

Do Escopo

Art. 1º. A Política de Segurança da Informação e Comunicações (POSIC) define as diretrizes, competências e responsabilidades relativas ao uso, compartilhamento e trâmite de dados, informações e documentos em conformidade com a Legislação vigente, inclusive a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e a Medida Provisória 2.200-2 de 24 de agosto de 2001, assim como com as normas técnicas pertinentes, com valores éticos e com as melhores práticas de segurança da informação e comunicações.

Parágrafo único: Este documento segue os conceitos e definições do Glossário de Segurança da Informação publicado na portaria GSI/PR Nº 93 de 18 de Outubro de 2021, da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), do Glossário de Proteção de Dados Pessoais publicado em 31 de Janeiro de 2024 pela Agência Nacional de Proteção de Dados (ANPD) e das normas internas da NUCLEP.

Art. 2º. Fazem parte desta POSIC os documentos que a complementam, destinados à proteção da informação e à disciplina de sua utilização.

Seção I

Do Objetivo

Art. 3º. A Política de Segurança da Informação e Comunicações da NUCLEP alinha-se às estratégias da empresa para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pela própria, independentemente do meio onde estejam registradas.

Aprovada na 198° Reunião do Conselho de Administração, realizada em 24/10/2025

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção II

Da Abrangência

Art. 4º. Esta política se destina a todos os ativos de informação e às comunicações da organização, incluindo dados, sistemas, aplicações, infraestrutura e pessoas.

Art. 5º. Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela NUCLEP devem atender a esta política.

CAPÍTULO II

Das Referências Legais e Normativas

Art. 6º. Esse documento foi elaborado com base nas seguintes referências:

a) Política Nacional de Segurança da Informação, decreto Nº 9.637, de 26/12/2018 que determina a implementação da PNSI nos órgãos da Administração Pública Federal;
b) Resolução CGPAR/ME Nº 41, de 4 de agosto de 2022 que estabelece o planejamento, implementação e manutenção de práticas de Governança de Tecnologia da Informação e Comunicação para empresas federais, de modo a atender os padrões reconhecidos;
c) Instrução Normativa Nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal; e
d) Portaria GSI/PR nº 93, de 18 de outubro de 2021 que dispõe sobre o Glossário de Segurança da Informação.

Art. 7º. Também considera a recomendação estruturante contida no Acórdão nº 1.603/2008-TCU-Plenário, que orienta quanto a ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 8º. Contempla ainda a orientação disposta pelo "Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR)", além das orientações gerais contidas na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e nas normas ABNT NBR IS0/IEC 27001:2022; ABNT NBR ISO/IEC 27002:2022 ABNT NBR ISO/IEC 27701:2019; ABNT NBR ISO/IEC 29100:2020.

CAPÍTULO III

Dos Princípios

Art. 9º. A segurança da informação e comunicações da NUCLEP deve obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade e do não repúdio.

CAPÍTULO IV

Das Diretrizes Gerais

Art. 10º. A segurança da informação e comunicações tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 11º. As diretrizes de segurança da informação e comunicações devem considerar, prioritariamente, objetivos estratégicos, processos e os requisitos legais da NUCLEP.

Art. 12º. As diretrizes de segurança da informação e comunicações descritas nesta política devem ser observadas por todos os usuários que executem atividades vinculadas à NUCLEP, durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 13º. O cumprimento desta política, bem como dos normativos que a complementam, deverá ser avaliado periodicamente, por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia das cláusulas de responsabilidade e sigilo.

Art. 14º. A NUCLEP deve observar as diretrizes estabelecidas nesta política, bem como deve se orientar pelas melhores práticas e pelos procedimentos de segurança da informação e comunicações recomendados por órgãos e entidades, tanto públicas quanto privadas, responsáveis pelo estabelecimento de padrões.

Art. 15º. A NUCLEP deve criar, gerir e avaliar critérios de tratamento da informação, de acordo com o sigilo requerido, a relevância, a criticidade e a sensibilidade, observando a legislação em vigor.

Art. 16º. É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela NUCLEP.

Parágrafo único: Cópias de documentos classificados deverão sofrer o mesmo processo de classificação do respectivo original.

Art. 17º. O custodiante do ativo de informação deve ser formalmente designado pelo Gestor do Ativo de Informação.

Parágrafo único: A não designação pressupõe que o gestor do ativo de informação é o próprio custodiante.

