POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

1.1. A Política de Segurança da Informação da Necta Gás Natural S.A. ("Necta") visa estabelecer as diretrizes que devem ser seguidas pelos Colaboradores e Terceiros garantir a observância às regras referentes ao tratamento e proteção das informações e ativos de informação, bem como assegurar a capacidade da Necta em garantir a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e responsabilidade, além de prevenir, detectar e reduzir riscos de segurança da informação e cibernética ("Política").

2. APLICAÇÃO E ABRANGÊNCIA

2.1. A presente Política aplica-se a todos os Colaboradores da Necta e suas Controladas, doravante em conjunto ou individualmente denominadas simplesmente de "Necta", bem como a Terceiros que realizarem o tratamento de informações ou utilizarem os ativos de informação da Necta.

3. DEFINIÇÕES

(i) **Ativo**: Segundo a norma ISO/IEC 27005 de Gestão de Riscos de Segurança da Informação, um ativo é qualquer coisa de valor para a organização e que precisa ser protegida. Isso inclui tanto elementos tangíveis, como equipamentos e infraestrutura, quanto intangíveis, como dados, informações e conhecimento;

(ii) **Ativos críticos do negócio** (CAN): são os ativos que garantem o funcionamento do negócio e são fundados nos pilares básicos da segurança - disponibilidade, integridade e confidencialidade. O não cumprimento de tais pilares, mesmo que momentaneamente, podem causar impactos à reputação e/ou ao faturamento da companhia e por este motivo devem possuir um suporte prioritário;

(iii) **Base de dados**: qualquer coleção de informações inter-relacionadas (estruturadas, não-estruturadas ou semiestruturadas), normalmente armazenadas eletronicamente em um sistema de computador.

(iv) ***Botnets***: é um grupo de computadores, máquinas ou dispositivos de internet das coisas ("IoT") que foram infectados por softwares maliciosos e podem ser controlados remotamente para executar ataques maliciosos.

(v) **Colaborador(es):** toda pessoa que mantém vínculo estatutário ou empregatício com a Necta. São os integrantes do Conselho de Administração, dos Comitês Estatutários ou não Estatutários e da

Diretoria Estatutária ou não Estatutária, bem como todos os empregados em tempo integral e temporário, empregados terceirizados e estagiários.

(vi) **Controladas:** empresas sobre as quais a Necta detém o controle de forma direta ou indireta.

(vii) **Dado Pessoal:** Qualquer informação relacionada a uma pessoa natural identificada ou identificável - ou seja, Dados que permitem identificar, ainda que indiretamente, a pessoa a qual eles pertencem. Exemplos: nome e sobrenome, foto, endereço de e-mail, número de afiliação da previdência social, dados de salário, registro de conexão etc.

(viii) **Dado Pessoal Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, Dado genético ou biométrico, quando vinculado a uma pessoa natural.

(ix) **Desenvolvimento de Software**: atividade de criar programas computacionais, executada por um desenvolvedor ou grupo de desenvolvedores;

(x) **Encarregado ("DPO"):** Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os Titulares e a Autoridade Nacional de Proteção de Dados;

(xi) ***Log***: termo técnico utilizado para descrever o registro das transações que ocorrem quando um software é utilizado;

(xii) ***Malwares***: variedade de formas de software hostil ou intruso que pode causar danos ao ambiente tecnológico;

(xiii) ***Software***: parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares;

(xiv) ***Spywares***: software espião que costuma ser instalado no celular ou no computador sem o consentimento do usuário;

(xv) **Terceiro(s):** são os clientes, parceiros de negócios, agentes intermediários, procuradores, subcontratados e fornecedores de bens e serviços, diretos ou indiretos, da Necta e suas Controladas.

