REVISÃO E APROVAÇÃO

Esta Política foi aprovada em Reunião do Conselho de Administração da ENEVA, realizada em 20/03/2025, e qualquer alteração ou revisão deverá ser a ele submetido.

Revisão	Data	Descrição das Atualizações
00	20/03/2025	Criação do documento

Criação	Revisão	Aprovação
Ruan Campos Analista de Governança de TI	**Alexandre Ferreira** Diretor de TI **Leonardo S. Oliveira** Coordenador de Cibersegurança	**Diretoria Executiva** **Conselho de Administração**

ÍNDICE

1. OBJETIVO

Este documento objetiva estabelecer os princípios da Eneva relacionados à Segurança da Informação para a parte de Tecnologia da Informação (TI) e Tecnologia Operacional (TA/OT), de modo a orientar os colaboradores, fornecedores e terceiros quanto às boas práticas acerca do tema, considerando também tópicos de comportamento seguro, visando proteger a organização e as informações de sua propriedade e/ou sob sua guarda.

2. APLICAÇÃO

Este documento aplica-se a todas as áreas que compõem a estrutura organizacional da Eneva, incluindo SPE's, joint ventures e sociedades coligadas em que o controle seja exercido pela Eneva.

Nos demais casos, o conteúdo deste documento deve ser levado ao conhecimento de seu(s) parceiro(s) de negócios para análise da pertinência de implementação integral ou parcial.

3. REFERÊNCIAS

- **PL.CRP.CMP.002** – Código de Conduta Eneva
- **DT.CRP.TIN.001 –** Diretriz de Segurança da Informação
- **DT.CRP.TIN.002 –** Diretriz Corporativa de Tecnologia da Informação
- **DT.CRP.GOV.004 –** Diretriz de Classificação da Informação
- **DT.CRP.GOV.005 -** Diretriz de Privacidade e Proteção de Dados
- **PR.CRP.GOV.009 –** Resposta a Incidentes de Segurança com Dados Pessoais
- **PR.CRP.GOV.012 –** Procedimento de Retenção e Descarte de Dados Pessoais
- **FL.CRP.TIN.004 -** Termo de Comodato - Equipamentos de Informática

4. DEFINIÇÕES

- **Ameaça:** Evento que tem potencial em si próprio para comprometer os objetivos da organização, seja por meio de danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas.
- **Ativo:** Todo e qualquer bem, tangível ou intangível, pertencente, administrado ou de responsabilidade da Eneva.
- **Ativo de Tecnologia da Automação (TA/OT):** Incluem, mas não se limitam à, equipamentos, instrumentos e controladores utilizados no processo de produção como, por exemplo: servidores industriais, *switches* de rede industriais, PLC's, sensores, atuadores, fontes de alimentação, dentre outros.

- **Confidencialidade:** Propriedade da informação que determina que a informação não esteja disponível ou não seja revelada a indivíduos, entidades ou processos não autorizados, sendo acessada apenas por aqueles estritamente autorizados pelo respectivo responsável.
- **Dado Pessoal:** Qualquer informação relacionada a pessoa natural identificada ou identificável.
- **Disponibilidade:** Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário correspondente.
- **Dispositivos de TI:** Equipamentos de processamento de informação que têm a capacidade de armazenar dados, estabelecer conexões e interagir com outros sistemas e/ou redes, além de ter a característica da mobilidade. Exemplos: aparelhos de telefone celular, iPhone, HD externo, rádio, etc.
- **Colaborador:** Todo e qualquer indivíduo que faz parte do quadro funcional da Eneva. Incluem-se neste grupo: funcionários, contratados, estagiários e jovens aprendizes.
- **Informação:** Ativo tangível ou intangível, de valor para a organização. Pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por e-mail ou por outros meios, exibida em vídeos ou falada em conversas.
- **Integridade:** Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (criação, armazenamento e descarte).
- **Prestador de Serviço (Fornecedor) e/ou Terceiro:** Pessoa física ou jurídica que oferece e realiza um conjunto específico de atividades para a Eneva em troca de pagamento, mediante acordo contratual ou de prestação de serviços, com estabelecimento de termos, condições, escopos e prazos.
- **Risco:** Combinação da probabilidade da ocorrência de um evento e o impacto deste, caso ocorra.
- **Segurança da Informação (SI):** Conjunto de ações e controles que objetivam garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, de modo a contribuir para o cumprimento dos objetivos estratégicos da Companhia.
- ***ServiceNow:*** Portal de Soluções Eneva, visando a resolução de problemas e irregularidades, abertura de chamados e gerenciamento de fluxos de trabalho.
- **Tecnologia Operacional (OT):** Uso de *hardware* e *software* para monitorar e controlar processos físicos, dispositivos e infraestrutura.

