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 567ª Reunião do Conselho de Administração, realizada em 23/12/2021.

dezembro/2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Apresentação

1.1. Esta Política de Segurança da Informação ("Política de SI") é uma declaração formal, aprovada pelo Conselho de Administração da CETESB - Companhia Ambiental do Estado de São Paulo, comunicada a todos os colaboradores e, sempre que cabível, a partes externas relevantes, acerca do compromisso da CETESB em adotar seus melhores esforços para garantir a preservação da segurança dos serviços, recursos, dados pessoais e das demais informações geridas dentro de sua infraestrutura física e de Tecnologia da Informação ("TI").

1.2. Esta Política de SI e todas as normas e procedimentos a ela conexos se aplicam a todos os usuários do site, aplicativos e redes sociais da CETESB, prestadores de serviços, fornecedores e agentes públicos.

1.3. Esta Política de SI é revisada e atualizada a cada 2 (dois) anos e sempre que os procedimentos de manutenção, análise crítica e melhoria no Sistema de Gestão da Segurança da Informação (SGSI) da CETESB demandem alterações significativas, com o objetivo de assegurar sua contínua pertinência, adequação e eficácia no alcance dos objetivos propostos.

1.4. É responsabilidade de cada parte interessada, seja ela interna ou externa, consultar sempre a versão mais atualizada da Política de SI quando houver qualquer questão referente aos temas nela tratados.

2. Definições

2.1. Para os efeitos desta Política de SI, aplicam-se os seguintes termos e definições:

a) Aceitação do risco: decisão de quem detenha competência de acordo com o Estatuto Social e normas internas da CETESB quanto à aceitação de um risco;

b) Agente público: administradores (conselheiros de administração, diretor-presidente e diretores), conselheiros fiscais, membros do comitê de auditoria estatutário, empregados (incluindo os cedidos pela e para a companhia e os licenciados por qualquer motivo), estagiários e aprendizes;

c) Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;

d) Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

e) Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento dos dados pessoais, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

f) Autenticação em dois fatores ou sistema de dupla verificação: medida de segurança para evitar

o uso indevido de senhas, exigindo que o usuário forneça, além da senha, outra informação, preferencialmente, que apenas ele tenha a resposta;

g) Autoridade Nacional de Proteção de Dados (ANPD): órgão da Administração Pública federal, ao qual se refere o art. 55-A e seguintes da LGPD, responsável por zelar pela proteção de dados pessoais, estabelecer diretrizes, fiscalizar e aplicar sanções;

h) Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

i) Ativo: qualquer bem ou direito pertencente à CETESB e que possa ser convertido em dinheiro;

j) Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados, e que gera a obrigação de preservá-la;

k) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

l) 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;

m) Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;

n) "*Data Protection Officer*" (DPO) ou encarregado de proteção de dados pessoais: a pessoa indicada, nos termos da "Política de Privacidade" da CETESB, para atuar como canal de comunicação com os contratantes, os titulares dos dados pessoais e a ANPD;

o) Evento de segurança da informação: uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

p) Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

q) Incidente de Segurança da Informação: um ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

r) Integridade: propriedade de salvaguarda da exatidão e completeza de ativos, assegura que a informação não seja modificada de forma indevida ou destruída de maneira não autorizada, seja de forma intencional, seja acidental;

s) Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709, de 14 de agosto de 2018;

t) Política de Privacidade: política da CETESB que disciplina o tratamento de dados pessoais, com vistas a proteger a privacidade dos titulares dos dados pessoais, tais como os usuários

dos serviços CETESB e colaboradores. A Política de Privacidade está disponível para consulta no site da CETESB e sua intranet;

u) Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

v) Sistema de gestão da segurança da informação (SGSI): a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Inclui estrutura organizacional, políticas, normas e procedimentos, atividades de planejamento, responsabilidades, práticas, processos e recursos;

w) Tratamento de dados: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

x) Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco;

y) Titular de dados pessoais: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

3. Princípios de Segurança da Informação

3.1. Para garantir a segurança da informação, a CETESB, na execução de sua atividade, se baseia nos seguintes princípios:

a) Confidencialidade;

b) Integridade;

c) Disponibilidade.