(xvi) **Usuário**: qualquer indivíduo, processo, dispositivo ou mecanismo que acesse, use ou manipule uma informação ou ativo de informação

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

4.1. A segurança da informação abrange cinco pilares fundamentais, destacados a seguir:

(i) Confidencialidade: Garante que a informação e ativos de informação sejam acessíveis somente pelos usuários autorizados, pelo período necessário;

(ii) Disponibilidade: Garante que a informação e ativos de informação estejam disponíveis para os usuários autorizados sempre que necessários aos processos de negócio ou a clientes;

(iii) Integridade: Garante que a informação e ativos de informação estejam completos e íntegros e que não tenham sido modificados ou destruídos de maneira não autorizada ou acidental durante o seu ciclo de vida;

(iv) Autenticidade: Garante a propriedade da informação e que esta seja proveniente da fonte anunciada e não foi alvo de alterações indevidas ao longo de um processo estabelecido.

(v) Irretratabilidade (não repúdio): Garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrônicos. Na gestão da segurança da informação, isso significa ser capaz de provar o que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das ações dos usuários.

5. ASPECTOS GERAIS

5.1. A proteção das informações e ativos de informação da Necta deve ser uma prioridade constante em todas as áreas de negócio e de suporte, de forma a reduzir riscos, bem como danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais.

5.2. A proteção das informações e ativos de informação deve ser aplicada de forma compatível com seu impacto à Necta, abrangendo todos os processos, informatizados ou não. As informações sob responsabilidade da Necta devem ser manuseadas de acordo com as leis vigentes e procedimentos internos e utilizadas apenas para a finalidade para a qual foi coletada, evitando o comprometimento de sua confidencialidade, integridade, disponibilidade e autenticidade, inclusive, mas não se limitando, quando no uso de soluções, plataformas e recursos externos, como por exemplo: aplicativos de mensagens, redes sociais, aplicativos de inteligência artificial etc. O colaborador se responsabiliza por ações ocorridas no trato dos dados de titularidade da Necta e/ou terceiros que lhe tenham sido confiados em virtude de sua atividade profissional, em todo o seu ciclo de vida. Assim, garante que o responsável responda por tais questões, inclusive diante da lei.

5.3. Uma pessoa ou entidade não pode negar a autoria da informação fornecida, portanto, a irretratabilidade garante a autenticidade de ações tomadas sob um determinado usuário ou processo.

5.4. Os processos da Necta devem garantir a segregação das funções por meio da participação de mais de um colaborador ou equipe de colaboradores nas atividades, a fim de evitar o conflito de interesse e reduzir o risco de uso indevido acidental ou proposital dos ativos de informação e sistemas.

5.5. Todos os Colaboradores e Terceiros da Necta devem ter ciência de que o uso dos ativos de informação, dos sistemas e ambientes, e respectivas políticas de senhas, podem ser monitorados e que os registros podem ser utilizados para detecção de violações desta Política e procedimentos de segurança da informação, servindo de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais.

5.6. Os riscos de segurança da informação, bem como dúvidas sobre a Política e procedimentos relacionados devem ser reportados à área responsável pela Segurança da Informação.

5.7. Exceto com a expressa autorização do seu proprietário responsável, as tecnologias, marcas, metodologias e quaisquer informações da Necta não devem ser repassadas ou compartilhadas com terceiros, assim como para fins pessoais, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador durante o exercício de suas funções.

6. DIRETRIZES, CONTROLES E PROCESSOS

6.1. Utilização segura de recursos de TI

6.1.1. Os recursos corporativos devem ser somente utilizados para fins profissionais, sendo resguardado à Necta o direito de controlar e monitorar a utilização dos recursos fornecidos aos colaboradores e terceiros.

6.2. Classificação das informações

6.2.1. Toda informação criada deve ser classificada e protegida ao longo de todo seu ciclo de vida, que compreende sua criação ou coleta, manuseio, armazenamento, transporte e descarte.

6.2.2. Para assegurar a proteção adequada das informações, elas devem ser classificadas de acordo com o seu valor, requisitos legais, relevância, sensibilidade e criticidade para a Necta. Os critérios de classificação devem considerar as necessidades de negócio, demandas regulatórias, compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

6.2.3. A classificação da informação (nível de sigilo) é de responsabilidade da área que a gerou. Abaixo seguem os níveis de sigilo recomendados (Público, Interno, Confidencial e Restrito):

(i) Informação Pública: pode ser disponibilizada sem restrições. O conhecimento dessa informação por qualquer indivíduo não causa impactos aos objetivos da Companhia.

