Eletrobras
Cepel
A pesquisa que constrói o futuro

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CEPEL

Versão 1.0

de 21/06/2022

Área responsável pela emissão:

Auditoria Interna, Gestão de Riscos e Compliance (ARC) do CEPEL

Público-Alvo:

Todos os empregados, gestores, dirigentes e terceiros do CEPEL.

Aprovação:

Resolução da 24ª Reunião, de 21/06/2022, item 075.24.2022, da Diretoria Executiva do CEPEL.
Reunião nº 223/2022, de 24/08/2022, do Conselho Deliberativo do CEPEL.

Repositório:

Todas as Políticas do CEPEL podem ser encontradas na Intranet do CEPEL.

Direitos de autor e confidencialidade

O conteúdo deste documento não pode ser reproduzido sem a devida autorização. Todos os direitos pertencem ao Centro de Pesquisas de Energia Elétrica - CEPEL.

Histórico de Edições:

Versão	Aprovação	Principais Alterações
1.0	21/06/2022	Não se aplica

Sumário

1. Objetivo

Orientar estrategicamente as questões relacionadas à segurança da informação, definindo diretrizes para proteção, preservação e descarte de informação no ambiente convencional ou de tecnologia do CEPEL.

2. Conceitos

2.1. Artefato malicioso

Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores.

2.2. Ataque

Tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.

2.3. Ativo

Qualquer recurso que tenha valor para o CEPEL.

2.4. Ativo da informação

Dados, informações e seus meios de armazenamento, transmissão e processamento, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

2.5. Colaborador

Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem no CEPEL.

2.6. Espaço cibernético

Espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantam a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente.

2.7. Gestor de Informação

Titulares das áreas que desempenham atividades gerenciais e de direção.

2.8. Incerteza

Estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A incerteza pode se transformar em ameaça ou em oportunidade para o Centro.

2.9. Incidente de Segurança da Informação

Qualquer evento adverso, confirmado ou sob suspeita, que afete a proteção dos sistemas de informação e que comprometa ou tenha potencial para comprometer a segurança da informação.

2.10. Informação

Dados, processados ou não, que possam ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

2.11. Privacidade

Propriedade que exige o direito à reserva de informações pessoais, além da prerrogativa de controlar a exposição e disponibilidade de informações acerca de si mesmo (regulação dos limites).

2.12. Proprietário da Informação

O CEPEL é proprietário e detentor do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

2.13. Proprietário do Risco (*risk owner*)

Colaborador que possui autoridade e responsabilidade pelo gerenciamento de um ou mais Riscos de Segurança da Informação.

2.14. Risco de Segurança da Informação

Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças.

2.15. Segurança cibernética

Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

2.16. Segurança da Informação

Ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade da informação.

2.17. Segurança Física

Medidas físicas destinadas a impedir, detectar e responder ao acesso não autorizado a pessoas, bens, valores, equipamento, instalações relacionadas aos ativos de informação.

2.18. Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

2.19. Usuário

Pessoa física, ou responsável por conta de serviço, habilitada para acessar os ativos de informação do CEPEL.

2.20. Violação

Qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer dos demais instrumentos regulamentares que a complementem.

3. Referências

- Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).
- Decreto nº 10.222, de 5 de fevereiro de 2020 – Aprova a Estratégia Nacional de Segurança Cibernética.
- Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.
- Portaria nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação.
- Portaria nº 09 GSI, de 9 de março de 2018, NC 14 IN01 Computação em Nuvem.
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.
- ABNT ISO GUIA 73:2009 – Gestão de riscos.
- Código de Conduta Ética e Integridade do CEPEL.
- Política de Proteção a Dados Pessoais e Privacidade do CEPEL

4. Princípios

4.1. Garantia de disponibilidade, para que a informação esteja acessível e utilizável sob demanda a todo o Centro.

4.2. Garantia de integridade da informação, para que não seja modificada ou destruída de maneira não autorizada ou acidental.

4.3. Garantia de confidencialidade da informação, para que não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada.

4.4. Garantia de autenticidade de autoria e origem da informação, para que sejam sempre identificáveis.

5. Diretrizes

5.1. O ativo "informação"

5.1.1. Toda informação utilizada pelo CEPEL é um ativo que possui valor e deve ser gerenciada adequadamente ao longo de todo seu ciclo de vida, para que esteja disponível para acesso pelo público adequado, protegida contra manipulação indevida, com tratamento adequado ao seu grau de sigilo ou restrição de acesso e passível de rastreamento.