Art. 18º. Os membros participantes de comitês e responsáveis pela gestão ou custódia dos ativos de informação deverão ter nomeados membros suplentes ou substitutos capacitados a substituir os membros titulares em caso de ausência prolongada.

Art. 19º. Os contratos, convênios, acordos e instrumentos congêneres firmados pela NUCLEP devem conter cláusulas que determinem a observância desta política e de seus documentos complementares.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

CAPÍTULO V

Das Competências e Responsabilidades

Seção I

Do Comitê de Governança Digital

Art. 20º. São competências do Comitê de Governança Digital:

I. analisar as políticas, diretrizes e planos relativos à governança de tecnologia da informação e comunicações (TIC) em um âmbito estratégico, em total alinhamento com as metas delineadas no Planejamento Estratégico Institucional da NUCLEP.

II. avaliar e aprovar alterações na Política de Segurança da Informação e Comunicações, assim como as normas e procedimentos relativos à segurança da informação e comunicações para a NUCLEP;

III. instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) em conformidade com a Norma Complementar nº O5/IN01/DSIC/GSIPR;

IV. instituir Grupo de Trabalho de Continuidade de TI, de caráter permanente, com objetivo de propor, manter e periodicamente testar medidas para continuidade e recuperação da informação, visando reduzir riscos e incertezas em TI.

V. instituir outros Grupos de Trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à tecnologia da informação e comunicações;

Seção II

Do Comitê de Segurança da Informação

Art. 21º. São competências do Comitê de Segurança da Informação:

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

I. assessorar o Gestor de Segurança da Informação na implementação das ações de segurança da informação e comunicações na NUCLEP;

II. avaliar propostas do Gestor de Segurança da Informação, bem como propor alterações na Política de Segurança da Informação e Comunicações, composta por diretrizes, normas e procedimentos relativos à segurança da informação e comunicações para a NUCLEP, em conformidade com a legislação existente sobre o tema, submetendo-as à apreciação da autoridade competente;

III. instituir Grupos de Trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à segurança da informação e comunicações;

IV. receber e analisar comunicações referentes a eventuais violações de segurança, apresentando parecer às autoridades / órgãos competentes para providências;

V. apoiar o Gestor de Segurança da Informação na implementação de programas destinados a conscientização e à capacitação de recursos humanos em segurança da informação e comunicações; e

VI. colaborar com o Gestor de Segurança de Informação na proposição de soluções técnicas de infraestrutura vinculadas à segurança da informação e comunicações.

Seção III

Da Gerência Geral de Tecnologia e Inovação

Art. 22º. São competências da Gerência Geral de Tecnologia e Inovação:

I. implantar, modernizar, manter e prover atendimento ao parque computacional e aos sistemas utilizados pelos colaboradores da NUCLEP;

II. implementar as ações do Plano Estratégico de TI e do Plano Diretor de TI, submetendo propostas à avaliação do Comitê de Governança Digital para aprovação pela Alta Direção da NUCLEP;

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

III. elaborar e implementar a Política de Segurança da Informação e Comunicações (POSIC) e suas normas relacionadas;

IV. criar e manter um Inventário de Ativos de Informação, com informações quantitativas e qualitativas necessárias para manter um controle de riscos eficiente.

V. Atuar como corresponsável pelo Inventário de Ativos de Informação, buscando ativamente informações junto às áreas responsáveis, sobre ativos identificados ainda não inventariados, sempre que identificar o uso destes enquanto pendentes de dados no Inventário de Ativos de Informação.

VI. prover soluções tecnológicas auditáveis para controle de acesso e movimentação de ativos de informação;

VII. estabelecer mecanismos de proteção física e lógica aos ativos de informação sob custódia da TI, contra acesso indevido, danos e interferências na disponibilidade desses recursos;

VIII. quando provocada pelos Gestores de Ativos de Informação, apoiar às demais áreas da NUCLEP na implantação de recursos de proteção física e lógica para seus respectivos ativos de informação; e

IX. viabilizar e manter junto à gestão de recursos humanos, um programa permanente de conscientização e capacitação em segurança da informação para todos os colaboradores da NUCLEP.

