RESOLUÇÃO ARPE Nº 312, DE 14 DE NOVEMBRO DE 2025.

Aprova a Política de Segurança da Informação (PSI) da Agência de Regulação dos Serviços Públicos Delegados de Pernambuco - ARPE.

A DIRETORIA COLEGIADA DA AGÊNCIA DE REGULAÇÃO DOS SERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DE PERNAMBUCO - ARPE, com fundamento na Lei nº 12.524, de 30 de dezembro de 2003, e alterações, e regulamentada pelo Decreto nº 30.200, de 9 de fevereiro de 2007;

CONSIDERANDO o Decreto Estadual nº 49.914, de 10 de dezembro de 2020, que institui a Política Estadual de Segurança da Informação – PESI, no âmbito da administração pública estadual;

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação (PSI) da ARPE, na forma do Anexo Único desta Resolução.

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

Recife, 14 de novembro de 2025.

Carlos Porto Filho
Diretor-Presidente

Frederico Arthur Maranhão Tavares de Lima
Diretor de Regulação Econômico-Financeira

Lara Pinheiro de Macedo Montarroyos
Diretora Administrativo Financeira

Documento assinado eletronicamente por **Lara Pinheiro**, em 14/11/2025, às 09:22, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

Documento assinado eletronicamente por **Carlos Porto**, em 14/11/2025, às 11:15, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

Documento assinado eletronicamente por **Frederico Arthur Maranhao Tavares de Lima**, em 14/11/2025, às 14:13, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **76548267** e o código CRC **ED1AF71A**.

AGÊNCIA DE REGULAÇÃO DE PERNAMBUCO

Av. Conselheiro Rosa e Silva, nº 975, - Bairro Aflitos, Recife/PE - CEP 52050-020, Telefone:

PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ARPE AGÊNCIA DE REGULAÇÃO DE PERNAMBUCO

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

Raquel Teixeira Lyra Lucena
GOVERNADORA

Priscila Krause Branco
VICE-GOVERNADORA

Carlos Porto de Barros Filho
DIRETOR-PRESIDENTE

Lara Pinheiro de Macedo Montarroyos
DIRETORA ADMINISTRATIVO FINANCEIRA

Roberta Araújo Machado
DIRETORA TÉCNICO-OPERACIONAL

Frederico Arthur Maranhão Tavares de Lima
DIRETOR ECONÔMICO-FINANCEIRO

ELABORAÇÃO E DIAGRAMAÇÃO

Luiz de Freitas Lima Neto
COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO

Jonathas Correia do Nascimento
APOIO ADMINISTRATIVO

Victor Daniel Dionízio Conde
ESTAGIÁRIO

Ítalo Artur Dantas de Vasconcelos
ESTAGIÁRIO

REVISÃO

Maria Olívia Leite de Aguiar Silva
COORDENADORA DE NORMATIZAÇÃO REGULATÓRIA

Marcela Magalhães Santos Gonçalves de Freitas
COORDENADORA DE CONTROLE INTERNO

ARPE AGÊNCIA DE REGULAÇÃO DE PERNAMBUCO

GOVERNO DE PERNAMBUCO ESTADO DE MUDANÇA

LGPD Pernambuco

Av. Rosa e Silva, nº 975, Aflitos, Recife/PE.

SUMÁRIO

Política de Segurança da Informação da Agência de Regulação dos Serviços Públicos Delegados do Estado de Pernambuco

1. Introdução

A informação é um ativo de valor inestimável para a Agência de Regulação dos Serviços Públicos Delegados do Estado de Pernambuco - ARPE, essencial para o cumprimento de sua missão institucional, para a tomada de decisões estratégicas e para a prestação de serviços de qualidade à sociedade pernambucana. No ambiente digital contemporâneo, a proteção adequada destes ativos de informação contra um perigo crescente de ameaças é fundamental para a continuidade operacional, a integridade institucional e a confiança pública.

