1. OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão da Petros e de seus participantes, observando as melhores práticas de mercado e regulamentações aplicáveis.

2. APLICAÇÃO

Este documento aplica-se à Petros, a todos os empregados, estagiários, jovens aprendizes, membros da alta administração (Presidente, Diretor e Conselheiro) e partes relacionadas (terceiros e fornecedores) que tenham algum tipo de relação de negócio ou contratual com a Petros.

3. DOCUMENTOS DE REFERÊNCIA

- Código de Condutas Éticas da Petros.
- NBR ISO/IEC 27001:2013 - Sistemas de Gestão da Segurança da Informação.
- NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação.
- NBR ISO/IEC 27701:2019 – Código complementar ao conjunto de normas NBR ISSO/IEC 27000, para adequação da segurança, quanto ao uso de dados pessoais, em conformidade a LGPD.
- Lei Geral de Proteção de Dados Pessoais (LGPD). Lei Nº 13.709, de 14 de agosto de 2018.
- IT-0114 - REVISAR ACESSOS PRIVILEGIADOS AOS AMBIENTES COMPUTACIONAIS
- IT-0154 - CLASSIFICAR E TRATAR A INFORMAÇÃO
- IT-0155 - TRATAR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
- IT-0157 - UTILIZAR RECURSOS DE TI
- IT-0158 - CONTROLAR ACESSO AOS RECURSOS DE TECNOLOGIA
- IT-0164 - GERIR VULNERABILIDADE DE ATIVOS DE TI
- PL-0060 - POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS
- PL-0028 - MEDIDAS DISCIPLINARES

4. DEFINIÇÕES E SIGLAS

- **Confidencialidade** - Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas. (vide sigilo)
- **Credencial de acesso** - Todo e qualquer meio que permita a identificação pessoal para acesso a um ambiente ou recurso de informação, tais como crachá, login, senha, token etc.
- **Custodiante da informação** - Gerente do órgão responsável pelo armazenamento, processamento, manutenção, recuperação, disponibilização, guarda, transporte e eventual descartada informação.
- **Disponibilidade da informação** - Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes durante o período acordado.
- **Força de trabalho** - São todos os empregados, cedidos, contratados e estagiários da Petros.
- **Gestor da informação** - Titular do órgão que origina ou adquire a informação, ou empregado por ele designado, responsável pela sua segurança e classificação.

- **Incidente de Segurança da Informação** - Ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso.
- **Informação** - Conjunto de dados, imagens, textos e quaisquer outras formas de representação dotadas de significado dentro de um contexto empresarial.
- **Informação custodiada** - É a informação cuja guarda está a cargo de entidade que não possui propriedade sobre ela.
- **Integridade da informação** - Salvaguarda da exatidão, perfeição e completeza da informação e dos métodos de processamento.
- **Processos críticos de negócio** - são aqueles que em situações de desastres eventuais devem ser reestabelecidos imediatamente sob pena de acarretar prejuízos financeiros ou de imagem para a Petros.
- **Recursos da informação** - Todos os meios usados para aquisição, geração, armazenamento e transporte de informação, incluindo recursos do ambiente tecnológico e meios convencionais como telefone, papel, microfilme, vídeo etc.
- **Segurança da informação** - É a proteção da informação de vários tipos de ameaças para garantir a continuidade e minimizar o risco ao negócio, além de maximizar o retorno sobre os investimentos e as oportunidades de negócio. É obtida a partir da implementação de um conjunto de controles adequados, que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.
- **Sigilo** - Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas. (vide confidencialidade).
- ***Token*** - Aparelho que fornece dígitos aleatórios (também chamado de "*one-time password*") trocados em um determinado intervalo de tempo e que, junto com o PIN, compõem a credencial de acesso para o usuário utilizar o Serviço de Acesso Remoto.
- **Usuário da informação** - Empregado, cedido, estagiário ou contratado autorizado a utilizar as informações e os recursos de informação da Petros.
- **Home Office** – Modalidade de trabalho corporativo, nas dependências da residência do empregado, autorizado pelo gestor imediato.

5. DESCRIÇÃO

A informação é um dos principais bens da Petros. Desta forma, definimos a estratégia de Segurança da Informação para proteger a integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes, visando fortalecer a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital da Petros.

A segurança da informação é essencial para as atividades de negócio da Petros e assegurá-la é responsabilidade de todos. Para nortear sua gestão, os princípios estabelecidos nesta Política devem ser seguidos.

Cada um dos empregados, prestadores de serviço, membros da Diretoria e do Conselho devem zelar pela segurança da informação da Petros, inclusive dos dados pessoais que estejam em meio físico ou digital, atuar em linha com as políticas, normas e procedimentos vigentes, sugerindo aperfeiçoamentos e agindo proativamente na salvaguarda das informações.