Seção IV

Do Gestor de Segurança da Informação

Art. 23º. As competências do Gestor de Segurança da Informação devem incluir:

I. promover cultura de segurança da informação e comunicações, propondo programas de conscientização e capacitação em segurança da informação para os colaboradores da NUCLEP;

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

II. apoiar na confecção de minutas de documentos da Política de Segurança da informação e Comunicações, composta por diretrizes, normas e procedimentos relativos à segurança da informação e comunicações para a NUCLEP, em conformidade com a legislação existente sobre o tema, submetendo-a a Presidência do Comitê de Governança Digital;

III. auxiliar na proposição de recursos necessários às ações de segurança da informação e comunicações;

IV. coordenar a Equipe de Prevenção, Tratamento e Resposta a incidentes Cibernéticos (ETIR);

V. acompanhar as investigações e as avaliações dos danos decorrentes de eventuais violações de segurança; e

VI. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações.

Seção VI

Dos Gestores de Ativos de Informação

Art. 24º. Compete aos Gestores de Ativos de informação da NUCLEP:

I. promover o levantamento contínuo dos ativos de informações relevantes em seus setores e incluí-las no Inventário de Ativos de Informação, incluindo dados precisos e relevantes sobre os mesmos, de modo a garantir que sejam protegidos usando os meios apropriados.

II. delegar o papel de Custodiante de Ativos de Informação para cada ativo sob sua responsabilidade.

III. registrar e conceder aos colaboradores, os devidos níveis de acesso sobre cada ativo identificado.

IV. manter atualizada a base de dados do Inventário de Ativos de Informação dos quais for responsável.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

V. a obrigação de informar à Gerência de Tecnologia da Informação e Inovação quanto a novos ativos de informação sob sua gestão ou quanto a ativos pré-existentes que devam ser protegidos.

Seção VII

Dos Custodiantes de Ativos de Informação

Art. 25º. Cabe aos Custodiantes de Ativos de Informação:

I. registrar e conceder os devidos níveis de acesso para cada ativo identificado, quando delegados para essa função;

II. manter atualizada a base de dados do Inventário de Ativos de Informação dos quais for responsável, quando for delegado para tal.

III. registrar e conceder aos colaboradores, os devidos níveis de acesso sobre cada ativo identificado, quando for delegado para essa atividade.

Seção VIII

Dos Usuários

Art. 26º. Compete à força de trabalho da NUCLEP:

I. cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações da NUCLEP;

II. buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III. assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação e Comunicações da NUCLEP, bem como assumindo responsabilidade por seu cumprimento;

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

IV. proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela NUCLEP;

V. assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela NUCLEP; e

VI. comunicar imediatamente o Gestor de Segurança da Informação qualquer descumprimento ou violação desta política e/ou de seus documentos complementares.

CAPÍTULO VI

Das Diretrizes Específicas

Art. 27º. Para cada uma das diretrizes constantes das seções deste capítulo deve, caso necessário, ser observada a pertinência de elaboração de procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o seu entendimento, incluindo, como estabelece a resolução CGPAR/ME Nº 41 em seu artigo 2, no inciso IX:

a) Classificação das informações pelas respectivas áreas de negócio e a disponibilização pela área de TIC de ambientes com o nível de segurança necessário ao seu armazenamento;

b) Controle de acesso local e remoto às redes de dados;

c) Controle de acesso aos sistemas;

d) Controle de acesso físico aos equipamentos de TIC;

e) Uso de unidades portáteis de armazenamento de dados e computadores portáteis;

f) Existência de rastro de auditoria (log) em sistemas críticos.

Parágrafo único: Todas os normativos e demais regras de segurança da informação da NUCLEP passam a ser parte integrante desta política e manterão suas características de disponibilidade, com intuito de estabelecer uma estrutura de normas definida, aprovada e compreendida para a implementação, operação e gestão da segurança da informação dentro da organização.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção I

Da Gestão da Segurança da Informação

Art. 28º. A Gestão de Segurança da Informação (GSI) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação.

Parágrafo único: Dessa forma, a GSI irá garantir que todos os produtos de TIC atendam aos padrões de segurança necessários e possuam as certificações ou avaliações apropriadas.

Art. 29º. A Gestão da Segurança da Informação (GSI) deve compreender ações e métodos que visem estabelecer parâmetros adequados, relacionados à segurança da informação e comunicações, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da NUCLEP.

Parágrafo único: De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Comitê de Governança Digital deve instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) conforme determina a Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018, que determina que compete aos órgãos da administração pública federal a instituição e implementação de uma ETIR, nos termos do inciso VII do art. 15.
A Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, estabelece alterações na Instrução Normativa GSI/PR nº 02, de 24 de julho de 2020, dispondo sobre a atuação destas equipes no âmbito da Administração Pública Federal.