Esta Política de Segurança da Informação (PSI) estabelece o compromisso da ARPE com a proteção da confidencialidade, integridade e disponibilidade das informações sob sua guarda, sejam elas pertencentes à própria Agência, aos seus regulados, aos seus fornecedores, aos seus colaboradores ou aos cidadãos.

A presente PSI visa, portanto, orientar e divulgar as ações e comportamentos relacionados à segurança da informação e à proteção de dados pessoais, em plena conformidade com a legislação vigente, em especial a Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais), e alinhada às melhores práticas e diretrizes governamentais. Sua observância é obrigatória e contribui para a construção de um ambiente organizacional seguro, resiliente e confiável.

2. Objetivo

Esta Política de Segurança da Informação tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para buscar garantir a proteção das informações da ARPE. A Política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

3. Princípios Gerais

Esta PSI da ARPE está baseada nos seguintes princípios:

- **Confidencialidade:** Garantir que as informações sejam acessada apenas por pessoas autorizadas;
- **Integridade:** Assegurar a exatidão e a completude da informação e dos métodos de seu processamento, prevenindo modificações não autorizadas;
- **Disponibilidade:** Garantir que a informação e os sistemas associados estejam acessíveis e utilizáveis sempre que necessário por usuários autorizados, resistindo a interrupções;
- **Privacidade e Proteção de Dados:** Realizar o tratamento de dados pessoais para finalidades legítimas, específicas e explícitas, garantido os direitos dos titulares; e
- Responsabilidade e Prestação de Contas (*Accountability*): Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados.

4. Abrangência

Esta Política se aplica a todos os ativos de informação da ARPE, incluindo dados, sistemas, aplicativos, dispositivos e redes, e é destinada a todos os colaboradores.

5. Termos e Definições

Para os fins desta Política, aplicam-se os seguintes termos e definições, complementados pelo glossário da LGPD e pelo Gabinete de Segurança Institucional (Portaria nº 93/2021):

Ativo de Informação: Qualquer ativo de informação ou recurso associado ao tratamento da informação, que tenha valor para a Agência. Inclui, mas não se limita a: equipamentos de informática, rede de computadores, sistemas, aplicativos, credenciais, dados de autenticação e ambientes físicos;

Colaboradores: Diretores, Conselheiros, servidores, estagiários, prestadores de serviço e terceiros que tenham acesso aos ativos de informação da Agência;

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Dado: Representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável;

Dado Pessoal Sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Encarregado pelo Tratamento de Dados Pessoais (DPO): Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou sob suspeita, que possa comprometer a segurança dos ativos de informação;

Princípio do Menor Privilégio: Princípio de segurança em que um usuário deve ter apenas os direitos de acesso mínimos necessários para realizar suas tarefas;

Risco: Efeito da incerteza nos objetivos, expresso em termos de combinação da probabilidade de um evento e suas consequências;

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Tratamento de Dados Pessoais: Toda operação realizada com dados pessoais (coleta, produção, recepção, classificação, etc.);

Vulnerabilidade: Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças;

Malware: Software malicioso desenvolvido com a finalidade de causar danos, explorar vulnerabilidades, obter acesso não autorizado ou comprometer a confidencialidade, integridade ou disponibilidade de ativos de informação;

Firewall: Dispositivo ou software de segurança responsável por monitorar e controlar o tráfego de rede, com base em regras pré-definidas, com o objetivo de permitir ou bloquear comunicações entre redes ou dispositivos, protegendo os ativos de informação contra acessos não autorizados; e

Log: Registro de eventos ou atividades realizados em sistemas, dispositivos ou aplicações, que permite rastrear ações, identificar comportamentos anômalos, realizar auditorias e apoiar investigações de incidentes de segurança da informação.

6. Diretrizes Gerais

6.1. Compromisso com a Segurança da Informação

Todos os colaboradores comprometem-se a proteger a confidencialidade, a integridade e a disponibilidade das informações da organização, de seus clientes, fornecedores e parceiros.