A inobservância dos princípios aqui descritos é passível de sanções disciplinares previstas na legislação vigente e normativos internos relacionados ao tema, incluindo o Código de Condutas Éticas da Petros.

Mesmo após se desligarem de suas atribuições, empregados e demais agentes não poderão revelar ou divulgar informações confidenciais ou sigilosas com as quais tenham lidado no exercício da função.

5.1. Processos de Segurança da Informação

Para assegurar que as informações estejam adequadamente protegidas, adotamos os seguintes processos:

5.1.1. Gestão de Ativos

Entende-se por ativo, tudo aquilo que a fundação considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou conformidade, gestão de atualizações, autenticação e autorização).

5.1.2. Classificação e Tratamento da Informação

As informações da Petros devem ser utilizadas de modo ético e seguro. Todas as informações, incluindo dados pessoais, devem ser classificadas de acordo com a confidencialidade, de maneira que possam ser adequadamente gerenciadas, protegidas e manipuladas durante o seu ciclo de vida, conforme descrito na NR-0152 – CLASSIFICAR E TRATAR A INFORMAÇÃO.

O ciclo de vida da informação compreende: Recebimento, Geração, Manuseio, Divulgação, Armazenamento, Transporte, Transmissão e Descarte.

Os recursos e as informações geradas internamente – salvo aquelas protegidas por lei – são de propriedade da Petros e seu uso deve servir exclusivamente ao atendimento dos interesses da fundação e de seus participantes.

A troca de informações internas da organização com parceiros de negócios e entidades externas deve seguir requisitos mínimos de segurança da informação a ser definido em normas complementares.

Toda informação envolvendo dados pessoais, controlados ou em posse da Petros, deve ser tratada como confidencial, utilizada para as finalidades definidas pela fundação e apenas por pessoas autorizadas, conforme a Lei Geral de Proteção de Dados e Diretrizes da Política de Privacidade da Petros.

5.1.3. Gestão de Acessos

A concessão, revisão e exclusão de acesso deve utilizar ferramentas e processos corporativos da Petros.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do empregado ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados. Não permitindo o compartilhamento indiscriminado de dados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer empregado deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

As senhas, utilizadas em qualquer finalidade corporativa, não devem ser anotadas ou armazenadas em arquivos eletrônicos não seguros, compreensíveis por linguagem humana (não criptografados), bem como, não devem ser baseadas em informações pessoais e não devem ser constituídas de combinações óbvias de teclado, que possam favorecer a aplicação de ataques de engenharia social ou similares.

Requisitos de Política de Senhas: tamanho mínimo, complexidade, necessidade de ser diferente da senha padrão do fabricante, ações a serem tomadas caso um número máximo de tentativas de acesso malsucedidas seja atingido, e critérios para a gestão de mudanças (prazo, ocorrência de incidentes etc.).

A política de senhas pode ser implementada por controles tecnológicos ou por procedimento. Caso as características de senha previstas na política não possam ser implementadas em determinados ativos devido à restrição tecnológica, deve-se implementar o nível máximo suportado pelo ativo.

Os acessos de administração dos ambientes de operação de tecnologia, como bancos de dados e sistemas operacionais produtivos, são de responsabilidade exclusiva da área responsável por Infraestrutura e Operações de Tecnologia ou seus delegados.

5.1.4. Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos da Petros, para que sejam recomendadas as proteções adequadas. Produtos, processos e tecnologias devem ter a adequada gestão dos riscos

de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura da Petros, parceiros ou prestadores de serviços.

As tecnologias em uso pela fundação devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

5.1.4.1. Gestão de Riscos em Prestadores de Serviços e Parceiros

Os prestadores de serviços e parceiros contratados pela Petros devem ser classificados considerando critérios, conforme documentos internos.

Dependendo da classificação, o prestador de serviços ou parceiro passará por avaliação de risco, que pode incluir a validação in loco dos controles de SI, avaliação remota das evidências ou outras avaliações, além do acompanhamento das correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Os prestadores de serviços e parceiros devem informar os incidentes, relacionados às informações da Petros armazenadas ou processadas por eles, em cumprimento às determinações legais e regulamentares.

5.1.5. Monitoramento de Incidente de Segurança da Informação e Cyber Security

Os ativos devem estar configurados para gerar logs de segurança apropriados para suportar investigações e a reconstrução de possíveis incidentes de segurança. Esses logs devem ser armazenados por prazo mínimo de 1 (um) ano.