Art. 30º. A Gestão da Segurança da Informação (GSI) deve garantir a segurança e integridade dos componentes críticos de todos os sistemas de informação e comunicação. Implementando processos de monitoramento adequados, garantia de rastreabilidade de componentes críticos e a prevenção de adulterações.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção II

Da Norma de Mesa Limpa e Tela limpa

Art. 31º. Este normativo estabelece diretrizes de mesa limpa e tela limpa com o princípio de mitigar que as informações corporativas, tanto no formato digital ou físico e, independente da sua classificação, sejam deixados desprotegidos em espaços públicos ou de trabalho (mesas, telas, entre outros), durante e fora do horário comercial.

Seção III

Da Norma de Armazenamento e Descarte de Ativos

Art. 32º. A NUCLEP estabelece diretrizes adicionais relacionadas ao armazenamento, manutenção e descarte correto dos ativos utilizados na organização, com intuito de proteger as informações contidas neles.

Seção IV

Da Norma de Uso de Controles Criptográficos e Chaves Criptográficas

Art. 33º. Essa norma estabelece os conceitos e requisitos para o uso dos controles criptográficos e das chaves criptográficos adequadas às necessidades de negócio. O uso eficaz dos controles criptográficos, deve ser usado para proteção da confidencialidade, autenticidade e integridade das informações da NUCLEP, sejam essas produzidas, armazenadas ou recebidas, sendo portanto, responsabilidade do Gestor de Segurança da Informação a implementação dos procedimentos relativos ao seu uso seguro, no âmbito dessas informações sob a responsabilidade da NUCLEP, estando em conformidade com as orientações contidas na norma e legislação específica.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção V
Da Norma de Categorização e Classificação dos Ativos de Informação

Art. 34º. Informações geradas, adquiridas ou custodiadas pela NUCLEP deverão ser categorizadas, recebendo classificação apropriada para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento.

§1º. A classificação da informação atenderá ao preconizado pelas leis que regem o assunto. Tipos de classificação não previstos na legislação e regulamentos específicos para a Administração Pública Federal (APF) poderão ser acrescentados à norma visando atingir objetivos corporativos de controle, específicos sobre a natureza das informações, desde que não conflitem com a legislação em vigor nem com outros regulamentos relacionados à Administração Pública Federal.

§2º. As normas e regras de segurança da informação e comunicação da NUCLEP definirão os responsáveis pela correta classificação das informações, assim como determinarão a forma de circulação dessas informações. Essas normas e regras deverão ser revistas e adequadas conforme exigências específicas da legislação em vigor, assim como por necessidades específicas da NUCLEP.

Seção VI
Da Segurança Física e do Ambiente

Art. 35º. A organização deve estabelecer diretrizes para proteção das instalações e ativos de informação da NUCLEP contra ameaças, riscos e eventos que possam comprometer a segurança, integridade e funcionamento eficaz dos recursos e das operações.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção VII

Da Norma de Uso de Recursos Computacionais

Art. 36º. A organização deve estabelecer diretrizes para o uso eficiente, seguro e responsável dos recursos tecnológicos, disponibilizados aos colaboradores, dentro do ambiente da NUCLEP.

Seção VIII

Da Norma de Uso da Internet e Mídias Sociais

Art. 37º. A NUCLEP estabelece diretrizes e responsabilidades quanto ao uso aceitável da internet e das mídias sociais no ambiente da NUCLEP para todos os colaboradores através da Norma de Uso da Internet e Mídias Sociais.

Seção IX

Da Norma de Uso de E-mails e Comunicadores Instantâneos

Art. 38º. A NUCLEP estabelece diretrizes de comportamento durante o envio e recebimento de e-mails na organização, com o intuito de garantir a segurança e a privacidade da informação.

Seção X

Da Norma de Proteção dos Ativos de Informação

Art. 39º. A Norma de Proteção dos Ativos de Informação estabelece diretrizes para proteção dos ativos de informação, físicos ou lógicos, críticos ou não, utilizados na organização ou por seus colaboradores durante a execução de suas atividades.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção XI

Da Norma de BYOD *(Bring Your Own Device)*

Art. 40º. A NUCLEP estabelece diretrizes para o uso seguro dos dispositivos pessoais que são utilizados para fins corporativos na empresa, visando delimitar responsabilidades e garantir a proteção das informações contidas nesses dispositivos.