6.2. Proteção de Dados Pessoais

A ARPE compromete-se a tratar os dados pessoais em conformidade com a Lei Geral de Proteção de Dados (LGPD), Política de Privacidade da ARPE e demais regulamentações aplicáveis, garantindo que o tratamento seja realizado para finalidades legítimas, específicas e explícitas, com respeito aos direitos dos titulares.

6.3. Uso Aceitável dos Recursos

A ARPE adota uma abordagem baseada em riscos para a segurança da informação, cujo processo é coordenado pela Coordenadoria de Tecnologia da Informação - CTI com o apoio da Unidade de Controle Interno. Os riscos aos ativos de informação e processos de negócio devem ser continuamente identificados, analisados, avaliados e tratados, conforme documentado nos planos de gerenciamento de riscos setoriais.

É vedado o uso dos recursos de Tecnologia da Informação e Comunicação da ARPE para:

- Fins pessoais, políticos, ilegais ou que comprometam a imagem institucional;
- Instalar softwares não autorizados; e
- Compartilhar senhas ou credenciais de acesso.

7. Diretrizes Específicas

7.1. Compromisso com a Segurança da Informação

Todos os colaboradores comprometem-se a proteger a confidencialidade, a integridade e a disponibilidade das informações da organização, cidadão, fornecedores, prestadoras de serviço e poder público.

Inventário: A Coordenadoria de Tecnologia da Informação manterá um inventário atualizado de todos os ativos de hardware e software da ARPE. Este inventário deverá conter, no mínimo, as informações coletadas via software, gerenciado pela equipe responsável pela segurança dos ativos, e ser enriquecido com dados de propriedade, criticidade e localização;

Software: É estritamente proibida a instalação e o uso de softwares não licenciados, piratas ou que utilizem mecanismos para burlar a ativação. Todo software utilizado deve ser previamente aprovado pela Coordenadoria de Tecnologia da Informação (CTI), acompanhado de justificativa de uso vinculada às atividades desempenhadas na área de lotação do solicitante e ter sua licença devidamente registrada; e

Descarte Seguro: Ativos de hardware (como HDs) e mídias que contenham informações da ARPE devem ser higienizados ou destruídos de forma segura antes do descarte, a fim de impedir a recuperação indevida de dados e garantir a proteção das informações conforme as diretrizes de segurança da informação e da LGPD.

7.2. Classificação da Informação

A ARPE adota a seguinte classificação das informações sob sua guarda, distribuídas em quatro níveis:

- **Pública**: Informações que podem ser divulgadas livremente, sem qualquer restrição de acesso;
- **Interna:** Informações destinadas exclusivamente aos colaboradores da ARPE, cujo acesso não deve ser permitido a pessoas externas ao órgão;
- **Restrita**: Informações cujo acesso depende de autorização específica, sendo permitido apenas a pessoas previamente designadas; e
- **Sigilosa**: Informações protegidas por legislações específicas, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI), cujo acesso é rigorosamente controlado e limitado, observada a legislação aplicável.

7.3. Controle de Acesso

Política de Senhas: Esta política deve ser formalmente documentada e comunicada a todos os usuários. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes;

Menor Privilégio: O acesso a pastas compartilhadas, sistemas e informações deve ser concedido com base no princípio do menor privilégio, garantindo que os usuários tenham acesso apenas aos recursos estritamente necessários para o desempenho de suas funções. As permissões de acesso devem ser revisadas periodicamente;

Acesso Remoto: O acesso remoto à rede da ARPE deve ser autorizado apenas para colaboradores que necessitem no exercício de suas funções, mediante solicitação formal e aprovação da CTI. O acesso deve utilizar autenticação e criptografia, sendo vedado para fins não institucionais. A CTI poderá revogar o acesso em caso de término de contrato, mudança de lotação, perda de necessidade, vulnerabilidade ou uso indevido; e

Contas de Usuário: É proibido o compartilhamento de contas de usuário. Contas genéricas somente poderão ser utilizadas quando estritamente necessário, previamente comunicadas e autorizadas pela CTI, com responsabilidade claramente definida e monitoramento de suas atividades. O acesso deve ser revogado imediatamente após o desligamento do usuário.