4. Objetivos

4.1. Esta Política de SI tem por objetivos:

a) Estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos de informação;

b) Implementar controles e procedimentos para reduzir a vulnerabilidade da CETESB a incidentes de segurança da informação;

c) Apoiar a alta direção na implementação da gestão de segurança da informação;

d) Prover os colaboradores e partes externas relevantes com orientação e apoio da Direção da

CETESB, para a garantia da segurança da informação, de acordo com os requisitos das atividades desempenhadas pela CETESB e com as leis e regulamentações aplicáveis;

e) Implementar controles buscando a disponibilidade, integridade, confidencialidade, segurança e autenticidade dos dados e das informações tratadas.

5. Coordenação de Segurança da Informação

5.1. São designados os seguintes "Coordenadores de Segurança da Informação", responsáveis pelo gerenciamento e aplicação da Política de SI em cada área da CETESB:

Coordenador	Atribuições centrais
Titular da unidade organizacional responsável por tecnologia da informação e comunicação	• Mapear as demandas internas, abrangendo os requisitos da legislação vigente e as especificações dos produtos e serviços, para oferecer soluções tecnológicas compatíveis às necessidades da empresa; • Procurar sempre a atualização tecnológica necessária, conforme às tendências de inovação e ofertas dos principais provedores de softwares, hardwares e serviços de tecnologia, para atender de forma proativa com soluções tecnológicas que promovam melhorias operacionais e ganho de performance nos processos corporativos da empresa; • Adotar práticas de redundância e disponibilidade no ambiente de tecnologia da CETESB, garantindo a estabilidade da rede lógica e continuidade ininterrupta dos sistemas em operação.
Titular da unidade organizacional responsável por conformidade e gestão de riscos	• Informar e aconselhar o responsável pelo tratamento e os demais profissionais sobre suas obrigações nos termos da LGPD; • Controlar a conformidade com as políticas do responsável pelo tratamento, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido no tratamento; • Prestar aconselhamento, se tal for solicitado, no que se refere à avaliação do impacto da proteção de dados, e acompanhar o seu desempenho; • Cooperar com as autoridades; • Servir de ponte para a autoridade de supervisão em questões relacionadas com o tratamento.
Titular da unidade organizacional responsável por apoio em assuntos institucionais da área jurídica	• auxiliar a CETESB na adequação de processos, procedimentos de registro e controles internos para atendimento dos princípios da LGPD; • revisar documentos no intuito de resguardar os direitos da empresa quanto à eventuais incidentes de privacidade.

5.2. É competência comum dos Coordenadores de Segurança da Informação:

a) Fornecer aos colaboradores os esclarecimentos necessários sobre quaisquer questões referentes aos temas tratados nesta Política de SI, devendo buscar as respostas que eventualmente não se sintam habilitados a responder junto ao responsável pelas iniciativas de segurança;

b) Receber eventuais denúncias realizadas por colaboradores acerca de potenciais infrações, eventos ou incidentes de segurança da informação, e encaminhá-los a investigação e mitigação de danos, nos termos previstos na Política de Privacidade, mantendo os registros das denúncias recebidas e do tratamento aplicado;

c) Comunicar imediatamente o DPO, sempre que alguma denúncia envolva potenciais eventos ou incidentes com dados pessoais;

d) Controlar a necessidade de compartilhamento de informações em sua área, devendo, sempre que cabível, celebrar acordos de confidencialidade.

5.3. Sempre que verificado que as medidas necessárias à mitigação de um risco são muito onerosas, a decisão quanto à Aceitação do Risco é competência exclusiva da Diretoria Colegiada da CETESB, observado o estabelecido em seu Estatuto Social.

