NPC **0301 - POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA**

TECNOLOGIA DA INFORMAÇÃO

Versão 15 de 15/10/2025

1. INTRODUÇÃO

A capacidade tecnológica da Copel não constitui um fim em si mesma. Ela está a serviço da estratégia corporativa e, por isso, exige condições que transcendem a simples aplicação de recursos tecnológicos.

1.1 - ESCOPO

A Política de Tecnologia da Informação e Segurança Cibernética estabelece os princípios e diretrizes que orientam a organização de pessoas, processos, dados e ferramentas, com o objetivo de gerar valor sustentável para os negócios através de uma atuação integrada, segura, eficiente e alinhada às boas práticas de gestão, inovação e conformidade.

1.2 - CONCEITOS

Os termos utilizados nessa política estão conceituados e organizados no Caderno de Conceitos que pode ser acessado no Portal de Sustentabilidade da Copel ou no site de Relações com Investidores.

1.3 - PROPÓSITO

Estabelecer os princípios e diretrizes que orientam a gestão estratégica da Tecnologia da Informação, Segurança da Informação e Cibernética, Governança de Dados e Inteligência Artificial (IA) aplicada, assegurando o uso eficiente e responsável dos ativos tecnológicos da Companhia.

Promover a geração de valor para o negócio por meio da transformação digital, da gestão efetiva de riscos, da proteção das informações corporativas e demais ativos digitais, e do fomento à inovação tecnológica. Também busca assegurar que os investimentos e iniciativas em tecnologia estejam alinhados ao Planejamento Estratégico, em conformidade com as melhores práticas de governança, segurança, privacidade de dados e resiliência operacional.

Esta política aplica-se à Companhia Paranaense de Energia - Copel (Holding), às suas subsidiárias integrais - Sis (diretas e indiretas) e controladas (diretas e indiretas), respeitados os seus trâmites societários. Também é aplicável,como recomendação, às controladas em conjunto, às empresas coligadas e a outras participações societárias, respeitados os seus trâmites societários.

1.4 - PRINCÍPIOS

a) **Confidencialidade**: garantir que todo acesso à informação seja disponibilizado apenas para as entidades oupessoas devidamente autorizadas pelo proprietário da informação.
b) **Integridade:** garantir que as informações sejam precisas, completas e protegidas de alterações indevidas durante o seu ciclo de vida no que tange às características de confidencialidade, disponibilidade e rastreabilidade.
c) **Disponibilidade:** garantir que toda informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitarem.
d) **Rastreabilidade:** garantir o acompanhamento das operações nos processos da Companhia, conforme mapeamento de criticidade, visando a identificação de qualquer tipo de alteração da informação.
e) **Privilégios mínimos:** garantir que as pessoas, os sistemas de informação e os processos acessem apenas as informações necessárias à execução de suas atividades.
f) **Exposição mínima:** garantir que a informação seja mantida protegida, sendo exposta apenas quando necessária.
g) **Dever de diligência:** todos os profissionais da Companhia (administradores, empregados, estagiários, aprendizes e terceiros), são corresponsáveis pela preservação e pelo cumprimento das políticas de segurança da informação e cibernética da Copel, realizando todo acesso e uso da informação de forma responsável e regular.
h) **Conformidade:** garantir que os processos da Companhia estejam de acordo com normativas internas e externas, seguindo de forma rigorosa protocolos exigidos em decorrência atividades realizadas.

i) **Autenticidade:** garantir integridade da informação desde sua fonte legítima até uso final.

j) **Não repúdio e responsabilidade:** garantir que a origem de qualquer ação no sistema possa ser verificada e associada a uma pessoa.

k) **Governança de Dados:** garantir que todos os dados sejam tratados como ativos, com uma governança visando a qualidade, segurança e uso adequado em toda a organização.

l) **Ética:** garantir o uso ético e seguro da Inteligência Artificial (IA) e dos demais ativos tecnológicos.

2. DIRETRIZES

2.1 - Os recursos de Tecnologia da Informação sob a responsabilidade da Companhia devem ser utilizados de forma otimizada, segura, ética e sustentável, abrangendo infraestrutura, sistemas, dados, pessoas e serviços. Seu uso deve estar alinhado ao Planejamento Estratégico e restrito aos interesses corporativos, sendo vedado qualquer uso em benefício próprio ou de terceiros, conforme previsto no Código de Conduta da Companhia.

2.2 - Todos os colaboradores da Copel devem proteger os ativos digitais da companhia de acordo com sua criticidade e relevância para os negócios, adotando práticas seguras e responsáveis no uso e no acesso às informações.

2.3 - Todas as decisões sobre aquisição, uso ou descontinuação de recursos tecnológicos devem considerar uma visão de longo prazo com critérios de desempenho, segurança, privacidade, escalabilidade, portfólio de produtos e projetos, custo-benefício, impacto ambiental, sustentabilidade e aderência às políticas corporativas vigentes da Copel.

2.4 - Estabelecer e manter processos de TI atualizados com base nas melhores metodologias do mercado, definindo de forma clara os papéis, responsabilidades e fluxos operacionais, promovendo maior eficiência, transparência e previsibilidade nas entregas e contribuindo para a redução de riscos operacionais, melhor uso dos recursos e aumento da confiança das áreas de negócio na TI como parceiro estratégico.

2.5 - Gerenciar os ativos de TI de forma a atender satisfatoriamente os serviços da Copel, fornecendo recursos e mantendo uma gestão e controle patrimonial e contábil atualizados.

2.6 - Assegurar a sustentação e continuidade do conhecimento por meio de seus sistemas e bases de dados corporativas, a fim de registrar, organizar, preservar e facilitar o acesso ao conhecimento gerado na empresa, garantindo sua disponibilidade para apoiar os negócios estratégicos da Copel.

2.7 - Estabelecer princípios e práticas que integrem os valores de *Environmental, Social and Governance* - ESG às atividades de Tecnologia da Informação, promovendo inovação responsável, ética digital, impacto positivo na sociedade e valor aos negócios.

2.8 - Assegurar a confidencialidade, integridade e disponibilidade das informações, sistemas e serviços, implementando controles técnicos e organizacionais adequados conforme o nível de risco.

2.9 - Adotar um modelo de maturidade em Segurança Cibernética, visando a defesa, mitigação de riscos, fortalecimento da resiliência organizacional e aumento da confiança de clientes, parceiros e reguladores.

2.10 - Assegurar a rastreabilidade de alterações e acessos a informações críticas durante o desenvolvimento ou aquisição de aplicativos, em conformidade com requisitos de segurança, auditoria, privacidade de dados e governança corporativa.

2.11 - Gerenciar riscos cibernéticos de forma contínua, identificando, analisando e tratando os riscos relacionados a ameaças digitais, falhas tecnológicas, acesso indevido, vazamento de dados e interrupções operacionais, com foco na mitigação proativa.

2.12 - Desenvolver um ambiente organizacional que habilite a Copel a identificar e gerenciar os riscos associados à segurança da informação e cibernética, à governança de dados e ao uso de Inteligência Artificial (IA) no que tange a sistemas, processos, pessoas, ativos, dados e recursos.

2.13 - Desenvolver a cultura de segurança da informação e cibernética por meio da conscientização dos administradores, empregados, estagiários, aprendizes e terceiros e disponibilização de meios para detecção e comunicação dos riscos à área de segurança da informação.

2.14 - Estabelecer e implementar um Plano de Resposta à Incidentes de Segurança da Informação e Cibernética, contemplando o monitoramento de eventos, identificação de ameaças e resposta rápida a incidentes, com registro, comunicação, contenção e análise pós-incidente.

2.15 - Realizar a gestão e revisão periódicas das identidades e dos acessos aos recursos computacionais da Copel, garantindo a definição de privilégios mínimos e rastreabilidade de acessos realizados.

2.16 - Desenvolver e implementar planos de resiliência a fim de restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança da informação e cibernética.

2.17 - Revogar o acesso do colaborador no caso de desligamento, mudança de função ou departamento, término de contrato, inatividade prolongada ou risco de segurança da informação.

2.18 - Implementar um Programa de Segurança da Informação e Cibernética para acompanhar as atividades corretivas e/ou preventivas nos processos sob sua responsabilidade.

2.19 - Estabelecer controles de segurança como parte integrante do processo de desenvolvimento, aquisição e vida útil dos aplicativos para assegurar que as informações processadas estejam protegidas, de acordo com sua classificação e exposição a risco.

2.20 - Gerenciar os riscos de Segurança da Informação em todo o ciclo de vida do relacionamento com fornecedores e prestadores de serviços, estabelecendo os requisitos mínimos de segurança aplicáveis. Estes requisitos serão baseados em avaliações de risco periódicas, implementação de mecanismos de proteção e defesa cibernética, aderência às políticas e controles de segurança vigentes, incluindo a realização de treinamentos e ações de conscientização, e a obrigação de gestão e reporte tempestivo de quaisquer incidentes de segurança da informação e cibernética que possam impactar a Companhia.

2.21 - Elevar continuamente os níveis de segurança, provendo melhoria contínua nos ambientes e sistemas da Copel.

2.22 - Garantir que a Inteligência Artificial (IA) generativa seja usada de maneira ética, respeitando rigorosamente a privacidade de dados e assegurando que informações críticas, pessoais ou confidenciais não sejam expostas sem autorização.

2.23 - Estabelecer controles necessários para o uso de IA nos ambientes e sistemas da Copel, garantindo a sua rastreabilidade e protegendo de manipulação de dados e vazamento de dados críticos.

2.24 - O colaborador deverá utilizar a IA em ambientes controlados, seguros e autorizados pela área de Tecnologia da Informação, respeitando os processos de privacidade e segurança, além das normas vigentes na Copel.

2.25 - Qualquer pessoa, independente do cargo, função ou local de trabalho será responsabilizada pelo descumprimento ou violação da presente política, mediante gestão de consequências a ser realizada pela companhia em acordo com as normativas internas e externas vigentes.

3. LEGISLAÇÃO ESPECÍFICA RELACIONADA AO ASSUNTO

A legislação e regulamentação que afeta diretamente as Políticas Corporativas da Copel estão organizadas no Caderno Legislação de Referência, que pode ser acessado no Portal de Sustentabilidade da Copel ou no site de Relações com Investidores.

Atualiza a NPC 0301 de 28/05/2024 e incorpora o conteúdo da NPC 0302 - Política de Tecnologia da Informação, de mesma data.

NPC 0301 aprovada pela 267ª Reunião Ordinária do Conselho de Administração - ROCAD, de 15/10//2025.