7.4. Gestão de Incidentes de Segurança

Todos e quaisquer incidentes de segurança da informação deverão ser comunicados imediatamente à Coordenadoria de Tecnologia da Informação. Caberá à ARPE manter um processo formal para o registro, tratamento, resposta e análise de incidentes, garantindo a adoção de medidas corretivas e preventivas que minimizem impactos e evitem recorrências.

7.5. Segurança de Redes e Comunicações

- **Documentação da Rede:** A CTI deverá criar e manter diagramas atualizados da topologia da rede interna (física e lógica) para facilitar a análise de segurança e a resposta a incidentes;
- **Segurança dos Equipamentos de Rede:** As senhas padrão de todos os equipamentos de rede (switches, roteadores, etc.) deverão ser obrigatoriamente alteradas para senhas fortes no momento da instalação. As portas de gerenciamento não utilizadas deverão ser desabilitadas; e
- **Segurança Wi-Fi:** Deverá ser criada uma rede Wi-Fi para convidados, separada e isolada da rede corporativa interna, para impedir o acesso indevido de visitantes aos ativos da ARPE.

7.6. Segurança das Operações

- **Proteção contra Malware:** Todos os servidores e estações de trabalho devem possuir uma solução de antivírus/antimalware corporativa, gerenciada centralmente e mantida atualizada, devendo ser avaliada quanto à sua adequação para o ambiente;
- **Gerenciamento de Logs:** Os logs de segurança do servidor, firewall e outros sistemas críticos devem ser habilitados, protegidos contra adulteração e revisados periodicamente pela CTI em busca de atividades suspeitas ou anômalas;
- **Monitoramento:** Ferramentas para o monitoramento da performance e da segurança do servidor e da rede interna deverão ser implementadas, visando a detecção proativa de falhas e incidentes. Diretrizes Específicas; e
- **Gestão de Atualizações:** A CTI deverá estabelecer um processo para garantir que as atualizações e correções de segurança para sistemas operacionais e softwares sejam aplicadas de forma tempestiva, com base na criticidade das vulnerabilidades.

8. Estrutura de Governança e Responsabilidade

A segurança da informação na ARPE é um compromisso coletivo e uma responsabilidade compartilhada que perpassa todos os níveis da Agência. Para garantir a efetividade desta Política e a proteção adequada dos ativos de informação, é fundamental que os papéis e as responsabilidades sejam claramente definidos e compreendidos por todos. A estrutura de governança a seguir estabelece as principais atribuições de cada agente no processo de gestão da segurança da informação:

Diretoria Colegiada: Aprovar a PSI e prover os recursos para sua implementação.;

Coordenação de Tecnologia da Informação (CTI): Implementar e gerenciar os controles técnicos de segurança;

Encarregado pelo Tratamento de Dados Pessoais (DPO): Orientar sobre práticas de proteção de dados pessoais, incluindo dados pessoais sensíveis, e atuar como canal com os titulares e a ANPD;

Gestores: Garantir a aplicação da PSI em suas áreas, gerenciar os riscos específicos de seus processos e informar à CTI a necessidade de retirada de acesso de usuários desligados do ambiente de trabalho, bem como comunicar qualquer indício de incidente; e

Todos os Colaboradores e Usuários: Cumprir a PSI, proteger as credenciais de acesso e reportar incidentes. Estendendo-se àqueles que realizam tratamento em nome da ARPE ou quem quer que tenha acesso a dados ou informação no ambiente da Agência.

8.1. Compete à Diretoria Colegiada

- Aprovar a Política de Segurança da Informação, bem como suas alterações e atualizações; e
- Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da ARPE, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados.