(ii) Informação Interna: somente pode ser disponibilizada para os usuários da Companhia. Informações deste nível de sigilo são operacionais e o seu conhecimento por pessoas alheias à Necta não impacta os objetivos de negócio.

(iii) Informação Confidencial: indica forte restrição ao uso e o acesso indevido. Pode acarretar impacto financeiro, operacional ou perda de vantagem competitiva. Quando extraviada ou indevidamente utilizada, pode prejudicar gravemente os objetivos de negócio. O gestor responsável deve indicar explicitamente quais funções podem ter acesso.

(iv) Informação Restrita: informação cujo uso e acesso são restritos a um grupo específico de colaboradores designados nominalmente, não podendo ser divulgado a pessoas não autorizadas, total ou parcialmente, em qualquer que seja o formato. Compreende assuntos, documentos, imagens, ou quaisquer materiais estratégicos, altamente sensíveis e críticos. A sua indisponibilidade, divulgação ou alteração não autorizadas causam graves prejuízos aos objetivos de negócios.

6.3. Proteção de Dados Pessoais e Dados Sensíveis

6.3.1. A Necta leva a sério a proteção de Dados Pessoais e de Dados Pessoais Sensíveis e as medidas de segurança estabelecidas nesta Política são essenciais para garantir o cumprimento da Política de Privacidade e Proteção de Dados Pessoais da Necta e à Lei n.º 13.853, de 14 de agosto de 2018 (“Lei Geral de Proteção de Dados”).

6.4. Segurança Cibernética

6.4.1. De forma a auxiliar na implantação das diretrizes estabelecidas nesta Política e dos controles, processos e procedimentos do Sistema de Gestão de Segurança de Informação e da Segurança Cibernética da Necta, são adotados, por padrão, as boas práticas disponíveis no mercado:

(i) Medidas de autenticação capazes de individualizar usuários que acessam ativos de informação, sistemas e ambientes da Necta;

(ii) Emprego de criptografia, mascaramento e ofuscação, quando aplicável, para o armazenamento de informações relevantes e sensíveis, inclusive dados pessoais, em ativos de informação, sistemas e ambientes da Necta e de fornecedores;

(iii) Soluções de prevenção e detecção de intrusão e acessos não autorizados aos ativos de informação, sistemas e ambientes da Necta;

(iv) Uso de procedimentos e controles para prevenir o vazamento de informações;

(v) Testes e varreduras periódicas para a detecção de falhas e vulnerabilidades nos procedimentos, controles, sistemas e ambientes da Necta;

(vi) Soluções de proteção contra softwares maliciosos (malwares, spywares, trojans, vírus, botnets etc.) que podem afetar ativos de informação, sistemas e ambientes da Necta;

(vii) Sistemas de rastreamento de atividade e registros (logs);

(viii) Controle de acesso dos usuários que fazem uso dos sistemas e ambientes da Necta;

(ix) Segregação e segmentação dos diferentes ambientes de rede disponibilizados pela Necta ou fornecedores por ele contratado aos seus colaboradores, fornecedores e clientes;

(x) Manutenção de cópias de segurança (backup) das informações;

6.4.2. Os controles mínimos listados também devem ser aplicados no desenvolvimento de novos produtos, soluções, aplicativos, sistemas e ambientes, bem como na aquisição de novas tecnologias e serviços que integrarão as atividades operacionais. Da mesma forma, os controles mínimos listados também deverão ser adotados, conforme aplicável, por fornecedores que processam ou armazenam informações sensíveis ou relevantes para a condução das atividades operacionais da Necta.

6.5. Gestão de Identidades e Acessos

6.5.1. Os processos de concessão, alteração e exclusão de acesso aos ativos de informação, sistemas de informação e/ou ambientes da Necta são realizados pela área competente mediante aprovação formal do gestor do solicitante e do respectivo proprietário do sistema e/ou perfil, sempre quando necessário, para o desempenho das atividades.