5.2. Proprietário da informação

5.2.1. O CEPEL é proprietário e detentor do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

5.3. Classificação da informação

5.3.1. As informações utilizadas no CEPEL devem ser classificadas a partir de metodologias e critérios definidos em documentos normativos internos específicos, quanto ao seu grau de sigilo ou nível de restrição de acesso, considerando os processos e atividades nas quais estão inseridas, a fim de assegurar que essas informações recebam um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para o Centro.

5.4. Utilização da informação e dos recursos corporativos

5.4.1. O gestor de cada informação deve determinar a autorização de acesso, incluindo os relacionados ao sistema de gestão empresarial, levando em consideração o sigilo adequado e a necessidade de acesso para cada tipo de público, no cumprimento dos objetivos estratégicos do Centro.

5.4.2. O acesso à informação deve ser autorizado apenas para os colaboradores que dela necessitem para o desempenho de suas atividades profissionais.

5.4.3. Cada colaborador deve acessar apenas as informações ou os sistemas previamente autorizados. Qualquer tentativa não autorizada de acesso à informação ou sistema deve ser considerada uma falta disciplinar.

5.4.4. A credencial (*login* e senha) concedida a um colaborador é de uso individual, intransferível e de conhecimento exclusivo.

5.4.5. Os recursos corporativos fornecidos pelo CEPEL, inclusive o correio eletrônico, devem ser utilizados prioritariamente para fins profissionais. Dessa forma, todo e qualquer uso não deve violar leis e normativos competentes, bem como o Código de Conduta Ética e Integridade do CEPEL.

5.4.6. Para garantir o cumprimento desta política, a utilização dos recursos corporativos deve ser registrada e monitorada pelo CEPEL, não devendo o colaborador ter expectativa de sigilo em sua utilização.

5.5. Proteção da informação

5.5.1. A segurança da informação deve ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e sistemas.

5.5.2. O CEPEL orienta, por meio de seu Código de Conduta Ética e Integridade do CEPEL, que os colaboradores devem "preservar a integridade de documentos, registros, cadastros, dados e sistemas de informação do CEPEL, bem como respeitar a privacidade dos titulares e proteger os seus dados pessoais, em todos os meios utilizados pela instituição, tanto físico quanto eletrônicos".

5.5.3. Os gestores das áreas devem providenciar proteção e controle de acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.

5.5.4. Todo incidente que afetar a segurança da informação deve ser reportado à Comitê de Tecnologia da informação.

5.5.5. Os riscos de segurança da informação devem ser identificados, quantificados e priorizados para que se adotem medidas de proteção adequada.

5.5.6. O Departamento de Tecnologia e Informação (DTI) deve manter registros atualizados dos indicadores de segurança da informação, bem como a adequada manutenção da arquitetura cibernética, dos ativos tecnológicos, das configurações e das soluções de segurança em uso no Centro.

5.5.7. O Departamento de Tecnologia e Informação (DTI) deve informar ao Comitê de Tecnologia da informação quaisquer dados que se façam necessários para compor relatórios à administração do CEPEL.

5.6. Sigilo da informação

5.6.1. Os colaboradores do CEPEL não devem divulgar ou fazer uso de informações corporativas do Centro em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado.

5.7. Continuidade do uso da informação

5.7.1. Os recursos de ambiente convencional ou de tecnologia utilizados nas atividades de gestão, operacionais e de suporte do CEPEL, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.

5.7.2. Os gestores das áreas devem definir e implementar medidas de prevenção e recuperação para situações de desastre e contingência, que devem contemplar os colaboradores e os recursos de tecnologia e de infraestrutura necessários.

5.8. Relacionamentos formais com terceiros

5.8.1. Todos os relacionamentos formais com terceiros (contratos, convênios, acordos, dentre outros) em que haja o compartilhamento de informações do CEPEL e/ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos corporativos devem ser precedidos por termos de confidencialidade e conter cláusulas que tratem especificamente de privacidade e segurança da informação.

5.9. Temporalidade da informação

5.9.1. O CEPEL deve garantir que qualquer informação com valor comprobatório para fins de auditorias, de conformidade e judiciais seja preservada na forma e pelos prazos demandados, em acordo com normativo específico.

5.10. Capacitação

5.10.1. O CEPEL deve incluir a segurança da informação em seus programas de capacitação.

5.11. Tratamento de dados pessoais

5.11.1. O CEPEL deve assegurar o adequado tratamento de dados pessoais, em estrita observância aos termos da Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), nomeando e garantindo o exercício pleno de um encarregado de tratamento de dados pessoais, estabelecer um canal de atendimento à sociedade civil e de interação com a Autoridade Nacional de Proteção de Dados (ANPD) e processos formais de tratamento de incidentes com privacidade dos dados pessoais.

5.12. Violações e penalidades

5.12.1. O CEPEL orienta os colaboradores, por meio de seu Código de Conduta Ética e Integridade do CEPEL, que o "descumprimento, devidamente apurado e comprovado, de algum dos princípios ou compromissos de conduta expressos neste Código poderá resultar na adoção de sanções de caráter educativo ou punitivo, sem prejuízo da adoção de medidas administrativas e/ou judiciais pelas instâncias cabíveis, quando se tratar, ademais, de infrações contratuais e/ou legais".

6. Responsabilidades

6.1. Conselho Deliberativo

- Aprovar o texto base da política de Segurança da Informação após manifestação da Diretoria Executiva sobre o mesmo.

6.2. Diretoria Executiva

- Manifestar-se sobre o texto base da política previamente ao encaminhamento do mesmo ao Conselho Deliberativo.
- Aprovar os documentos normativos derivados que permitam sua implementação.
- Determinar, uma vez aprovadas no nível hierárquico competente, a ampla divulgação das políticas, disponibilizando-as na homepage do CEPEL, na intranet e no Gerenciador Eletrônico de Documentos (GED).

6.3. Comitê de Tecnologia da informação no CEPEL

- Gerir os processos e planejamento de ações de desdobramento desta política, promover treinamentos e campanhas de conscientização em SI, coordenar o tratamento de incidentes de SI, apoiar a gestão dos riscos de SI definindo controles adequados em conjunto com os *risk owners*, gerir a matriz de classificação da informação, coordenar a implementação e manutenção do Plano de Continuidade de Negócio em relação à disponibilidade de informações, prestar suporte a 1ª linha de defesa, atuar junto ao encarregado pelo tratamento de dados pessoais; e, apoiar e participar da execução das ações estabelecidas pelo Comitê de Tecnologia da Informação.

6.4. Gestores das áreas

- Zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política.

6.5. Departamento de Tecnologia e Informação (DTI)

- Gerir os indicadores cibernéticos, comunicar os incidentes, alinhar o planejamento de projetos e iniciativas cibernéticas e atender às solicitações do coordenador do GRSI – Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação, planejar a segurança cibernética do ambiente em que atuam, definindo as configurações tecnológicas necessárias para o alcance da segurança da informação.

6.6. Responsável pela segurança física

- Prevenir e proteger instalações e ativos de informação contra acessos não autorizados, danos ou comprometimento de informações. Compete ainda avaliar regularmente o ambiente e encaminhar relatório das vulnerabilidades encontradas nas medidas de segurança física ao responsável pela segurança da informação.

6.7. Colaboradores

- Cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pelo CEPEL.

6.8. Departamento de Gestão de Pessoas (DGP)

- Promover ações de treinamento e desenvolvimento referentes à segurança da informação, incluindo aspectos técnicos, normativos e comportamentais.

7. Disposições Gerais

7.1. As diretrizes aqui estabelecidas devem nortear a atuação de todos os colaboradores e, destacadamente, do Departamento de Tecnologia e Informação e do Comitê de Tecnologia da Informação, contribuindo para uma visão única e integrada.

7.2. O CEPEL deve adequar seus documentos normativos e os controles que se fizerem necessários em consonância com o estabelecido nesta política no prazo máximo de 180 dias a partir da aprovação pelo Conselho Deliberativo do CEPEL.

7.3. Deve ser assegurado pelo CEPEL que esta política e seus documentos normativos complementares sejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.

7.4. Esta política pode ser desdobrada em documentos normativos internos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

7.5. Esta política, e demais instrumentos regulamentares subordinados a ela, devem ser atualizados sempre que houver necessidade, visando garantir que os requisitos técnicos e legais de segurança implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados às diretrizes que conduzem o desenvolvimento dos nossos negócios, presentes no nosso planejamento estratégico.