8.2. Compete à Coordenadoria de Tecnologia da Informação

- Participar ativamente da elaboração e propor atualizações para a Política de Segurança da Informação (PSI) e suas normas complementares, garantindo que reflitam as necessidades tecnológicas e as melhores práticas de mercado;
- Avaliar soluções, ferramentas e processos de segurança da informação propostos por outras áreas ou pelo Gestor de Segurança; Implementar, gerenciar e monitorar as técnicas de segurança da infraestrutura de TI da ARPE;
- Acompanhar e monitorar o ciclo de vida das vulnerabilidades, buscando identificá-las, visando aplicar as correções e realizar atualizações possíveis de segurança nos sistemas e softwares;
- Administrar e revisar os controles de acesso lógico aos sistemas e dados, em conformidade com o princípio do menor privilégio;
- Executar e testar as rotinas de cópias de segurança (backup) e os planos de recuperação de desastres, visando garantir a disponibilidade e a integridade das informações;
- Monitorar continuamente as redes, sistemas e fluxos de dados para detectar atividades suspeitas, anomalias, artefatos maliciosos e possíveis ataques cibernéticos;
- Documentar e elaborar relatórios sobre os incidentes de segurança, analisando a causa raiz e recomendando melhorias para prevenir futuras ocorrências;
- Promover benchmarking com outras equipes e organizações, e representar a ARPE em fóruns, grupos de trabalho e redes de colaboração sobre segurança e resposta a incidentes; e
- Conduzir ou apoiar a realização de treinamentos e campanhas de conscientização sobre os aspectos técnicos da segurança da informação para os demais colaboradores.

8.3. Compete ao Coordenador de Tecnologia da Informação

- Coordenar a elaboração da PSI e das normas internas de segurança da informação da Agência, observadas a legislação vigente e as melhores práticas sobre o tema;

- Assessorar a Diretoria Colegiada na implementação da Política de Segurança da Informação;
- Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão; e
- Incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação; Propor soluções necessárias à manutenção da segurança da informação; Acompanhar os trabalhos de prevenção, tratamento e resposta a incidentes cibernéticos; e Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

8.4. Compete ao DPO

Compete ao Encarregadopelo Tratamentodos Dados Pessoais,dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD):

- Conduzir o diagnóstico de privacidade;
- Orientar, no que couber, os gestores proprietários dos ativos de informação; e
- Planejar e implementar a melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

9. Monitoramento e Revisão da PSI

9.1. Monitoramento

AARPE deverá manter mecanismos de controle e avaliação das práticas relacionadas à segurança da informação. O monitoramento será conduzido pela CTI com o apoio da Unidade de Controle Interno.

9.2. Revisão da PSI

Esta PSI deverá ser revisada a cada 3 anos ou sempre que ocorrerem:

- Alterações significativas no ambiente tecnológico;
- Mudanças nas legislações aplicáveis; e/ou
- Identificação de falhas relevantes nos controles de segurança.

A revisão será conduzida pela CTI e aprovada pela Diretoria Colegiada, com representantes das áreas técnicas e jurídicas, se necessário. A Política atualizada será disponibilizada no ambiente institucional da ARPE, bem como no seu sítio eletrônico, garantindo o acesso a todos os servidores e colaboradores.

10. Descumprimento e Sanções

O descumprimento das diretrizes estabelecidas nesta Política e em seus documentos complementares poderá resultar na aplicação de sanções administrativas, disciplinares ou contratuais, conforme a natureza de infração. As sanções poderão ser aplicadas sem prejuízo das demais responsabilidades nas esferas civil e criminal, nos termos da legislação vigente.

11. Referências

Lei nº 13.709/2018 (LGPD) – Lei Geral de Proteção de Dados Pessoais;
Lei nº 12.965/2014 – Marco Civil da Internet e seu regulamento (Decreto nº 8.771/2016);
ABNT NBR ISO/IEC 27001 e 27002 – Normas de gestão de segurança da informação;
Portaria GSI/PR nº 93/2021 – Estabelece requisitos de segurança da informação no âmbito da Administração Pública Federal; e
Normativos da SCGE/PE – Instruções e diretrizes de controle interno e gestão de riscos no âmbito estadual.

ARPE
AGÊNCIA DE REGULAÇÃO DE PERNAMBUCO

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA