CETESB

SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS
Secretaria de Meio Ambiente, Infraestrutura e Logística

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aprovada na 610ª Reunião do Conselho de Administração, realizada em 17/12/2024.

dezembro/2024

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Esta Política de Segurança da Informação (POSIN) tem como finalidade estabelecer princípios, diretrizes, responsabilidades e práticas para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, assegurando o uso adequado dos ativos de informação produzidos ou custodiados pela CETESB — Companhia Ambiental do Estado de São Paulo e a mitigação de riscos à Segurança da Informação, visando ao interesse da sociedade em conformidade com a Lei Geral de Proteção de Dados — LGPD e demais normas vigentes.

Esta Política será publicada pelo Setor de Qualidade Organizacional e Normatização — PDPQ, por meio do sistema de gestão de documentos e divulgada no site da Companhia, em atendimento ao público interno e externo.

A POSIN tem como objetivos principais:

- Proteger os ativos de informação de qualquer tipo de ameaça, interna ou externa, deliberada ou acidental, assegurando sua integridade, disponibilidade, autenticidade e confidencialidade;
- Assegurar a conformidade com as leis e regulamentos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) e outras normativas pertinentes à segurança da informação e privacidade;
- Promover uma cultura de segurança entre todos os colaboradores, parceiros e partes interessadas (stakeholders), visando à conscientização e responsabilidade no tratamento das informações;
- Mitigar riscos associados à segurança da informação, através de uma abordagem estruturada de gestão de riscos, com ações preventivas e corretivas voltadas à proteção dos dados;
- Garantir a continuidade dos negócios, estabelecendo processos resilientes e planos de resposta a incidentes que visam minimizar os impactos de falhas e brechas de segurança;
- Manter a privacidade e a proteção dos dados pessoais, conforme estipulado pela LGPD, protegendo a integridade e os direitos dos titulares de dados.

1.1 Dos Princípios

A CETESB adota os seguintes princípios como pilares da sua política de segurança da informação:

1.1.1. Disponibilidade, integridade, confidencialidade e autenticidade das informações;
1.1.2. Garantir que o acesso à informação seja restrito apenas às partes autorizadas, prevenindo a divulgação não autorizada ou acidental de dados;
1.1.3. Assegurar que as informações estejam completas e inalteradas, preservando sua precisão e confiabilidade durante o ciclo de vida dos dados;
1.1.4. Garantir que as informações e sistemas estejam acessíveis e utilizáveis por pessoas ou sistemas autorizados quando necessário;
1.1.5. Garantir que as informações sejam genuínas, assegurando sua origem e autenticidade ao longo de sua gestão;
1.1.6. Promover o tratamento adequado dos dados pessoais, respeitando os direitos das pessoas naturais conforme definido pela Lei Geral de Proteção de Dados (LGPD) e outras regulamentações correlatas;
1.1.7. Agir de maneira transparente no tratamento das informações, permitindo que as partes interessadas conheçam sobre como os dados são gerenciados e protegidos.

2. Abrangência

Esta Política se aplica a todos os colaboradores, estagiários, parceiros e terceiros que atuem no âmbito da CETESB, assim como a qualquer pessoa física ou jurídica que tenha acesso a informações sob custódia da CETESB.

3. Conceitos

Este glossário define os termos e siglas utilizados nesta Política de Segurança da Informação, visando garantir a compreensão clara e uniforme dos conceitos aplicados.