6. Classificação da Informação

6.1. Os titulares das unidades organizacionais da CETESB são responsáveis por alocar a informação que transita por sua área conforme a classificação abaixo, responsabilizando-se por tal alocação e fornecendo as orientações pertinentes à sua equipe. As informações serão classificadas entre:

a) Informação Pública: toda informação que possa ser acessada por usuários da organização, fornecedores, prestadores de serviços e público em geral. São informações que são divulgadas pela CETESB de forma pública e que podem ser acessadas por terceiros sem qualquer restrição ou necessidade de sigilo;

b) Informação Interna: toda informação que possa ser acessada apenas por colaboradores da organização, independentemente do pertencimento a uma área específica. São sigilosas em relação ao público, seja porque poderiam comprometer a imagem da organização, seja por razões estratégicas sobre as atividades desempenhadas, incluindo, ainda informações relativas aos clientes, fornecedores e prestadores de serviços;

c) Informação Restrita: toda informação que possa ser acessada apenas por colaboradores da organização, desde que explicitamente indicados pelo nome ou pela área a que pertencem. São sigilosas em relação público e também aos colaboradores vinculados às demais áreas da CETESB que não estejam expressamente autorizadas a acessá-las;

d) Informação Confidencial: toda informação que possa ser acessada apenas por colaboradores da organização, desde que explicitamente indicados pelo nome ou pela área a que pertencem e desde que tenham inequívoca necessidade de conhecimento da informação para o desempenho de alguma de suas funções. Inserem-se nessa categoria também os dados pessoais de colaboradores, prestadores de serviços e de usuários dos serviços da CETESB. São sigilosas em relação público e também aos colaboradores vinculados às demais áreas da CETESB que não tenham expressa necessidade de acessá-las para desempenhar suas funções.

6.2. A classificação das informações conforme o item 6.1 acima gera para os colaboradores e quaisquer pessoas que tenham acesso a informações da CETESB, a obrigação de preservá-las nos termos previstos, mantendo o seu sigilo em relação aos grupos de pessoas identificados acima.

6.3. Os titulares das unidades organizacionais da CETESB devem orientar sua equipe a tratar a Informação Restrita e a Informação Confidencial como se fossem seus próprios dados sigilosos, destacando que a divulgação não autorizada pode causar sérios danos às atividades da CETESB e/ou comprometer a atuação da organização.

6.4. Os dados pessoais deverão, independentemente de qualquer indicação, ser sempre considerados como Informação Confidencial, de modo que colaboradores que tenham acesso a tais dados deverão zelar pelo sigilo dessas informações e não poderão transferi-las a terceiros sem expressa autorização do titular, tampouco a colaboradores da CETESB que não tenham expressa necessidade de acessá-las para fins de cumprimento de suas funções.

7. Armazenamento de Informações em Suporte Físico

7.1. As informações em suporte físico deverão ser armazenadas em local apropriado, sendo que as classificadas como internas, restritas ou confidenciais devem estar protegidas de acesso indevido por meio de chave e com controle de retirada e devolução.

8. Obrigações dos Colaboradores

8.1. Todos os colaboradores são responsáveis por proteger a informação contra qualquer acesso não autorizado.

a) A obrigação de confidencialidade inclui o dever de, considerados o conteúdo e a finalidade das informações, não compartilhá-las com pessoas que não tenham expressa autorização para acessá-las nos termos da Cláusula 6 acima e, na hipótese de não haver clareza quanto ao tipo de informação acessada, não compartilhá-la com quem não tenha necessidade de acessá-la para o desempenho de suas funções dentro da CETESB, preservando-se,

entretanto, o direito dos titulares de dados pessoais de acessar suas próprias informações. Referente aos dados sediados em servidores, os proprietários dos dados ficam obrigados a anualmente revisar a lista de usuários com os permissionamentos.

