POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

1 . Política de TI

A Política de Tecnologia da Informação estabelece as diretrizes corporativas da Companhia Campolarguense de Energia – Cocel para garantir o uso eficiente, seguro e ético dos recursos de Tecnologia da Informação (TI), bem como para proteger os ativos digitais, a privacidade, a integridade e a disponibilidade das informações da Cocel.

Tem por finalidade orientar todos os usuários quanto à adequada utilização dos recursos tecnológicos e prevenir riscos operacionais, legais e reputacionais, devendo ser observada e aplicada em todas as áreas da Companhia.

2. Objetivo

Estabelecer diretrizes que permitam aos empregados, aprendizes, estagiários e prestadores de serviço que utilizem recursos de Tecnologia da Informação da Companhia, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como, a implementação de controles e processos para seu atendimento.

Preservar as informações da Companhia Campolarguense de Energia - Cocel quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

3. Abrangência

As diretrizes estabelecidas nesta Política deverão ser observadas por todos os empregados, aprendizes, estagiários e prestadores de serviço que utilizem recursos

de Tecnologia da Informação da Companhia, aplicando-se às informações em qualquer meio ou suporte.

Para fins desta Política, todas essas categorias serão conjuntamente denominadas "usuários".

4. Responsabilidades

Dos Empregados, Aprendizes e Estagiários

Para fins desta Política, consideram-se:

- empregados: pessoas físicas contratadas sob o regime da CLT;
- aprendizes: contratados nos termos da legislação específica;
- estagiários: contratados nos termos da Lei nº 11.788/2008.

As disposições desta Política aplicam-se aos empregados, aprendizes, estagiários e prestadores de serviço que utilizem recursos tecnológicos da Companhia, observada a natureza do vínculo jurídico de cada categoria.

Será de inteira responsabilidade de cada usuário, todo prejuízo ou dano que vier a sofrer ou causar a Companhia Campolarguense de Energia - Cocel e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

- Uso dos equipamentos: computadores (CPUs), monitores e periféricos (teclado, mouse, leitores, pendrives) devem ser corretamente conectados e bem utilizados, de acordo com orientações da Divisão de Informática.
- Formas de acesso: acessar a rede de COCEL apenas para fins relacionados ao trabalho e de acordo com os acessos a sistemas previamente liberados pela Divisão de Informática, sem tentativas de acesso a áreas não permitidas.
    - A viabilidade de permissão para acesso externo aos sistemas da Cocel será avaliada e configurada por um empregado da Divisão de Informática.
    - A utilização de pendrives e outros equipamentos ou sistemas para leitura e armazenamento externo de dados (fora da rede da Cocel) deve ocorrer com a autorização de um empregado da Divisão de Informática.
- Uso dos aplicativos: devem ser utilizados somente os aplicativos instalados localmente no computador ou com acesso externo configurado por um empregado da Divisão de Informática, sendo proibida a instalação de qualquer outro aplicativo sem a autorização daquela Divisão.
- Uso do e-mail da COCEL: deve ser utilizado somente para fins profissionais, evitando o uso particular. Deve-se ter prudência ao abrir qualquer mensagem suspeita e, em caso de dúvida sobre a integridade da mensagem, deve-se entrar em contato com a Divisão de Informática.

Dos Gestores de Pessoas e/ou Processos

Os gestores devem manter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os empregados, aprendizes, estagiários e prestadores de serviço sob a sua gestão.

Os gestores devem assegurar, ainda na fase de contratação ou de formalização dos instrumentos contratuais de trabalho, estágio, aprendizagem, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta Política.

Os gestores devem exigir dos empregados a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Companhia Campolarguense de Energia - Cocel.

Antes de conceder aos empregados acesso às informações da instituição, os gestores devem exigir a assinatura do Acordo de Confidencialidade dos empregados casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Da Área de Tecnologia da Informação/ Divisão de Informática

- Deve testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Deve configurar os equipamentos, ferramentas e sistemas concedidos aos empregados com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política.
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Companhia Campolarguense de Energia - Cocel.
- Implantar controles que gerem registros auditáveis para retirada e transporte das informações custodiadas pela Divisão de Informática, nos ambientes totalmente controlados por ela.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Atribuir a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
  - os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

- os usuários (logins) de terceiros serão de responsabilidade do gestor do contrato.