3.1 **Ativos de Informação**: Todos os recursos de informação que possuem valor para a organização, incluindo, mas não se limitando a pessoas, dados, documentos, sistemas, e-mails, e dispositivos físicos e digitais;
3.2 **Autenticação Multifator (MFA)**: Processo de verificação da identidade do usuário utilizando dois ou mais métodos de autenticação (e.g., senha e código enviado por SMS) para aumentar a segurança de acesso aos sistemas;

3.3 **Backup**: Cópia de segurança de informações e sistemas críticos, realizada periodicamente para assegurar a recuperação de dados em caso de falhas ou incidentes;

3.4 **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;

3.5 **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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

3.6 **Confidencialidade**: Garantia de que as informações são acessíveis somente por pessoas autorizadas;

3.7 **Disponibilidade**: Capacidade de garantir que os sistemas e informações estejam acessíveis e utilizáveis por pessoas ou sistemas autorizados sempre que necessário;

3.8 **Gestão de Riscos**: Processo de identificação, análise, avaliação, tratamento e monitoramento de riscos para minimizar o impacto de ameaças sobre os ativos de informação;

3.9 **Incidente de Segurança**: Evento ou ação que compromete a integridade, confidencialidade ou disponibilidade das informações ou sistemas;

3.10 **Integridade**: Garantia de que a informação é precisa, completa e protegida contra alterações não autorizadas;

3.11 **LGPD**: Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/2018), que regulamenta o tratamento de dados pessoais no Brasil;

3.12 ***Phishing***: Método fraudulento utilizado para obter informações confidenciais, como senhas e dados bancários, através de e-mails ou mensagens enganosas;

3.13 **Política de Segurança da Informação (POSIN)**: Conjunto de diretrizes e normas estabelecidas pela organização para assegurar a proteção, integridade e disponibilidade de suas informações e sistemas;

3.14 **Segurança da informação**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

3.15 ***Keylogging***: Método que captura tudo que o usuário digita, utilizado pela instalação de software ou hardware no computador da vítima;

3.16 **Ataque de Engenharia Social**: O atacante manipula a vítima para que essa passe sua senha pessoal, geralmente se passando por uma entidade confiável (suporte técnico, pessoa conhecida e outros);

3.17 **Captura de cache de navegador**: Senhas salvas no navegador podem ser acessadas se o dispositivo for comprometido;

3.18 **Teletrabalho**: Modalidade de trabalho em que os colaboradores realizam suas atividades fora das dependências físicas da organização, utilizando-se de recursos tecnológicos e seguindo as diretrizes de segurança estabelecidas;

3.19 **VPN (Virtual Private Network)**: Rede privada virtual que garante conexões seguras para acesso remoto aos sistemas da organização;

3.20 **Vulnerabilidade**: Fraqueza ou falha em sistemas, processos ou procedimentos que pode ser explorada para comprometer a segurança da informação;

3.21 **Autenticidade**: Garantia de que a informação é genuína e originada de uma fonte confiável;

3.22 **Criptografia**: Técnica de codificação de informações para proteger dados durante a transmissão ou armazenamento, assegurando que apenas partes autorizadas possam acessá-los;

3.23 ***Firewall***: Sistema de segurança que monitora e controla o tráfego de rede, permitindo ou bloqueando conexões com base em regras de segurança pré-definidas;

3.24 ***Malware****:* Programa ou código malicioso que pode comprometer a segurança de um sistema ou roubar informações;

3.25 **Gestão de Acessos**: Processo de controle e monitoramento do acesso aos sistemas e informações, garantindo que apenas pessoas autorizadas possam acessar determinados recursos;

3.26 **Auditoria de Segurança**: Avaliação sistemática dos sistemas e processos para identificar vulnerabilidades e garantir que as políticas de segurança sejam cumpridas.

4. Diretrizes

A POSIN da CETESB adota uma abordagem baseada em riscos, promovendo maior agilidade, flexibilidade e responsabilidade nas ações de segurança da informação. O tratamento de dados pessoais deve seguir os princípios da Lei Geral de Proteção de Dados (LGPD).