5. PRINCÍPIOS E DIRETRIZES

A finalidade desta Política é determinar os controles necessários para implementação e manutenção da gestão de Segurança da Informação, bem como o comportamento esperado de todos os envolvidos.

A proteção da informação disponível na organização contra possíveis ameaças, vulnerabilidades e/ou vazamentos é fundamental para o atingimento dos direcionamentos estratégicos, regulamentações/leis vigentes, melhores práticas e os objetivos de negócio da Eneva.

5.1 Gestão da Segurança da Informação e Ativos

- A gestão da segurança da informação é responsabilidade de todos aqueles que utilizam algum sistema e/ou tem acesso a qualquer informação disponível na Eneva, sendo devidamente coordenada pela equipe de Segurança da Informação.
- A gestão será orientada por meio desta Política e com base nas melhores práticas de mercado e procedimentos de segurança da informação recomendados pelos órgãos e entidades responsáveis pelo estabelecimento dos devidos padrões relacionados à Segurança da Informação.
- A informação será sempre considerada um ativo de valor para organização, o qual, consequentemente, deve ser adequadamente protegido.
- A equipe de Segurança da Informação é responsável pela proteção dos ativos contra possíveis ameaças, de modo a garantir a continuidade dos negócios, minimizando possíveis danos e maximizando o retorno dos investimentos e as oportunidades de negócio.
- De modo a garantir a aderência perante a realidade da Companhia, este documento poderá ser atualizado pela equipe de Segurança da Informação a qualquer momento, caso a Diretoria entenda ser necessário/aplicável, devendo esta atualização ser submetida ao Conselho de Administração.
- A organização promoverá a disseminação dos princípios desta Política por meio de programas de conscientização e capacitação, visando fortalecer a cultura da Segurança da Informação, incluindo, por exemplo: campanhas periódicas, treinamentos, simulações de phishing, dentre outros.
- Periodicamente, devem ser realizados testes e/ou avaliações de vulnerabilidade. No caso das redes de OT, é importante que estas atividades sejam devidamente planejadas, uma vez que podem comprometer a segurança e disponibilidade do sistema.
- As configurações dos ativos devem ser aderentes aos padrões de segurança estabelecidos por esta Política, incluindo o devido suporte, mediante processo de identificação e remediação de vulnerabilidades.

- Todos os funcionários e prestadores de serviços são responsáveis diretos pela utilização segura e adequada dos ativos sob sua responsabilidade.
- A equipe de Segurança da Informação será a responsável pelo estabelecimento e coordenação do processo de melhoria necessário, de modo a abranger todas as mudanças que possam ocasionar impacto associado à Segurança da Informação na Companhia (TI e TA).
- O funcionário é diretamente responsável pelo uso dos computadores, periféricos e demais itens que lhe forem disponibilizados, devendo respeitar e zelar pela marca, imagem e reputação da Companhia, utilizando-os com responsabilidade e cautela, visando proteção física e lógica destes.

5.2 Gerenciamento de Riscos, Ameaças e Vulnerabilidades

- Possíveis riscos e/ou ameaças identificadas pelos funcionários devem ser notificados, de forma imediata, ou sem demora indevida, à equipe de Segurança da Informação.
- Possíveis incidentes e/ou irregularidades devem ser reportados, de forma imediata, ou sem demora injustificada, mediante abertura de chamado no Portal de Soluções, no item de catálogo específico para tal fim (“Relatar Incidente de Segurança”), localizado na aba de Segurança da Informação.
- Caso seja identificado que o incidente envolve dados pessoais, é importante que o caso também seja reportado, tempestivamente, junto ao Encarregado pelo Tratamento de Dados Pessoais, por meio do e-mail:dpo@eneva.com.br, para as devidas tratativas e direcionamentos.
- O gerenciamento de vulnerabilidades e ameaças deve apoiar a Gestão de Riscos da Companhia, de forma proativa, de modo a reduzir a probabilidade e materialização dos riscos e seus impactos.

5.3 Monitoramento e Classificação da Informação

- Os dados e informações criados nos recursos dos ativos da Eneva são de sua propriedade e devem ser utilizados somente pelas pessoas devidamente autorizadas e/ou responsáveis, exclusivamente, no exercício de suas atividades junto à empresa, para atendimento dos objetivos do negócio.
- Os softwares adquiridos e/ou desenvolvidos internamente pertencem exclusivamente à Eneva, considerando o seu período de vigência e/ou duração de contrato.
- É vedada a cópia e/ou disponibilização de quaisquer recursos, dados, materiais, equipamentos, informações tecnológicas e/ou segredos comerciais pertencentes à Eneva,

em qualquer meio (eletrônico ou físico), para ambientes externos sem a prévia e devida autorização.

- Todas as informações devem ter um proprietário associado (mesmo que indiretamente) e ser devidamente classificadas quanto ao seu nível de confidencialidade, sempre que possível e permitido pelo ativo/software utilizado, de modo a garantir a proteção adequada destas, conforme estabalecido no **Normativo DT.CRP.GOV.004 – Diretriz de Classificação da Informação.**
- A Eneva **não recomenda** o armazenamento de dados pessoais nas Pastas/Drivers da Rede Corporativa. Dessa forma, também não se responsabiliza por nenhum dado pessoal que tenha sido incluído na Rede diretamente pelo funcionário.
- Os equipamentos, meios de comunicação e sistemas da Eneva estão sujeitos a monitoramento, sempre que autorizado pela área de Compliance, visando garantir maior robustez e proteção às informações da Companhia.
- A proteção das informações deve contemplar todo o ciclo de vida destas, incluindo: geração, acesso, utilização, armazenamento, compartilhamento e descarte.

5.4 Gestão de Acessos

- Todos os acessos aos sistemas e ativos devem ser gerenciados e controlados, considerando aprovações necessárias (Gestor Responsável e/ou Owner do Sistema) e as devidas evidenciações, para fins de formalização, histórico e/ou solicitações de Auditoria.
- Senhas devem ser armazenadas de maneira segura e, sempre que possível, é recomendado o uso da autenticação multifator, como medida adicional de segurança.
- Permissões para administradores devem ser exclusivos e utilizados apenas para atividades que, de fato, necessitam deste tipo de privilégio.
- A concessão de acessos obedecerá, sempre, os padrões adequados de segregação de funções, bem como ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação estritamente necessários para o pleno desempenho de suas atividades e devidamente autorizados.
- Acessos remotos no ambiente da Eneva devem ser realizados por meio de rede segura (VPN, antivírus e *firewall*) e, sempre que possível, utilizar duplo fator de autenticação.

5.5 Segurança Cibernética e Continuidade de Negócios

- Os processos críticos devem ser suportados pelo processo de Continuidade de Negócios, de modo a garantir o devido desempenho destes nas operações de recuperação.
- Todos os empregados da Eneva devem manter os sistemas e softwares de proteção de seus

ativos devidamente atualizados, sinalizando à equipe de Segurança da Informação qualquer anormalidade ou falha nos ativos.

- Toda e qualquer concepção e/ou desenvolvimento de novos processos, projetos e sistemas deve considerar os aspectos de Segurança da Informação e de proteção de dados, contemplando todas as fases do ciclo de vida.
- A Internet deve ser utilizada apenas para fins relacionados ao trabalho, sendo proibido o acesso à conteúdos que possam ferir o Código de Conduta, Políticas e Diretrizes da Companhia, incluindo, mas não se limitando à: downloads, pornografia, atividades ilegais, jogos de azar,conteúdos difamatórios/caluniosos, dentre outros. **Ativos de Tecnologia da Automação (TA/OT) não devem possuir conexão à Internet.**
- O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra, de modo a evitar possíveis fragilidades de segurança. A porta USB é um dos principais pontos de vulnerabilidade, podendo ser usada para vazamento de informações sensíveis e/ou instalação de vírus.
- No caso do ambiente de Tecnologia Operacional (TA/OT), o uso de mídias removíveis, se necessário, deve ser analisado no que tange a códigos maliciosos **antes do uso.** Ademais, só devem ser permitidas mídias da Eneva destinadas para esse uso/finalidade. **Possíveis exceções devem ser autorizadas e documentadas.**
- O empregado é responsável exclusivo pelo uso de suas respectivas senhas de acesso, as quais devem ser individuais, instransferíveis e sigilosas. Além disso, é importante que estas sigam os padrões mínimos exigidos pelos sistemas, serviços e dispositivos da Eneva, conforme detalhado no **Normativo DT.CRP.TIN.001 – Diretriz Corporativa de Segurança da Informação.**

5.6 Gestão de Fornecedores

- Todos os Fornecedores e terceiros devem estar cientes do conteúdo desta Política e devem cumprir com os procedimentos e diretrizes aqui estabelecidos.
- Todos os Fornecedores e terceiros devem utilizar as melhores práticas de segurança, conforme órgãos específicos do setor e instituições reconhecidas (por exemplo: NIST, ISO), de modo a garantir o fornecimento adequado dos serviços acordados.
- O acesso remoto aos ativos e sistemas da Eneva por parte dos Fornecedores e/ou terceiros na rede do ambiente de OT somente poderá ocorrer após autorização formal e deverá ser utilizado única e exclusivamente para realização das atividades acordadas junto à organização.