Os dispositivos de segurança como Firewalls, IDS/IPS, Anti-Malware e subsistemas de autenticação devem estar configurados para gerar alertas caso identifiquem atividades suspeitas:

a) As regras para geração de alertas devem ser revisadas periodicamente;

b) Todos os alertas devem ser reportados imediatamente à equipe responsável da Gerência de Segurança da Informação, bem como para a Gerência de Infraestrutura e Arquitetura e Help Desk, para atuação o mais breve possível.

c) Os alertas gerados devem ser analisados e respondidos no prazo de 7 (sete) dias definido através da presente política de segurança da informação.

5.1.6. Tratamento de Incidentes de Segurança da Informação e Cyber Security

A Gerência de Segurança da Informação monitora a segurança do ambiente tecnológico da Petros, analisando os eventos e alertas para identificar possíveis incidentes de segurança.

Os incidentes que são identificados pelos alertas, são classificados com relação ao impacto, de acordo com os critérios adotados pela Fundação. Incidentes classificados como relevantes devem ser

comunicados ao Regulador, ao titular do dado, e ao Comitê de Segurança da Informação, quando envolverem dados pessoais que possam acarretar risco ou causar dano relevante aos participantes.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação etc.

O tratamento dos incidentes dessa natureza, serão liderados pela área de segurança da informação, com apoio de outras áreas da fundação, conforme definição em norma complementar.

Visando aprimorar a capacidade de resposta a incidentes, a Petros deve realizar testes de continuidade de negócios simulando cenários de incidentes críticos de Segurança da Informação, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

Todo empregado deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

5.1.7. Conscientização em Segurança da Informação e Cyber Security

A Petros deve promover a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação.

Periodicamente, devem ser disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação.

5.1.8. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de Segurança da Informação e Arquitetura.

Qualquer projeto, iniciativa ou demanda sobre ativo ou artefato de tecnologia, deve ser adquirido, autorizado e disponibilizado pela Gerência de Tecnologia (GTI), salvo quando definido modelos de governança claros e práticos que garantam o controle, padronização, otimização, resiliência, confiabilidade, conformidade e segurança de todo ambiente.

5.1.9. Segurança Física do Ambiente

A segurança física tem por objetivo prevenir o acesso físico não autorizado, danos às instalações e equipamentos, fraude ou sabotagem, dentre outras ameaças. As instalações de processamento da informação críticas devem ser mantidas em áreas seguras.

Todo empregado Petros, deverá nas dependências empresariais, portar crachá de identificação, devendo o empregado, não utilizar o meio de identificação, fora das dependências corporativas, para prevenção de vazamento de informações, como nome, setor e empresa.

Somente pessoas identificadas e autorizadas devem ter acesso físico às instalações da Petros e a ambientes restritos. A identificação do usuário, independentemente do meio, é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas por meio dela.

Conversas referentes a assuntos corporativos devem ocorrer, preferencialmente nas dependências da Petros ou no local de home office, usado pelo empregado, desde que exista uma mínima privacidade para conversas e reuniões como medida de cuidado para o não vazamento de informações internas, reservadas e confidenciais.

Os visitantes devem, obrigatoriamente, estar acompanhados de um empregado Petros, o qual será responsável por solicitar o seu acesso ao edifício e instalações da fundação, durante toda visitação.

Contratados e prestadores de serviço, devem se adequar as normas internas. Em caso de necessidade de acesso a rede da Petros, deverão solicitar a criação de uma credencial de acesso e utilizará a rede interna da Petros, através da solução de virtualização de ambientes e acesso remoto vigentes.

5.1.10. Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de aquisição, desenvolvimento e manutenção de sistemas deve garantir a aderência aos documentos internos e boas práticas estabelecidos pela área de segurança da informação.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

Os ambientes de homologação e desenvolvimento, que possuam dados pessoais, não devem ser carregados com dados produtivos atualizados.

Todo projeto ou iniciativa que envolva tecnologia, deve ser analisado e testado quanto aos riscos de segurança da informação, antes de ser disponibilizado em produção, aos empregados ou participantes da Petros.

5.1.11. Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado. Essas devem ser protegidas contra modificações e acessos não autorizados.

5.1.12. Proteção de Perímetro

Para proteção do ambiente da Petros contra um ataque externo, devem ser utilizadas, no mínimo, ferramentas e controles contra: ataques de negação de serviços distribuídos, e-mails maliciosos (Spam/Phishing), ameaças avançadas persistentes, invasão de dispositivos de rede e servidores, ataques a aplicação e scans de vulnerabilidades externos e internos.

Para mitigação do risco de vazamento de informações devem ser utilizadas ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação *web*, soluções contra vazamento de dados, além do uso de criptografia.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da fundação, por equipamentos particulares não gerenciados ou não homologados.

Os recursos computacionais são corporativos e a Petros realiza a monitoração do uso e a custódia das informações armazenadas ou trafegadas por esses dispositivos.

O acesso à Internet, bem como mensagens enviadas ou recebidas através do correio eletrônico corporativo, incluindo seus anexos, aplicativos de mensagens e outros similares, serão controlados e auditados.