Seção XII

Do Norma de Acesso Remoto

Art. 41º. A Norma de Acesso Remoto preconiza diretrizes para que o acesso remoto aos recursos e informações corporativas da NUCLEP sejam realizadas de maneira segura e em conformidade com as políticas de segurança.

Seção XIII

Da Propriedade da Informação

Art. 42º. As informações produzidas por pessoas físicas e jurídicas, sob a responsabilidade da NUCLEP, são consideradas parte do seu patrimônio intelectual, não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei Nº 10.973/2004 - Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta política, em seus documentos complementares e demais regulamentações em vigor.

Art. 43º. É vedada a utilização de informações produzidas para uso exclusivo da NUCLEP, por terceiros em quaisquer outros projetos ou atividades de uso diverso ao originalmente estabelecido, salvo com autorização específica emitida pelo gestor do ativo de informação, nos processos e documentos de sua competência, observando a legislação em vigor.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 44º. O colaborador responsável por produzir, tratar ou fazer a custódia de informações, deverá assinar Termo de Responsabilidade, tomando ciência desses termos.

Seção XIV

Das Normas de Controle de Acesso Físico e Lógico

Art. 45º. A Norma de Controles de Acesso Lógico estabelece os normativos e procedimentos necessários para o eficaz controle de acesso lógico a todos os ativos de informação pertencentes à NUCLEP.

Art. 46º. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 47º. Devem ser criados, e mantidos, mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 48º. Todos os ativos de informação da NUCLEP, quando registrados no Inventário de Ativos de Informação, devem ter um Custodiante do Ativo da Informação formalmente designado pelo Gestor do Ativo de Informação, que deve definir os privilégios de acesso às informações, observando a regulamentação em vigor.

a. É obrigação dos gestores das áreas informar à Gerência de Tecnologia da Informação e Inovação quanto a novos ativos ou pré-existentes que devam ser inventariados e protegidos.
b. É obrigação da Gerencia Geral de TI e Inovação, buscar detalhes junto às áreas, sempre que identificar o uso de novos ativos de informação para inventariar.

Art. 49º. O usuário é responsável por todos os atos praticados com suas credenciais, entre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital.

Art. 50º. O usuário responderá pela segurança dos ativos, dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas credenciais, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário, e desde que o mesmo tenha tomado precauções apropriadas para proteção de suas credenciais, não compartilhando-as ou facilitando o seu uso indevido.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Parágrafo único: A identificação do usuário, independentemente do meio e a forma, deve ser pessoal e intransferível, permitindo o reconhecimento do usuário de maneira clara e irrefutável.

Art. 51º. A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de autorização, acesso ou uso necessitará de prévia autorização do Gestor do Ativo de Informação, observando-se a legislação em vigor.

Parágrafo único: A autorização de que trata o caput poderá ser delegada ao custodiante do ativo de informação, desde que o mesmo seja devidamente treinado previamente para tal tarefa.

Art. 52º. Sempre que houver mudanças nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser readequados imediatamente, devendo ser cancelados em caso de desligamento da NUCLEP.

Art. 53º. Toda movimentação funcional deverá ser obrigatoriamente registrada através do formulário apropriado no sistema de registro de movimentação de pessoal.

Art. 54º. É atribuição do Gestor da área informar à Gerência Geral de Tecnologia e Inovação sobre a saída de colaboradores de seu setor, visando a revogação de acessos.

Art. 55º. A NUCLEP estabelece uma norma específica de controles de acesso, para promover a segurança do ambiente, a fim de estabelecer regras, procedimentos e acordos para proteger informações.

Art. 56º. A Gerência Geral de Tecnologia e Inovação deve, de ofício, estabelecer mecanismos de proteção contra acesso indevido, danos e interferências às instalações físicas associadas à Tecnologia da Informação, e se provocada, deverá apoiar as demais áreas na provisão de soluções para proteção e controle de acesso nas demais áreas de processamento de informações críticas ou sensíveis, sendo essas de responsabilidade de seus próprios Gestores.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Parágrafo único. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados entre os ativos de informação inventariados na organização.

