ESTADO DO PARANÁ

ePROTOCOLO

Órgão Cadastro:	ELEJOR
Em:	23/09/2022 14:11
CNPJ Interessado	04.557.307/0001-49

Protocolo:

19.518.584-0

Interessado 1:	ELEJOR - CENTRAIS ELÉTRICAS DO RIO JORDÃO S/A
Interessado 2:	-
Assunto:	DOCUMENTACAO/INFORMACAO
Cidade:	CURITIBA / PR
Palavras-chave:	ASSINATURA DOCUMENTO
Nº/Ano	-
Detalhamento:	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA VF.

Código TTD: -

Para informações acesse: https://www.eprotocolo.pr.gov.br/spiweb/consultarProtocolo

elejor
ENERGIA PARA UM MUNDO SUSTENTÁVEL
ENERGY FOR A SUSTAINABLE WORLD

Política
POL/CAD/007/2019
Política de Segurança da Informação e Cibernética
Versão 2.0

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Administrador da POL	Autor/Responsável por Alterações
11/03/2019	1.0	Política de Segurança da Informação	Cleverson Silveira	Cleverson Silveira
29/08/2022	2.0	Política de Segurança da Informação e Cibernética	Cleverson Silveira	Cleverson Silveira

1. FINALIDADE

Estabelecer princípios e diretrizes para a gestão estratégica da segurança da informação e cibernética a serem observados e aplicados de forma a salvaguardar as informações corporativas e demais ativos de informação por meio do gerenciamento adequado dos riscos e suporte à manutenção dos negócios da Companhia.

2. APLICABILIDADE

Esta política aplica-se à Elejor.

3. CONCEITOS

3.1 - INFORMAÇÃO

Ativo, expresso de forma impressa, escrito em papel, armazenado digitalmente, transmitido por correio ou meios eletrônicos, mostrado em filmes, dialogado em palestras, postado em redes sociais, mídias sociais ou em reuniõesformais ou informais, que necessita, por sua importância, ser adequadamente protegido, manuseado e gerenciado.

3.2 - SEGURANÇA DA INFORMAÇÃO

Conjunto de diretrizes, instrumentos e ações que garantem adequado grau de confidencialidade, integridade, disponibilidade e rastreabilidade à informação na Elejor.

3.3 - SEGURANÇA CIBERNÉTICA

Conjunto de diretrizes, instrumentos e ações que buscam proteger as informações e seus sistemas, os dispositivose os ativos digitais da Elejor, assegurando a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação da companhia.

3.4 - CONFIDENCIALIDADE

Característica da informação que a torna reservada, com acesso por pessoas autorizadas.

3.5 - INTEGRIDADE

Característica da informação que a torna exata e completa.

3.6 - DISPONIBILIDADE

Característica da informação que a torna acessível quando necessária em prazo compatível com o processo de negócio.

3.7 - RASTREABILIDADE

Característica da informação que possibilita acompanhar ou identificar algo durante um processo: saber "o quê", "quem", "quando", de "onde" e "para onde".

3.8 - DEVER DE DILIGÊNCIA

Obrigação de ter o cuidado necessário na execução de ato ou procedimento num negócio, para que tudo se cumpra com regularidade.

3.9 - SOFTWARE APLICATIVO

Programa de computador (normalmente referido apenas como aplicativo).

3.10 - PROPRIETÁRIO DA INFORMAÇÃO

Colaborador que, por obrigação legal ou por delegação, é responsável pela informação.

3.11 - PESSOA AUTORIZADA

Pessoa que recebeu autorização, do proprietário da informação, para ter acesso a ela.

4. PRINCÍPIOS

4.1 **Confidencialidade**: garantir que todo acesso à informação seja disponibilizado apenas para as entidades ou pessoas devidamente autorizadas pelo proprietário da informação.

4.2 **Integridade:** garantir que as informações sejam precisas, completas e protegidas de alterações indevidas durante o seu ciclo de vida no que tange às características de confidencialidade, disponibilidade e rastreabilidade.

4.3 **Disponibilidade:** garantir que toda informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitarem.

4.4 **Rastreabilidade:** garantir o acompanhamento das operações nos processos da Companhia, conforme mapeamento de criticidade, visando a identificação de qualquer tipo de alteração da informação.

4.5 **Privilégios mínimos:** garantir que as pessoas, os sistemas de informação e os processos acessem apenas as informações necessárias à execução de suas atividades.

4.6 **Exposição mínima:** garantir que a informação seja mantida protegida, sendo exposta apenas quando necessária.

4.7 **Dever de diligência:** todos os profissionais da Companhia (administradores, empregados, estagiários, aprendizes e terceiros), são corresponsáveis pela preservação e pelo cumprimento das políticas de segurança cibernética da Elejor, realizando todo acesso e uso da informação de forma responsável e regular.

4.8 **Conformidade:** garantir que os processos da Companhia estejam de acordo com normativas internas e externas, seguindo de forma rigorosa protocolos exigidos em decorrência atividades realizadas.

5. DIRETRIZES

5.1 – Adotar um modelo de **maturidade em segurança cibernética,** visando mitigar riscos e preservar as operações da companhia.

5.2 – Elevar continuamente os **níveis de segurança da informação**.

5.3 – Desenvolver um ambiente organizacional que habilite a Elejor a identificar e **gerenciar o risco de segurança cibernética** no que tange a sistemas, processos, pessoas, ativos, dados e recursos.

5.4 – **Proteger os ativos digitais** da Elejor de forma compatível com sua criticidade e relevância aos negócios dacompanhia.

5.5 – Garantir o atendimento às **exigências de rastreabilidade** nas alterações e acessos às informações quando do desenvolvimento e/ou aquisição de aplicativos.

5.6 – Realizar a **gestão e revisão das identidades** e dos acessos aos recursos computacionais da Elejor, garantindo a **definição de privilégios mínimos** e **rastreabilidade** de acessos realizados.

5.7 – **Gerenciar as vulnerabilidades** mantendo as tecnologias devidamente atualizadas, revisadas e testadas periodicamente.

5.8 – Estabelecer **controles de segurança** como parte integrante do processo de desenvolvimento, aquisição e vida útil dos aplicativos para assegurar que as informações processadas estejam **protegidas**, de acordo com sua **classificação e exposição a risco**.

5.9 – Administrar, monitorar e proteger contra **acessos não autorizados** as redes e aplicativos prioritários.

5.10 – Desenvolver a **cultura de segurança cibernética** por meio da conscientização dos administradores, empregados, estagiários, aprendizes e terceiros e disponibilização de meios para detecção e comunicação dos riscos à área de segurança da informação.

5.11 – Desenvolver e implementar **atividades apropriadas** para agir contra um **incidente de segurançacibernética detectado**.

5.12 – Desenvolver e implementar **planos de resiliência** a fim de **restaurar** quaisquer recursos ou serviços queforam prejudicados devido a um incidente de segurança cibernética.

6. REFERÊNCIAS

a) Planejamento Estratégico da Elejor;
b) Código de Conduta da Elejor;
c) Instituto Nacional de Padrões e Tecnologia – NIST;
d) Agência Nacional de Energia Elétrica – Aneel;
e) Lei Geral de Proteção de Dados – LGPD;
f) Marco Civil da Internet – MCI;
g) Código de Defesa do Consumidor – CDC.

Esta Política foi aprovada na 168ª Reunião do Conselho de Administração do dia 19/09/2022.