A arquitetura de segurança, envolvendo os ativos tecnológicos, bem como os modelos de acesso às aplicações e informações devem obedecer às regras de segurança estabelecidas em normas complementares de segurança da informação. Qualquer proposta de alteração destes, a qualquer tempo, deve ser analisada pela área de segurança da informação.

5.1.13. Uso Responsável dos Recursos de Tecnologia

Os mecanismos de segurança implementados nos ativos devem ser mantidos e nunca desabilitados.

A utilização dos recursos de tecnologia, tais como: Equipamentos de Microinformática, Correio Eletrônico Corporativo e Internet deve ser restrito aos interesses da fundação.

Todos os recursos computacionais corporativos (Notebooks, Desktops, Smartphones e outros) capazes de armazenar dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis, dados pessoais e softwares licenciados tenham sido removidos ou sobre gravados com segurança.

O uso de dispositivos de armazenamento removíveis ou armazenamento em nuvem (cloud) não corporativa/homologada, seja para armazenamento permanente ou transferência de informações corporativas, não é permitido, salvo exceções, analisadas e autorizadas pela área de Segurança da Informação ou previstas em normas complementares de segurança da informação.

Devem ser utilizados somente softwares fornecidos ou homologados pela Gerência de Tecnologia (GTI), independentemente se obtido de forma gratuita ou remunerada, devendo observar os direitos de propriedade intelectual, pertinentes tais como copyright, licenças e patentes.

5.1.14. Disponibilidade das Informações

Os processos críticos de negócios devem ser assegurados por um Plano de Continuidade de Negócios, atualizado e testado de forma periódica.

As informações devem ter a sua disponibilidade garantida pelo período requerido pelo negócio, pelo período de guarda legal e durante os processos judiciais nos quais componham evidências objetivas.

As informações corporativas mantidas em meios eletrônicos (servidores ou serviços de tecnologia disponibilizados) devem possuir políticas de backup periódicas e devem permanecer íntegras pelo período definido. As informações presentes nos equipamentos de uso individual (desktops e notebooks), são de responsabilidade dos usuários e devem se utilizar dos sistemas e serviços homologados e disponibilizados pela área de Tecnologia para garantia de disponibilidade dessas informações, armazenamento de informações pessoais em dispositivos de uso restrito da Petros não é permitido. Em casos de desligamento, o colaborador não poderá solicitar arquivos pessoais armazenados nos

dispositivos da Petros, salvo exceções, analisadas e autorizadas pela área de Segurança da Informação ou previstas em normas complementares a esta política.

5.1.15. Sanções disciplinares

A violação de qualquer item desta Política pode resultar em consequências graves à Fundação e aos envolvidos. Portanto, a falha em cumpri-la ou em relatar o conhecimento de violação da mesma poderá resultar em medida disciplinar conforme previsto na "NR-0038 – CONSEQUÊNCIAS PARA O CÓDIGO DE CONDUTA E ÉTICA DA PETROS".

5.1.16. Auditoria e validade

Esta política deverá ser auditada e revisada dentro de um prazo máximo de dois anos, visando garantir que a Fundação permaneça aderente à legislação vigente e em conformidade com a evolução tecnológica aplicável. Ela possui validade de até 4 anos, a partir da sua aprovação pelo Conselho Deliberativo.

5.2. Papéis e Responsabilidades

5.2.1. Conselho Deliberativo – CD

Aprovar a estratégia, objetivos e orçamento necessários para a mitigação dos riscos dos processos de segurança da informação.

5.2.2. É Responsabilidade do Comitê Permanente de Segurança da Informação - CPSI: Acompanhar, priorizar e deliberar as demandas relativas à Segurança da Informação da Petros, bem como garantir a consonância das demandas com o planejamento estratégico e com o Plano Diretor de Segurança da Informação (PDSI).

5.2.3. Gerência de Segurança da Informação

Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CPSI;

Apoiar o CPSI em suas deliberações;

Elaborar e propor ao CPSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir esta política;

Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

Tomar as ações cabíveis para se fazer cumprir os termos desta política;

Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.2.4. Gestores da Informação

Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela PETROS;

Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela PETROS;

Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;

Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela PETROS.

5.2.5. Usuários da Informação

Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da PETROS;

Assinar o Termo de Uso de Sistemas de Informação da PETROS, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item 5.1.15 sanções disciplinares.

6. ANEXOS

Não se aplica.

7. DESCRIÇÃO DA REVISÃO

- 25/11/2021: Conversão do normativo para o novo formato de documentação.
- 22/11/2022: Reestruturação do documento incluindo documentos internos de referência.
- 14/08/2023: Revisão e Atualização da Política incluindo novos tópicos e novas responsabilidades.