Seção XV

Da Gestão Arquivística de Documentos Eletrônicos

Art. 57º. A Gestão Arquivística de Documentos Eletrônicos tem por objetivo a produção / criação, uso / acesso, avaliação e destinação (arquivamento ou descarte) dos documentos eletrônicos autênticos e fidedignos.

Art. 58º. Os documentos eletrônicos produzidos no âmbito da NUCLEP se houver necessidade jurídica comprovada, terão garantia de autenticidade, confidencialidade, integridade, disponibilidade e não repúdio asseguradas, mediante utilização de assinatura eletrônica, nos termos das leis nº 14.063, de 23 de Setembro de 2020, que dispõe sobre as regras para uso das assinaturas eletrônicas no Brasil, e nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que dispõe sobre as assinaturas eletrônicas qualificadas, emitidas pela ICP-Brasil ou sobre o uso de certificados digitais de terceiros como meio de reconhecimento aceito entre ambas as partes, conforme a legislação vigente.

Seção XVI

Da Gestão Arquivística do Correio Eletrônico

Art. 59º. As mensagens de correio eletrônico de caráter corporativo deverão ser reconhecidas como documento de arquivo, sujeitas às normas vigentes na empresa.

Art. 60º. Para garantia dos requisitos de segurança e privacidade necessários ao pleno uso do correio eletrônico corporativo serão adotados recursos de alta disponibilidade, salvaguarda apropriada e meios reforçados de autenticação que tratem essa ferramenta como ativo de informação crítico a ser resguardado.

Art. 61º. O Correio Eletrônico Corporativo é uma ferramenta de uso exclusivo da empresa e todo conteúdo de informação contido nele, pertence a NUCLEP.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção XVII

Da Preservação dos Documentos em Meio Eletrônico

Art. 62º. O tratamento arquivístico de documentos eletrônicos, inclusive o descarte, deve observar procedimentos definidos na legislação sob a responsabilidade de cada área da NUCLEP.

Seção XVIII

Da Segurança em Recursos Humanos

Art. 63º. A NUCLEP deve estabelecer procedimentos de segurança em recursos humanos que vise desde a parte da contratação até o processo de desligamento.

Art. 64º. Os usuários devem ter ciência:

I. Das ameaças e preocupações relativas à segurança da informação e comunicações; e
II. De suas responsabilidades e obrigações no âmbito desta política.

Art. 65º. Todos os usuários devem difundir e exigir o cumprimento desta política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 66º. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem toda a força de trabalho da NUCLEP, obtendo comprovação destes quanto à presença e satisfatória absorção dos conceitos apresentados, de acordo com suas competências funcionais.

Art. 67º. O setor responsável pelos treinamentos na empresa, em conjunto com a Gerência Geral de Tecnologia e Inovação devem manter um fluxo constante de treinamentos em segurança da informação e privacidade, para toda a força de trabalho, já começando desde a ambientação, de forma a manter todos os colaboradores engajados e conscientes de sua responsabilidade em proteger os ativos de informação da NUCLEP, mantendo registros auditáveis sobre esses treinamentos.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção XIX

Da Gestão de Riscos

Art. 68º. As áreas responsáveis por ativos de informação devem implantar processos próprios de gestão contínua de riscos, cujos relatórios serão insumos na implementação e operação da Gestão da Segurança da Informação.

§1°. A Gerência Geral de Tecnologia e Inovação deverá fazer a gestão dos riscos específicos de TI, avaliando os riscos relativos à segurança dos ativos de informação e a conformidade com exigências regulatórias ou legais;

§2°. Finalizado cada ciclo de tratamento dos riscos identificados, os resultados devem ser documentados e relatados por meios seguros;

§3°. Deve ser mantida uma estrutura de gestão de risco continuamente monitorada e adaptada para abordar as mudanças internas e externas;

§4°. Será mantido um histórico evolutivo auditável quanto às atividades da gestão dos riscos identificados e os respectivos tratamentos dados, pela TI e pelas áreas responsáveis.

Seção XX

Da Continuidade de Serviços de TI

Art. 69º. O Comitê de Governança Digital deverá instituir um Grupo de Trabalho de Continuidade de TI, de caráter permanente, sob liderança da Gerência Geral de Tecnologia e Inovação, com objetivo de propor, manter e periodicamente testar medidas para continuidade e recuperação da informação, visando reduzir riscos e incertezas em TI para um nível aceitável ou previamente definido, prevenindo interrupções e reduzindo impactos causados por desastres nos recursos de tecnologia da informação vitais aos processos da NUCLEP.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Seção XXI

Do Tratamento de Incidentes de Rede

Art. 70º. O Comitê de Governança Digital deverá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Norma Complementar nº O5/IN01/DSIC/GSIPR, provendo meios para prevenir e tratar especificamente os incidentes cibernéticos.