6.6. Uso de Senhas

6.6.1. A senha é de responsabilidade de cada colaborador, que deve considerar minimamente as seguintes regras:

(i) A senha é pessoal e intransferível;

(ii) O uso de senhas corporativas em computadores e dispositivos móveis não homologados pela Necta é expressamente proibido;

(iii) O armazenamento de senha em navegadores da web deve ser evitado;

(iv) As senhas não devem ser anotadas ou armazenadas em meios físicos e digitais (ex.: e-mail, planilhas, bloco de notas, arquivos na rede etc.);

(v) Devem ser usadas senhas diferentes para diferentes serviços. Senhas de uso particular devem ser diferentes das senhas corporativas;

(vi) Se o colaborador desconfiar que a senha foi descoberta, deve solicitar alteração e/ou bloqueio imediato através da formalização de chamado;

(vii) É proibido o uso do nome de qualquer empresa, produtos ou serviços da Necta, e números sequenciais na formação da senha.

6.7. Gerenciamento de Ativos

6.7.1. O inventário de ativos de Tecnologia da Informação (TI) precisa ser mantido e constantemente atualizado contemplando os principais ativos de informação, tais como: sistemas, aplicações, bases ou bancos de dados e servidores e sua classificação.

6.7.2. Os ativos críticos de negócio (“ACN”) devem ser classificados pelos responsáveis das áreas de negócio em conjunto com a área responsável pela Segurança da Informação.

6.7.3. Os critérios de classificação dos ativos críticos de negócio devem considerar as necessidades de negócio, as leis e regulamentações, classificação da informação e os impactos financeiro, comercial, de segurança, social, ambiental, operacional, de imagem e reputação, tendo como objetivo priorizar o suporte para eventos que comprometam a confidencialidade, integridade e disponibilidade destes ativos.

6.7.4. O hardware deve ser adquirido apenas de fornecedores aprovados, e mantido considerando as seguintes diretrizes:

(i) Somente configurações de software aprovadas devem ser aplicadas ao novo hardware;

(ii) Os usuários finais devem tomar os devidos cuidados com qualquer hardware que lhes tenha sido entregue;

(iii) O hardware perdido e/ou roubado deve ser relatado imediatamente para o Service Desk através de formalização de chamado e respectivo Boletim de Ocorrência;

(iv) O hardware em fim de vida útil deve ser descartado com segurança, de acordo com as orientações do Service Desk ou área competente.

6.8. Gestão de Riscos em Segurança da Informação

6.8.1. A Necta possui um processo estruturado de monitoramento, análise e identificação dos riscos, vulnerabilidades, ameaças e impactos sobre os ativos de informação, para que sejam identificados os controles adequados e a eficácia periodicamente testada.

6.9. Gestão de Incidentes de Segurança da Informação

6.9.1. A Necta adota procedimentos, requisitos e controles específicos para a detecção, tratamento e resposta a incidentes ocorridos. Os procedimentos, controles e requisitos para fornecedores devem estar alinhados com os próprios níveis de complexidade, abrangência e precisão da Necta.

6.10. Treinamento e Conscientização em Segurança da Informação

6.10.1. Como parte do seu compromisso, a Necta adota ações e iniciativas para promover a capacitação, aculturamento e avaliação dos colaboradores sobre o tema segurança da informação, reforçando as diretrizes declaradas nesta Política.

6.11. Avaliação de Segurança da Informação na Contratação de Serviços

6.11.1. Os processos e os controles necessários para reduzir os riscos associados às iniciativas de terceirização, incluindo acordos de computação em nuvem, devem fazer parte dos acordos comerciais entre os fornecedores e a Necta. A Necta se reserva ao direito de avaliar se o fornecedor atende aos requisitos de segurança da informação, baseados em normas e boas práticas de mercado. Os contratos com terceiros devem garantir que a equipe ou subcontratados da organização externa cumpram os documentos normativos de segurança da informação da Necta.

6.12. Aquisição, Desenvolvimento e Manutenção Segura de Software

6.12.1. O processo de aquisição de software deve respeitar todos os direitos autorais de software de computador e os termos de todas as licenças de software das quais a Necta é parte.

6.12.2. A Necta deve gerenciar seus ativos de software e assegurar somente o uso de software legal em suas estações de trabalho e servidores.