5.7 Proteção de Dados Pessoais

- A organização deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais.
- A organização deverá adotar as medidas de segurança aptas a proteger os dados pessoais contra acesso não autorizado, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito, **em observância a Lei Federal nº 13.709/2018** (Lei Geral de Proteção de Dados Pessoais ou LGPD) e demais normativas internas aplicáveis.
- Possíveis incidentes e/ou irregularidades envolvendo dados pessoais devem ser comunicados à Encarregada pelo Tratamento de Dados Pessoais (DPO), por meio do canal ***Eneva - Fazer manifestação (contatoseguro.com.br)***.

6. RESPONSABILIDADES

As informações tratadas nos processos da Eneva podem ser utilizadas por todos aqueles envolvidos nas operações internas. Sendo assim, é responsabilidade de todos proteger os bens, informações e recursos da Companhia aos quais possuem acesso de acordo com as suas funções, bem como o cumprimento das demais normativas atreladas a essa Política.

6.1 Equipe de Segurança da Informação

- Estar ciente e manter-se atualizado com essa Política e demais normativas internas complementares.
- Proteger os ativos contra possíveis ameaças, de modo a garantir a continuidade dos negócios. minimizando possíveis danos e maximizando o retorno dos investimentos e as oportunidades de negócio.
- Realizar testes e/ou avaliações de vulnerabilidades periódicos e planejados.
- Estabelecer e coordenar os processos de melhorias de seguranca da informação necessários.

6.2 Terceiros/Prestadores de Serviços

- Estar ciente e manter-se atualizado com essa Política.
- Comunicar a ocorrência ou a suspeita de ocorrência de incidentes e/ou irregularidades, imediatamente ou sem demora injustificada à Equipe de Segurança da Informação e/ou ao Encarregado de Dados Pessoais (DPO), quando aplicável.
- Atuar em observância às melhores práticas de segurança da informação e proteção de dados pessoais.

6.3 Colaboradores

- Estar ciente e manter-se atualizado com essa Política e demais normativas internas complementares.
- Comunicar a ocorrência ou a suspeita de ocorrência de incidentes e/ou irregularidades, imediatamente ou sem demora injustificada à Equipe de Segurança da Informação e/ou ao Encarregado de Dados Pessoais (DPO), quando aplicável.
- Utilizar os ativos disponibilizados pela Eneva com cautela, de forma a respeitar e zelar pela marca, imagem e reputação da Companhia, bem como pela proteção física e lógica dos ativos.
- Manter os sistemas e softwares utilizados devidamente atualizados, informando a Equipe de Segurança da Informação qualquer situação irregular ou falha nos ativos.
- Utilizar senhas fortes, de forma individual, intransferível e sigilosa, em observância às normativas internas da Eneva.

6.4 Encarregado pelo Tratamento de Dados Pessoais (DPO)

- Receber os comunicados a respeito de ocorrência ou suspeita de incidentes ou irregularidades, e dar as devidas providências de acordo com o Procedimento de Resposta a Incidentes, acionando a equipe de Segurança da Informação, quando aplicável.
- Garantir que o tratamento de dados pessoais tenha o mesmo nível de proteção que as informações classificadas como confidenciais.

7. DISPOSIÇÕES GERAIS

Esta Política de Segurança da Informação (TI e TA) é complementada por meio das Diretrizes de Segurança da Informação e Tecnologia da Informação (DT.CRP.TIN.001 e DT.CRP.TIN.002, respectivamente), bem como outros procedimentos/manuais internos e atividades/treinamentos de conscientização, focados no tema de segurança (por exemplo: phishing, newsletter, dentre outros).

Esta Política deve estar sempre disponível e acessível para todos os colaboradores, bem como Fornecedores e terceiros, de modo a garantir o cumprimento integral dos tópicos aqui abordados.

Este Normativo (bem como demais documentos relacionados e aplicáveis) será continuamente atualizado, seja por necessidade identificada diretamente pela Companhia (estratégia e/ou regras de negócio) ou por implicações regulatórias, de conformidade e/ou de Auditoria, visando garantir os devidos alinhamentos frente às melhores práticas e regulamentações vigentes.

Eventuais violações a qualquer aspecto desta Política sujeitará o infrator a ações

administrativas e/ou disciplinares pertinentes, podendo este ser responsabilizado administrativa, civil e/ou criminalmente.

Qualquer dúvida, comportamento e/ou situação anormal que possa gerar conflito com esta Política deve ser comunicado à equipe de Segurança da Informação, de forma imediata ou sem demora injustificada, por meio do endereço do **e-mail *service.desk@eneva.com.br*** ou no **Portal de Soluções.**

Assim como a ética, a segurança da informação deve ser entendida e aplicada como parte fundamental da cultura interna da Eneva e pilar imprescindível para o atingimento dos objetivos da Companhia.