CNPEM Centro Nacional de Pesquisa em Energia e Materiais	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ("PSI")**	**Emissão** 04/08/2023	**Classificação** Uso Público
		Versão 3.00	**Aprovado por:** Aprovada pelo Conselho de Administração na 127ª Reunião Ordinária, em 03/12/2025.

1. Introdução

1.1. O Centro Nacional de Pesquisa em Energia e Materiais (CNPEM) tem como missão integrar competências singulares em Laboratórios Nacionais para o desenvolvimento científico e tecnológico e apoio à inovação em energia, materiais e biociências.

1.2. O CNPEM entende que a informação é um bem essencial para suas atividades e que sua manipulação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações institucionais.

2. Propósito

2.1. Estabelecer diretrizes de segurança da informação que permitam aos colaboradores atenderem aos padrões de comportamento seguro e adequados às regras e orientações definidas pelo CNPEM.

2.2. Resguardar as informações institucionais e promover a segurança das operações, garantindo os requisitos básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

3. Abrangência e Validade

3.1. A PSI se aplica a todos os colaboradores do CNPEM e terceiros que desenvolvem suas atividades na instituição, e deve ser adotada por suas subsidiárias e afiliadas no Brasil e em outros países.

3.2. Este documento deve ser revisado em, no máximo, 12 (doze) meses da data de sua aprovação.

4. Glossário

4.1. **Ameaça**: É um evento ou atitude indesejável que remove, desabilita ou destrói um recurso. As ameaças normalmente aproveitam as falhas de segurança da instituição. Possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica.

4.2. **Ativo**: Todo elemento que agregue valor ao negócio, podendo ser uma informação digital ou física, hardware, software, pessoa ou ambiente físico, cuja quebra da confidencialidade, integridade ou disponibilidade trará prejuízo.

4.3. **Usuário da Informação**: Qualquer pessoa física ou jurídica que trate ou utilize informações, sistemas e infraestrutura tecnológica do CNPEM.

4.4. **Informação**: Conjunto de dados estruturados que geram valor, entendimento ou sentido sobre determinado assunto.

4.5. **Ativo de informação**: Patrimônio intangível do CNPEM, constituído por suas informações de qualquer natureza, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional dentro e fora de sua estrutura física.

4.6. **Comitê de Segurança da Informação, Privacidade e Proteção de Dados Pessoais (“Comitê”)**: Grupo de trabalho multidisciplinar permanente, designado pela Diretoria-Geral do CNPEM, que tem por finalidade tratar questões ligadas à segurança da informação e à privacidade e proteção de dados pessoais.

4.7. **Confidencialidade**: Não disponibilização e/ou divulgação dos ativos da informação para indivíduos, processos ou entidades não autorizados.

4.8. **Disponibilidade**: Os ativos da informação devem estar acessíveis e utilizáveis sempre que demandados.

4.9. **Gestor da Informação**: Funcionários do CNPEM aos quais foram atribuídas responsabilidades sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob sua gestão e/ou de sua área de atuação.

4.10. **Incidente de Segurança da Informação**: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações e imagem do CNPEM.

4.11. **Integridade**: Propriedade dos ativos da informação do CNPEM de serem exatos e completos.

4.12. **Gestão de Segurança da Informação**: Área responsável pela preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do CNPEM.

4.13. **Comitê de Ética**: Colegiado interdisciplinar e independente, de caráter consultivo, deliberativo e educativo, criado para defender os interesses da instituição com relação a sua integridade e dignidade dentro de padrões éticos.

4.14. **Termo de Uso dos Recursos de Tecnologia de Informação e Comunicação (TIC) do CNPEM**: Documento declaratório de responsabilização pelo bom uso dos equipamentos de tecnologia fornecidos pelo CNPEM aos usuários da informação da instituição.

5. Papéis e Responsabilidades

5.1. Comitê de Segurança da Informação, Privacidade e Proteção de Dados Pessoais

5.1.1. É responsabilidade do Comitê:

5.1.1.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

5.1.1.2. Promover esforços para garantir a disponibilidade dos recursos necessários para uma efetiva gestão de segurança da informação, privacidade e proteção de dados pessoais;

5.1.1.3. Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do CNPEM.

5.2. Área de Gestão de Segurança da Informação

5.2.1. É responsabilidade do Gerente de Segurança da Informação:

5.2.1.1. Conduzir a Gestão da Segurança da Informação, tendo como base a PSI, normas e procedimentos;

5.2.1.2. Elaborar e propor ao Comitê as normas e procedimentos de segurança da informação necessários para se fazer cumprir a PSI;

5.2.1.3. Dar publicidade a PSI, normas e procedimentos, por meio da realização de campanhas de educação e conscientização sobre o tema segurança da informação para todos os Usuários da Informação;

5.2.1.4. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e implantar, mediante aprovação da diretoria do CNPEM, medidas corretivas para mitigar o risco;

5.2.1.5. Tomar as ações cabíveis para se fazer cumprir os termos da PSI;

5.2.1.6. Realizar a gestão dos Incidentes de Segurança da Informação, garantindo o tratamento adequado.

5.3. Gestor da Informação:

5.3.1. É responsabilidade do Gestor da Informação, de forma adicional ao estabelecido para o papel de Usuário da Informação:

5.3.1.1. Gerenciar os ativos de informação sob a responsabilidade da sua área durante todo o seu ciclo de vida e conforme as normas e procedimentos existentes no CNPEM, uma vez que estejam estabelecidos.