6.12.3. Cópias de software de terceiros, com direitos autorais do desenvolvedor do software, a menos que expressamente autorizado, são proibidas.

6.12.4. Os sistemas e aplicativos desenvolvidos internamente ou por especificação da Necta devem garantir:

(i) Avaliação de impacto em privacidade (privacidade por padrão e desde a concepção) deve ser concluída para as principais alterações de software;

(ii) Os requisitos de segurança do software devem ser documentados como parte do processo de desenvolvimento;

(iii) As alterações de software devem estar sujeitas a procedimentos de controle;

(iv) Somente usuários autorizados têm permissão para implantar alterações de software;

(v) Garantia de conceito de segregação de funções tanto para atividades de negócio quanto para administração de TI;

(vi) Garantia de autenticação e configuração de segurança para senhas de acesso;

(vii) Segregação de ambientes para desenvolvimento, qualidade e produção;

(viii) A contratação de serviços para manutenção e desenvolvimento de aplicações deverá conter requisitos de segurança (ex.: utilizando um modelo de RFP ou documento específico para contratações);

(ix) Garantia de avaliação de segurança em código antes da promoção para ambientes produtivos.

6.13. Auditorias De Segurança Da Informação E Cibernética

6.14.1. A área responsável pela Segurança da Informação deve realizar auditorias internas e/ou externas de forma periódica para avaliar a eficácia dos controles de segurança implementados. Essas auditorias seguirão metodologias e critérios definidos, com o objetivo de identificar desvios, vulnerabilidades e oportunidades de melhoria.

6.14.2. Os resultados das auditorias serão analisados pela gestão e as ações corretivas necessárias serão implementadas em um prazo definido.

7. REPORTE E DÚVIDAS

7.1. Constitui responsabilidade de todos os Colaboradores e Terceiros garantir o cumprimento desta Política. Indícios de descumprimento ou dúvidas acerca do cumprimento desta Política e do Código de Conduta, poderão ser reportados ao gestor imediato do Colaborador, à área de Pessoas e Cultura, à Auditoria Interna Corporativa[1], ao Compliance ou por meio de um dos canais de comunicação disponíveis (0800 725 0039 ou www.canaldeetica.com.br/cosan), para apuração conforme Política de Gestão de Denúncias da Commit.

7.2. A Necta não tolera qualquer retaliação contra qualquer pessoa, interna ou externa, que comunique de boa-fé uma violação ou suspeita de violação a esta Política ou ao seu Código de Conduta, sendo garantida a confidencialidade acerca da identidade de qualquer pessoa que comunicar eventual violação. A prática de retaliação é sujeita a medidas disciplinares que podem resultar, inclusive, no desligamento do Colaborador da Necta ou encerramento de um contrato, conforme o caso.

8. REFERÊNCIAS

i. Código de Conduta da Necta;
ii. Estatuto Social da Necta;
iii. Lei Geral de Proteção de Dados Pessoais - Lei 13.709/18 (“LGPD”)
iv. Política de Gestão de Denúncias da Commit;
v. Política de Medidas Disciplinares da Necta; e
vi. Política de Privacidade e Proteção de Dados Pessoais da Necta.

9. DISPOSIÇÕES GERAIS

9.1. Compete exclusivamente ao Conselho de Administração da Necta aprovar qualquer alteração à presente Política, que acontecerá quando do advento de mudanças de processo e/ou alteração de tecnologia (sistemas aplicativos), mudanças de diretrizes ou legislação vigente ou ainda por determinação do Conselho de Administração.

9.2. Esta Política será arquivada durante o prazo de sua vigência, sendo descartada somente no caso de suas versões subsequente estarem em uso (divulgadas) por no mínimo 05 (cinco) anos.

9.3. A presente Política revoga todas as disposições em contrário.

[1] Significa a Auditoria Interna da Cosan S.A, controladora indireta da Necta.

9.4. Conforme disposto no Estatuto Social da Necta, a presente Política foi aprovada pelo Conselho de Administração.

Responsável:	TI
Emissão:	Novembro/2024
Vigência:	Indeterminada
Classificação:	Interno / Externo