4.1 Controle de Acesso

O controle de acesso aos sistemas e informações da CETESB deve ser estruturado de acordo com o princípio do menor privilégio, garantindo que cada usuário tenha acesso apenas às informações necessárias para o cumprimento de suas responsabilidades. As diretrizes incluem:

4.1.1 O acesso aos sistemas será protegido por métodos de autenticação fortes, como senhas seguras e, sempre que possível, autenticação multifator (MFA);

4.1.2 A autorização para acessar dados e sistemas será concedida com base no cargo e nas necessidades funcionais de cada colaborador, estagiário, parceiro ou terceiro;

4.1.3 Todos os acessos serão monitorados regularmente para garantir que não ocorram tentativas de acesso não autorizadas. Auditorias periódicas serão realizadas para verificar a conformidade com as políticas de controle de acesso;

4.1.4 O acesso aos sistemas será revogado imediatamente após o término do vínculo do colaborador, estagiário ou terceiro com a CETESB ou quando não houver mais necessidade de acesso às informações.

4.2 Política de Senhas

As senhas são uma das principais linhas de defesa na proteção dos sistemas da CETESB e devem ser gerenciadas de acordo com as seguintes diretrizes:

4.2.1 As senhas devem conter no mínimo 12 caracteres e incluir uma combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais;

4.2.2 Para minimizar o risco de comprometimento, as senhas deverão ser trocadas a cada 180 dias no primeiro ano de vigência da POSIN e a cada 90 dias a partir do segundo ano;

4.2.3 Não será permitido o uso das últimas 2 senhas anteriormente utilizadas;

4.2.4 Após 3 tentativas de login falhadas, a conta será temporariamente bloqueada:

4.2.5 Sistemas críticos da CETESB, que lidam com informações sensíveis, devem ser protegidos pela autenticação multifator quando possível, além do uso de senhas.

4.3 Gerenciamento de Mudanças

As mudanças em sistemas, processos e infraestrutura de TI da CETESB devem ser gerenciadas de forma estruturada, de acordo com as regras pré-estabelecidas pelo Departamento de Tecnologia da Informação.

4.4 Utilização de Inteligência Artificial (IA)

A CETESB reconhece o papel crescente da Inteligência Artificial (IA) em seus processos e adota as seguintes diretrizes para o uso seguro e responsável de IA dentro da organização:

4.4.1 A utilização ou o acesso a dados pessoais de colaboradores, terceiros ou cidadãos por meio de soluções de IA devem estar em conformidade com as normas da Lei Geral de Proteção de Dados (LGPD) e contar com a aprovação do Departamento Jurídico e ciência do Departamento de Tecnologia da Informação da CETESB;

4.4.2 Antes de disponibilizar qualquer solução de IA, uma avaliação de risco deverá ser realizada para identificar possíveis impactos na segurança da informação, na privacidade de dados e na integridade dos sistemas;

4.4.3 Todas as soluções de IA deverão ser monitoradas continuamente para assegurar que operem conforme as regras de negócio da Companhia e sem comprometer a segurança. Auditorias periódicas deverão verificar o desempenho, a conformidade legal e a ética no uso das soluções de IA;

4.4.4 A CETESB assegura que a utilização de IA não substituirá a responsabilidade humana final. Todas as decisões críticas, especialmente aquelas relacionadas à segurança da informação, devem ser supervisionadas por colaboradores devidamente autorizados.

4.5 Da Computação em Nuvem

O uso de soluções de computação em nuvem pela CETESB deve garantir a segurança da informação, a proteção de dados pessoais e a conformidade com as regulamentações aplicáveis. Antes de qualquer implementação de soluções de computação em nuvem na CETESB, a equipe de segurança da informação deve revisar e autorizar o uso da tecnologia. A autorização deve ser baseada minimamente em:

4.5.1 Garantir que a solução esteja em conformidade com as regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD);

4.5.2 Assegurar que a solução tenha medidas adequadas de controle de acesso, criptografia e monitoramento contínuo, além de políticas de backup robustas;

4.5.3 Todos os acessos aos dados e sistemas em nuvem devem ser autenticados, e deve haver monitoramento e auditoria periódica para verificar a conformidade com as políticas de segurança da informação;

4.5.4 Os serviços em nuvem devem garantir alta disponibilidade e recuperação rápida em caso de falhas.

4.6 Gestão de Riscos de Segurança da Informação

A CETESB deve implementar Gestão de Risco para proteger adequadamente seus ativos de informação e garantir a continuidade das operações. Os riscos de

segurança da informação devem ser periodicamente avaliados e geridos de acordo com as melhores práticas.