8.2. É obrigação dos colaboradores zelar para que a Integridade da informação seja mantida.

a) A obrigação de preservação da integridade das informações inclui o dever de abster-se de promover qualquer alteração do conteúdo das informações ou de descartá-las sem observância dos procedimentos exigidos ou fora das hipóteses em que o descarte objetive o cumprimento das finalidades de manutenção da segurança da informação.

8.3. É dever dos colaboradores zelar para que seja mantida a Disponibilidade da informação para os processos e atividades da CETESB.

a) O dever de manter a disponibilidade inclui a vedação a que informações sejam mantidas fora dos ambientes eletrônicos ou físicos a elas destinados, ou que seu depósito ou armazenamento seja feito com restrição que impeça o acesso a quem tenha o dever de acessar as respectivas informações.

8.4. Todos os colaboradores têm obrigação de participar de Treinamento sobre Segurança da Informação e repeti-lo, pelo menos, a cada 2 (dois) anos, devendo realizá-lo novamente, sempre que houver qualquer atualização relevante no SGSI ou nas políticas a ele relacionadas.

8.5. Na hipótese de suspeita de violação a qualquer norma contida nesta Política de SI ou incidente de segurança, os colaboradores têm obrigação de comunicar imediatamente o titular da unidade organizacional.

a) Caso se trate de situação que envolva tecnologia da informação e comunicação, incluindo, mas não se limitando a perda de senha, invasões de sistemas e situações semelhantes, o colaborador deve reportar o ocorrido ao departamento responsável por tecnologia da informação e comunicação simultaneamente;

b) É obrigação do titular da unidade organizacional acompanhar o tratamento da questão junto ao departamento responsável por tecnologia da informação e comunicação;

c) É obrigação do departamento responsável por tecnologia da informação e comunicação reportar ao titular da unidade organizacional e à Diretoria de Gestão Corporativa da CETESB sobre os tratamentos conferidos;

d) Caso se trate de problema que envolva dado pessoal, os colaboradores, incluindo os titulares das unidades organizacionais e o departamento responsável por tecnologia da informação e comunicação, devem reportar o ocorrido simultaneamente ao DPO.

9. Penalidades

9.1. Nenhum colaborador poderá, sob qualquer circunstância, alegar o desconhecimento desta Política de SI para justificar eventuais violações ou inobservância aos termos nela previstos, ainda que por omissão ou falta nos deveres de cuidado descritos.

9.2. A inobservância às regras e aos procedimentos estabelecidos e implícitos nesta Política de SI poderá sujeitar o infrator e aqueles que com ele colaborarem, às sanções previstas nas regulamentações internas da CETESB, no Código de Conduta e Integridade, na legislação vigente, bem como no contrato pelo qual estejam vinculados à CETESB, sem prejuízo da aplicação de outras sanções administrativas ou legais, cíveis ou criminais, bem como de ações por reparação de eventuais perdas e danos que a CETESB venha a enfrentar em decorrência da violação.

9.3. O não cumprimento desta Política de SI configura falta grave e poderá resultar nas seguintes ações por parte da CETESB, que poderão ser aplicadas cumulativamente, a critério da Diretoria Colegiada da CETESB, em conformidade com a gravidade do descumprimento e/ou o cargo ou tipo de vínculo do colaborador junto à CETESB:

a) Advertência formal (verbal e/ou escrita);

b) Suspensão;

c) Demissão sem ou por justa causa;

d) Rescisão do contrato de prestação de serviços;

e) Ação disciplinar;

f) Processo administrativo, civil e/ou criminal.

9.4. O titular da unidade organizacional é responsável por comunicar a unidade organizacional responsável pela conformidade e gestão de riscos da CETESB sobre toda e qualquer infração a esta Política de SI, incluindo as suspeitas, sob pena de incorrer pessoalmente nas penalidades previstas no item 9.3 acima.