5.3.1.2. Autorizar e revisar os acessos às informações, aos documentos e/ou aos sistemas de informação sob sua responsabilidade;

5.3.1.3. Solicitar a concessão ou revogação de acesso às informações, aos documentos e/ou aos sistemas de informação sob sua responsabilidade, de acordo com os procedimentos adotados pelo CNPEM.

5.4. Usuários da Informação

5.4.1. É responsabilidade dos Usuários da Informação:

5.4.1.1. Cumprir os termos da PSI e demais dispositivos que regulamentam a segurança da informação no CNPEM;

5.4.1.2. Zelar pela segurança dos ativos de informação que lhes forem disponibilizados;

5.4.1.3. Comunicar qualquer evento que coloque ou possa vir a colocar em risco a segurança das informações, infraestrutura e sistemas do CNPEM;

5.4.1.4. Comunicar à área de Gestão de Segurança da Informação, por meio do canal seg.info@cnpem.br, qualquer suspeita de violação da PSI;

5.4.1.5. Formalizar a ciência e o aceite integral das disposições do Termo de Uso dos Recursos de TIC do CNPEM.

5.5. Auditoria Interna

5.5.1. A área de Auditoria Interna poderá avaliar, desde que incluído no Plano Anual de Auditoria, se os controles de segurança da informação recomendados pela organização estão sendo atendidos.

5.6. Diretoria

5.6.1. A Diretoria está comprometida com a gestão efetiva de segurança da informação do CNPEM e empenhará esforços para que a PSI seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

6. Diretrizes

6.1. A informação é propriedade do CNPEM e seu uso deve ser feito exclusivamente para os seus interesses.

6.2. Toda informação (documentos eletrônicos, e-mails, mensagens enviadas através de comunicadores instantâneos, sistemas de informação, bases de dados, documentos em papel, pen drives, cartões de memória, informações transmitidas verbalmente etc.) deve ser classificada a fim de garantir o nível de segurança adequado à informação.

6.3. Os canais de comunicação disponibilizados (e-mail, telefonia, Internet, etc.), assim como os equipamentos fornecidos pelo CNPEM (Notebooks, desktops, celulares, tablets, etc.), somente devem ser utilizados pelos colaboradores com vistas ao atendimento dos interesses do CNPEM.

6.4. As credenciais de identificação (crachá, conta de acesso à rede e aos sistemas, senha etc.) fornecidas aos colaboradores ou terceiros contratados para acessar e utilizar as instalações, informações e ativos do CNPEM, são pessoais e intransferíveis, não sendo permitido o seu compartilhamento.

6.5. Devem ser respeitadas as permissões de acesso às informações da instituição, conforme definido pelo Gestor da Informação.

6.6. No desempenho de suas funções, o colaborador, quando devidamente autorizado, poderá acessar/utilizar os recursos da infraestrutura tecnológica do CNPEM a partir de dispositivos particulares (pen drives, notebooks, tablets, celulares, smartphones etc.), observando as orientações dispostas no Termo de Uso dos Recursos de TIC do CNPEM.

6.7. Em qualquer caso, é vedada a utilização de recursos particulares do colaborador para armazenamento de dados e informações confidenciais do CNPEM.

6.8. Incidentes de Segurança da Informação deverão ser comunicados pelos colaboradores ou terceiros, por meio do e-mail seg.inf@cnpem.br ou da abertura de uma Solicitação de Serviços de Informática (“SSI”), para o devido registro e início das atividades de tratamento e resposta.

6.9. Os Incidentes de Segurança da Informação deverão ser tratados integralmente, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às autoridades pertinentes.

6.10. A continuação das atividades do CNPEM deverá ser garantida por meio da adoção, implementação, teste e evolução constante dos planos de continuidade e recuperação de desastres.

6.11. As redes de comunicações devem possuir estrutura adequada de proteção de modo a prevenir o vazamento, modificação, remoção ou destruição dos Ativos, Ativos de Informação e a interrupção das atividades do CNPEM.

6.12. É reservado ao CNPEM o direito de acessar e auditar todas as informações em seus recursos institucionais tecnológicos, independente de notificação prévia ao colaborador.

6.13. Deverão existir, em complemento às diretrizes expostas nesta PSI, normas e procedimento que regulem e orientem as ações definidas pelo CNPEM relacionadas à Segurança da Informação.

6.14. Os colaboradores das áreas definidas pela Diretoria Geral devem realizar toda comunicação, interna ou externa, que possam conter informações sensíveis ou confidenciais da organização, apenas por meio dos canais oficiais de comunicação fornecidos pelo CNPEM (softwares de comunicação e colaboração, linhas telefônicas e sistemas computacionais em geral), com o objetivo de evitar vazamento de informações sensíveis e confidenciais.

6.15. Não deve ser realizado o compartilhamento ou armazenamento de informações sensíveis ou confidenciais da organização em canais de comunicação não oficiais do CNPEM.

7. Sanções e Punições

7.1. As violações, mesmo que por mera omissão ou tentativa não consumada, da PSI, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades previstas no Código de Conduta, e aplicadas conforme o regimento do Comitê de Ética do CNPEM.

8. Casos Omissos

Os casos omissos serão avaliados pelo Diretor-Geral para posterior deliberação.

Esta versão 3.00 substitui a versão 2.00, da PSI aprovada pelo Conselho de Administração em sua 115ª Reunião Ordinária, em 27/8/2024.