4.7 Da Gestão de Ativos

Os ativos de informação da CETESB devem ser mapeados e protegidos contra divulgação, modificação ou destruição não autorizada, independentemente do meio em que estejam armazenados.

4.8 Backups e Gestão da Continuidade de Negócios

A CETESB deve manter controles internos efetivos sobre os procedimentos de backup para assegurar a continuidade dos negócios e minimizar impactos de eventuais incidentes que comprometam a disponibilidade dos serviços.

4.8.1 Os backups devem ser realizados de acordo com o Procedimento de Backup estabelecido internamente pela CETESB, que define a periodicidade, os métodos de backup e os locais de armazenamento, garantindo a proteção e a recuperação das informações críticas. Esse procedimento também inclui a verificação regular da integridade dos backups e a realização de testes de restauração para assegurar que os dados possam ser recuperados com sucesso em caso de necessidade.

4.9 Gestão de Incidentes de Segurança da Informação

Os incidentes de segurança da informação devem ser identificados, monitorados e tratados tempestivamente, com o objetivo de garantir a continuidade das operações da CETESB e a proteção dos dados. O tratamento de incidentes de segurança da informação seguirá o Procedimento para Incidentes de Segurança da Informação estabelecido pela CETESB.

4.10 Do Teletrabalho

O teletrabalho, ou trabalho remoto, deve seguir as diretrizes de segurança para garantir a proteção das informações e sistemas da CETESB:

4.10.1 Os colaboradores em regime de teletrabalho devem utilizar dispositivos fornecidos pela CETESB para acessar os sistemas e informações corporativas, garantindo que esses dispositivos estejam adequadamente protegidos com antivírus e atualizações de segurança;

4.10.2 O acesso remoto aos sistemas da CETESB deve ser realizado por meio de conexões seguras, como VPN (Virtual Private Network), para assegurar a proteção dos dados transmitidos;

4.10.3 Os colaboradores devem garantir que informações não sejam acessadas ou manipuladas em ambientes públicos ou que possam comprometer a privacidade dos dados.

4.11 Do Uso do E-mail

O uso do e-mail corporativo da CETESB deve seguir as seguintes diretrizes para proteger a integridade e a segurança das informações:

4.11.1 O e-mail corporativo é uma ferramenta de comunicação profissional e deve ser utilizado exclusivamente para fins relacionados às atividades da CETESB;

4.11.2 E estritamente proibido o envio de informações sensíveis ou confidenciais sem a utilização de criptografia ou outros métodos de proteção recomendados pelo setor de segurança da informação e em conformidade com a Lei Geral de Proteção de Dados (LGPD);

4.11.3 É estritamente proibido o envio de documentos, informações corporativas ou qualquer outro dado pertencente à CETESB para e-mails pessoais, seja do colaborador ou de terceiros. Toda transmissão de dados deve ser feita por meios corporativos e seguros, assegurando que as informações sejam protegidas conforme as diretrizes de segurança;

4.11.4 Mensagens de e-mail suspeitas ou com anexos desconhecidos devem ser imediatamente reportadas e excluídas, evitando possíveis ataques de *phishing* ou *malware*.

4.12 Outras diretrizes

O detalhamento desta Política poderá ser regulamentado em normas complementares ou instruções normativas, quando necessário, e poderá ter:

4.12.1 Padrões, que definam os procedimentos a serem seguidos;

4.12.2 Boas práticas, que apresentem modelos aderentes à POSIN;

4.12.3 Manuais operacionais que formalizem o seu modus operandi em termos de segurança da informação;

4.12.4 É estritamente proibido o desenvolvimento, instalação ou uso de qualquer software, aplicação ou sistema que não tenha sido previamente autorizado e aprovado pela equipe de Tecnologia da Informação (TI) ou regras pré-estabelecidas pela CETESB;

4.12.5 Qualquer projeto de desenvolvimento de software deve ser submetido ao departamento de Tecnologia da Informação, para garantir que os requisitos de segurança, conformidade e integridade dos sistemas sejam atendidos;

4.12.6 Todos os softwares desenvolvidos ou implementados devem passar por auditoria e testes de segurança conduzidos pela TI para garantir que não comprometam os sistemas e as informações da organização;

4.12.7 O uso de ferramentas ou plataformas externas para desenvolvimento de software só é permitido mediante aprovação formal e homologação pela TI.