Art. 71º. Deve-se prever recursos especializados para que essa equipe seja qualificada e reciclada dentro das premissas anteriores, assim como fomentar a integração com as ETIR de outras instituições públicas, de modo a compartilhar recursos e conhecimentos técnicos na esfera de outros órgãos da Administração Pública Federal.

CAPÍTULO VII

Da Proteção de Dados Pessoais

Art. 72º. A NUCLEP se compromete a observar os deveres previstos na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), aplicando medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de pessoas naturais contra riscos tais como acessos não autorizados, situações acidentais ou ilícitas de destruição de ativos de informações, assim como o uso não autorizado, modificação, perda, roubo, divulgação ou quaisquer formas de tratamento inadequado ou ilícito, por todo o ciclo de vida das informações, desde a fase de coleta de dados, concepção de sistema, produto ou projeto que exijam tratamento de dados pessoais, até o seu descarte apropriado.

Art. 73º. Conceber e implementar mecanismos para assegurar e garantir o exercício dos direitos do titular de dados, de acordo com a Política de Privacidade da NUCLEP e os termos previstos na LGPD.

Art. 74º. Zelar, verificar e demonstrar que o tratamento de dados atende aos requisitos, tanto de proteção de dados quanto de garantia da privacidade.

Art. 75º. Inventariar e avaliar os riscos, bem como implementar medidas, tanto de segurança quanto de privacidade, em toda e qualquer operação com dados pessoais em sistemas, produtos, processos ou serviços; contemplando as finalidades, hipóteses de tratamento e bases legais que fundamentam as atividades de tratamento de dados pessoais ou dados pessoais sensíveis.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 76º. Manter os dados pessoais armazenados pelo tempo estritamente essencial para o cumprimento dos propósitos contratuais estipulados ou pelo período necessário estabelecido em obrigações legais ou regulatórias, garantindo a efetiva confidencialidade, o armazenamento seguro com rastreabilidade e a destinação final segura.

Art. 77º. Garantir a eliminação dos dados pessoais após o término de seu tratamento, ressalvada a conservação dos dados para: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; e uso exclusivo do controlador, sendo vedado o acesso por terceiros e desde que anonimizados os dados.

Art. 78º. Os dados pessoais sensíveis devem ser armazenados em local segregado dos demais dados pessoais e submetidos a um nível de restrição mais rígido, sendo disponibilizados apenas mediante requerimento formal e justificativa legítima.

Art. 79º. Caso ocorra um incidente de segurança com dados pessoais que possa resultar em riscos ou em danos relevantes ao titular, é necessário informar imediatamente ao Encarregado de Proteção de Dados *(Data Protection Officer - DPO),* que tomará as ações cabíveis conforme a Política de Privacidade da NUCLEP e os termos previstos na LGPD.

CAPÍTULO VIII

Da Relação com Terceiros

Art. 80º. Nos editais de licitação, nos contratos, convênios, acordos e nos instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços, deverá constar cláusula específica sobre a obrigatoriedade de observância a esta política, bem como deverá ser exigida, da entidade contratada, a assinatura dos Termos de Responsabilidade apropriados.

Art. 81º. Os contratos, convênios, acordos ou instrumentos congêneres deverão prever a obrigação da outra parte em divulgar esta política, bem como respectivas normas e procedimentos complementares, aos seus empregados e prepostos envolvidos em atividades na NUCLEP.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

CAPÍTULO IX

Da Norma de Uso de Ferramentas de Inteligência Artificial e Aprendizado de Máquina

Art. 82º. A Empresa deve estabelecer diretrizes, condições e limites para uso responsável de ferramentas de Inteligência Artificial e Aprendizado de Máquina no tratamento de dados sob guarda da NUCLEP, com o intuito de garantir a segurança e a privacidade desses dados.