- Deve proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Garantir, da forma mais rápida possível, após o recebimento de –solicitação formal dos gestores, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Ministrar, para todos os usuários, palestras orientativas e de reciclagem sobre segurança da informação.
- Divulgar aos usuários, na forma de e-mail, contato pessoal ou quadro de avisos, as diretrizes de segurança da informação e orientações sobre o correto uso dos ativos de informática.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

• uso da capacidade instalada da rede e dos equipamentos;

• tempo de resposta no acesso à internet e aos sistemas críticos;

• períodos de indisponibilidade no acesso à internet e aos sistemas críticos;

• incidentes de segurança (vírus, trojans, furtos, acessos indevidos, entre outros); e

• atividade de todos os usuários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5. Monitoramento, Auditoria do Ambiente e Resposta a Incidentes

Para garantir as regras mencionadas nesta Política, a Companhia Campolarguense de Energia - Cocel poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada

para identificar usuários e respectivos acessos efetuados, bem como, material manipulado;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; e/ou

• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Uso do e-mail/Correio eletrônico

É proibido aos usuários, no uso do e-mail/ correio eletrônico da Companhia Campolarguense de Energia - Cocel:

• enviar mensagem por correio eletrônico através do endereço de seu departamento ou usando o nome de usuário de outra pessoa ou, ainda, endereço de correio eletrônico que não esteja autorizado a utilizar;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a da Companhia Campolarguense de Energia - Cocel vulneráveis a ações civis ou criminais;

• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

• apagar mensagens pertinentes de correio eletrônico quando a —Companhia Campolarguense de Energia - Cocel estiver sujeita a algum tipo de investigação;e/ou

• produzir, transmitir ou divulgar mensagem que:

- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou, de qualquer forma, mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal.

Internet

Todas as regras atuais da Companhia Campolarguense de Energia - Cocel visam basicamente o desenvolvimento de um comportamento eminentemente ético e

profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Tecnologia da Informação e Segurança Cibernética.

Ao monitorar a rede interna, a Companhia pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao empregado e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Resposta a Incidentes de Segurança

A Companhia manterá procedimentos formais para tratamento de incidentes de segurança cibernética, observando as seguintes diretrizes:

- **Plano de Resposta:** desenvolver, manter e atualizar plano de resposta a incidentes de segurança cibernética;
- **Notificação:** todo incidente ou suspeita de incidente de segurança deverá ser comunicado imediatamente à Divisão de Informática;
- **Investigação e Auditoria:** os incidentes serão analisados de forma técnica, com apuração das causas, avaliação de impactos e definição de medidas corretivas e preventivas, visando evitar recorrências;
- **Registro:** os incidentes deverão ser formalmente registrados para fins de rastreabilidade e melhoria contínua.

6. Identificação

Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os usuários.

Todos os dispositivos de identificação utilizados na Companhia Campolarguense de Energia - Cocel, tais como: o número de registro do empregado, as identificações de acesso aos sistemas, os certificados e assinaturas digitais, e os dados biométricos, têm que estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Os usuários podem alterar a própria senha, e são orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Divisão de Recursos Humanos deverá imediatamente comunicar tal fato à Divisão de Informática, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como, aos usuários de testes e outras situações similares.

Caso o usuário esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à Divisão de Informática para cadastrar uma nova.

7. Treinamento e Conscientização

A Companhia promoverá treinamentos periódicos em segurança da informação e segurança cibernética, com o objetivo de fortalecer a cultura de proteção dos ativos informacionais.

Todos os usuários deverão participar das capacitações, que poderão abranger temas como prevenção a phishing e engenharia social, uso seguro de e-mail e internet, proteção de credenciais, tratamento adequado das informações e comunicação de incidentes.

A participação deverá ser devidamente registrada.

As ações de treinamento que envolvam tratamento de dados pessoais deverão observar a Política de Privacidade e Proteção de Dados da Companhia, em conformidade com a Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD).

8. Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Companhia Campolarguense de Energia - Cocel. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição. Sendo assim, todos os usuários que utilizem recursos de Tecnologia da Informação da Companhia devem estar cientes acerca desta Política, cumprindo as diretrizes que nela estão estabelecidas.

O responsável pela Politica de Tecnologia da Informação e Segurança Cibernética da Companhia Campolarguense de Energia – Cocel é o Sr. **Rubens Mazzon Junior**, Encarregado de Dados da empresa. Sendo que quaisquer assuntos relacionados às diretrizes estipuladas nesta Política, deverão ser reportados a ele.

RESPONSABILIDADES DE ELABORAÇÃO, VERIFICAÇÃO E APROVAÇÃO.

Elaboração/Revisão	Verificação	Aprovação
Camila Cristina Grassani Kaizu	Rubens Mazzon Junior	Conselho de Administração
Controladoria & Compliance	Encarregado de Dados da Cocel	Ata da 305ª Reunião realizada em 17/04/2026

DE ACORDO:

Samir Moussa	Henrique Gesser	Luciano Marcos Klos	Rafael Rogiski
Diretor Administrativo	Diretor Técnico	Diretor Econômico-Financeiro	Diretor-Presidente

ÍNDICE DE REVISÕES

Revisão	Data	Descrição
00	10/06/2022	Emissão inicial.
01	03/03/2026	Alterados termo “colaborador” para “empregado”; Incluídos estagiários, aprendizes e prestadores de serviços também como “usuários”; Reescritos itens: 1. Política de TI; 3. Abrangência; Incluído no item 5. Parágrafo sobre “Resposta a Incidentes de Segurança”. Incluído item 7. Treinamento e Conscientização.