5. *Prazo de revisão*

Esta Política deve ser revisada no prazo máximo de 2 (dois) anos, ou sempre que necessário, de forma a manter o seu conteúdo atualizado.

6. Temas da segurança

A segurança da informação na CETESB envolve diversos temas interconectados, os quais devem operar de forma conjunta para garantir a proteção, a integridade e a disponibilidade das informações. Os temas de segurança incluem:

6.1 Segurança Cibernética

Abrange a proteção dos sistemas de TI contra ameaças digitais, como ataques cibernéticos, *malware*, *phishing*, *keylogging*, engenharia social e outros tipos de invasão que possam comprometer a integridade dos dados e dos sistemas da CETESB.

6.2 Segurança Física

Inclui o controle de acesso físico a áreas críticas da CETESB, como datacenter, para proteger os ativos de informação e os equipamentos de TI contra roubo, vandalismo ou acesso não autorizado.

6.3 Proteção de Dados Organizacionais

Envolve medidas para garantir a proteção dos dados sensíveis e críticos da organização, incluindo o uso de criptografia, controle de acesso, políticas de retenção de dados e eliminação segura de informações.

7. Papéis e Responsabilidades

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação na CETESB é uma responsabilidade compartilhada, e os papéis devem ser claramente definidos e atribuídos para garantir a eficácia das ações de proteção de dados e mitigação de riscos. As responsabilidades são distribuídas da seguinte forma:

7.1 Diretoria Colegiada e Conselho de Administração

A Alta Administração da CETESB composta pela Diretoria Colegiada e Conselho de Administração são responsáveis por:

7.1.1 Estabelecer e promover uma cultura de segurança da informação em toda a organização, garantindo o comprometimento de todos os níveis hierárquicos;
7.1.2 Prover os recursos necessários (humanos, financeiros e tecnológicos) para a implementação das políticas e controles de segurança;
7.1.3 Designar formalmente um gestor de segurança da informação, responsável pela coordenação e supervisão das iniciativas de proteção de dados e segurança;
7.1.4 Apoiar a criação e manutenção de um Comitê de Segurança da Informação, com o objetivo de deliberar sobre decisões estratégicas relacionadas à segurança dos ativos da CETESB;
7.1.5 Formalizar e aprovar a Política de Segurança da Informação da CETESB, bem como suas alterações e atualizações.

7.2 Gestor de Segurança da Informação

O gestor de segurança da informação é responsável por:
7.2.1 Coordenar o Comitê de Segurança da Informação;
7.2.2 Coordenar a elaboração e a implementação de políticas de segurança da informação, incluindo normas e manuais operacionais;
7.2.3 Assessorar a Alta Administração na implementação da Política de Segurança da Informação;
7.2.4 Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
7.2.5 Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;
7.2.6 Incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;
7.2.7 Propor recursos necessários às ações de segurança da informação;

7.2.8 Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

7.2.9 Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

7.2.10 Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

7.2.11 Planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

7.2.12 Monitorar e avaliar continuamente os riscos de segurança da informação, garantindo que os controles apropriados sejam aplicados;

7.2.13 Contratar auditorias regulares de segurança da informação e encaminhar relatórios para o Departamento de Auditoria Interna, a fim de garantir a conformidade com a legislação, como a LGPD, além de normas e regulamentos internos;

7.2.14 Esclarecer questões referentes à resposta de incidentes de segurança da informação.

7.3 O Departamento de Tecnologia da Informação (TI)

O Departamento de Tecnologia da Informação é responsável por:

7.3.1 Implementar e manter os controles técnicos de segurança da informação, como *firewalls*, sistemas de prevenção de intrusões (IPS), backups, e criptografia;

7.3.2 Garantir que os sistemas de TI da CETESB estejam sempre atualizados com as últimas medidas de segurança e corrigir vulnerabilidades identificadas;

7.3.3 Garantir o monitoramento contínuo da infraestrutura de TI e responder de forma proativa a ameaças emergentes.

7.4 Todos os Colaboradores e Terceiros

Todos os indivíduos que têm acesso às informações e sistemas da CETESB devem:

7.4.1 Cumprir a política de segurança da informação e normas complementares durante o uso das tecnologias da informação, incluindo a proteção de senhas, autenticação, controle de acesso e o cumprimento das diretrizes de segurança da informação estabelecidas;

7.4.2 Participar de treinamentos e programas de conscientização em segurança da informação, assegurando que estejam atualizados quanto às ameaças e às boas práticas recomendadas pela CETESB;

7.4.3 Relatar imediatamente qualquer incidente, vulnerabilidade ou atividade suspeita relacionada à segurança da informação ao setor responsável, visando uma rápida mitigação dos riscos.

7.5 Comitê de Segurança da Informação

O Comitê de Segurança da Informação tem minimamente a responsabilidade de:

7.5.1 Analisar periodicamente os riscos e as políticas de segurança, propondo atualizações ou melhorias nas práticas de proteção;

7.5.2 Deliberar sobre as estratégicas de investimentos, implementação de novas tecnologias e modificações nas políticas de segurança;

7.5.3 Garantir que as ações de segurança da informação estejam alinhadas aos objetivos estratégicos da CETESB.

8. Das Sanções

O não cumprimento das diretrizes, políticas e procedimentos de segurança da informação estabelecidos pela CETESB poderá resultar em sanções de natureza disciplinar, civil e penal, de acordo com a gravidade da infração. As sanções aplicáveis visam garantir a proteção dos ativos de informação da organização e a conformidade com as leis e regulamentos vigentes, incluindo a Lei Geral de Proteção de Dados (LGPD).

9. Referências

Esta Política está fundamentada nas seguintes legislações e normas:

9.1 Lei Federal n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD);

9.2 Lei Federal n° 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso ll do § 3º do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei n' 8.112, de 11 de dezembro de 1990; revoga a Lei n° 11.111, de 5 de maio de 2005, e dispositivos da Lei n° 8.159, de 8 de janeiro de 1991; e dá outras providências;

9.3 Política de Privacidade da Companhia Ambiental do Estado de São Paulo - CETESB, disponível em https://cetesb.sp.gov.br/politica-de-privacidade/

9.4 Norma ABNT NBR ISO 27002:2022, que fornece os controles de Segurança da informação, Segurança Cibernética e Proteção à Privacidade;

Norma ABNT NBR/ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

9.5 Norma ABNT NBR ISO/IEC 27005:2019, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

9.6 Norma ABNT NBR ISO/IEC 27701:2019, que fornece as diretrizes para a Gestão da Privacidade da Informação;

9.7 Marco Civil da Internet — Lei 12.965/2014;

9.8 Decreto Estadual n° 58.052/2012, que regulamenta a Lei federal n° 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas;

9.9 Política de Governança de Dados da CETESB.

10. Disposições Finais

Esta Política deve ser revisada e atualizada periodicamente, no máximo a cada dois anos, ou quando houver mudanças significativas nos requisitos de segurança da informação. Casos omissos serão resolvidos pela Diretoria Colegiada da CETESB.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

11. Controle de Versões

Versão	Autor	Descrição	Data
01	AI/PMC	Criação	23/12/2021
02	AI	Revisão pelo Departamento de Tecnologia da Informação (AI), com participação da Assessoria da Diretoria de Gestão Corporativa e Sustentabilidade (A), Departamento de Governança e Inteligência de Dados (AD) e Divisão Conformidade e Gestão de Risco (PMC)	12/12/2024