Art. 83º. É vedado o uso de ferramentas de IA para tratamento de dados pessoais, dados sob sigilo previstos em legislações específicas, ou de natureza estratégica para a NUCLEP. A proibição se deve à condição em que as ferramentas de Inteligência Artificial, gratuitas e de acesso público, em sua maioria, tem seus motores básicos hospedadas em datacenters de terceiros, fora do Brasil, tendo ainda dados eventualmente tratados por sistemas intermediários, igualmente de terceiros, fora do escrutínio da companhia, configurando potencial fonte de vazamento de dados.

Art. 84º. As exceções e condições apropriadas para o uso das ferramentas de IA na NUCLEP serão detalhadas em normativo específico para essa finalidade.

CAPÍTULO X

Das Penalidades

Art. 85º. A não observância desta política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

§1º. As penalidades administrativas serão aplicadas após a sua devida apuração em processo administrativo disciplinar, sendo observados critérios de gravidade e reincidência dos atos de violação cometidos à Política de Segurança da Informação e Comunicações.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

§2º. As infrações ocorridas violando as normas que compõem a Política de Segurança da Informação e Comunicações deverão ser analisadas pelo gestor imediato do infrator, que deverá comunicar imediatamente ao Comitê de Segurança da Informação para fins de determinação da apuração das eventuais responsabilidades dos funcionários envolvidos.

CAPÍTULO XI

Da Auditoria e Conformidade

Art. 86º. A autorização, o acesso e o uso da informação e dos procedimentos de auditoria devem ser executados nos recursos de tecnologia da informação e comunicações formalmente estabelecidos pela NUCLEP.

Art. 87º. Deve ser realizada, com periodicidade máxima de três anos, a verificação de conformidade entre as práticas de segurança da informação e comunicações executados na NUCLEP em relação a esta política, assim como suas normas e procedimentos complementares.

Art. 88º. A verificação de conformidade também deve ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a NUCLEP.

Art. 89º. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pelo Comitê de Segurança da Informação.

Art. 90º. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 91º. As auditorias de segurança da informação somente terão início após definidos os padrões de conformidade, provendo prazo para prévia adaptação e treinamento dos colaboradores, em cada uma das gerências auditadas.

Art. 92º. Nenhum órgão ou unidade, abrangidos por esta política, poderá permanecer sem verificação de conformidade de suas práticas de segurança da informação e comunicações por período superior a três (3) anos.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 93º. A verificação de conformidade será executada por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação, sendo que, com a prévia aprovação deste, tal serviço poderá ser subcontratado no todo ou em parte.

Art. 94º. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 95º. A verificação de conformidade poderá combinar uma ampla variedade de técnicas, tais como: análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 96º. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, que o Gestor de Segurança da Informação encaminhará ao gestor do ativo de informação do órgão ou unidade verificada, para ciência e tomada das ações cabíveis.

Art. 97º. As não conformidades identificadas, após documentadas e informadas ao gestor do ativo de informação impactado terão prazo para adequação, com consequente nova verificação de conformidade.

CAPÍTULO XII

Da Vigência E Atualização

Art. 98º. Esta política, bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou quando necessário, não excedendo o período máximo de dois anos.

CAPÍTULO XIII

Normativos Complementares

Art. 99º. Para fins de detalhamento para a implantação e manutenção da presente política, foi elaborado um glossário de termos relativos à segurança da informação e um conjunto de normas complementares.

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br

Art. 100º. A estrutura formal da Política de Segurança da Informação e Comunicações da NUCLEP foi elaborada conforme os documentos a seguir:

1. Política de Segurança da Informação e Comunicações – POSIC (este documento)
2. Glossário de Segurança da Informação (Anexo I da POSIC da NUCLEP)
3. Norma de Classificação de Ativos de Informação
4. Norma de Mesa Limpa Tela Limpa
5. Norma de Armazenamento e Descarte de ativos
6. Norma de Uso de Controles Criptográficos e Chaves Criptográficas
7. Norma de Controle de Acesso Lógico
8. Norma de Segurança Física e do Ambiente
9. Norma de Uso dos Recursos Computacionais
10. Norma de Uso de Internet e Mídias Sociais
11. Norma de Uso de e-mails e Comunicadores Instantâneos
12. Norma de Proteção de Ativos de Informação
13. Norma de Uso de Dispositivos Particulares - BYOD (Bring Your Own Device)
14. Norma de Acesso Remoto
15. Norma de Uso de Ferramentas de Inteligência Artificial e Aprendizado de Máquina
16. Política de Privacidade da NUCLEP

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4303 | www.nuclep.gov.br | presidencia@nuclep.gov.br