10. Política de Senhas

10.1. As senhas iniciais são definidas no ato da admissão do funcionário, pela unidade organizacional responsável pela administração de pessoal no momento de criação do usuário no sistema interno da CETESB, após assinatura de Termo de Responsabilidade, devendo ser alteradas no momento do primeiro acesso. A comunicação da senha inicial ao usuário é feita

por intermédio da unidade organizacional responsável pela administração de pessoal.

a) A criação de usuário e senha para terceiros será feita pela unidade organizacional responsável pela tecnologia da informação e comunicação, mediante a assinatura de Termo de Responsabilidade.

10.2. Não é permitido o uso de senha genérica, devendo todo usuário/senha ser de uso individual, pessoal e intransferível e de responsabilidade exclusiva do colaborador a quem se vinculam.

10.3. Não são permitidas tentativas de:

i. Obter acesso não autorizado a sistemas ou ambientes digitais internos da CETESB;
ii. Fraudar a autenticação de usuário ou segurança de qualquer servidor, rede ou conta ("*cracking*");
iii. Acesso a dados não disponíveis para o colaborador;
iv. Conexão a servidor ou conta cujo acesso não seja expressamente autorizado;
v. Colocar à prova a segurança de outras redes.

10.4. As senhas são pessoais e devem ser protegidas pelos colaboradores, não podendo ser transferidas a terceiros e, ainda:

a) Cada colaborador é exclusivamente responsável pela confecção e confidencialidade de sua senha de conta de acesso, bem como por zelar pelo uso correto de sua identificação. Os atos praticados por terceiros serão de responsabilidade dos colaboradores cujo acesso estiver habilitado no equipamento;

b) As senhas não poderão ser divulgadas, cedidas e/ou compartilhadas, ou ainda mantidas escritas ou armazenadas, manualmente ou digitalmente, sem mecanismos adequados de proteção homologados pela unidade organizacional responsável pela tecnologia da informação e comunicação;

c) Não é permitida a gravação de senhas para serem automaticamente utilizadas por programas, sistemas, serviços, computador, códigos fonte, scripts, exceto em aplicações single-sign-on, plataformas de cofre de senha (Kee Pass) e contas de serviço.

10.5. Caso o colaborador perca a senha ou desconfie do acesso ao seu equipamento por terceiros deverá informar imediatamente a unidade organizacional responsável pela tecnologia da informação e comunicação, que providenciará a troca da senha.

10.6. Caso a senha cadastrada seja esquecida, nova senha deverá ser cadastrada pela unidade organizacional responsável pela administração de pessoal pelo RH.

10.7. As senhas criadas pelos colaboradores devem, conforme as possibilidades de cada sistema, atender aos seguintes requisitos mínimos de segurança descritos abaixo:

a. Tamanho mínimo: 8 caracteres
b. Possíveis caracteres sequenciais: 2 caracteres (11, 22, aa, bb...)
c. Possíveis caracteres repetidos: 2 caracteres (11, 22, aa, bb...)
d. Composição: conter, pelo menos, 2 categorias abaixo:
    a. Caracteres numéricos (0 a 9)
    b. Caracteres especiais (! @ # $ % & *)
    c. Caracteres maiúsculos (A a Z)
    d. Caracteres minúsculos (a a z)

10.8. Não são permitidas senhas fora dos critérios definidos nesse documento, tampouco em branco.

10.9. Os sistemas utilizados pela CETESB devem ser configurados, respeitadas suas limitações, para atender aos atributos de configuração de senhas conforme abaixo:

a. Prazo para expiração da senha: 90 dias
b. Fator de repetição: 5 vezes
c. Tentativas antes de bloqueio por erro: 5 tentativas
d. Desbloqueio por tentativas: logon seguinte

10.10. As senhas de acesso a rede devem ser renovadas a cada 90 dias. Para tanto, a solicitação automática de renovação de senha será requerida, e o acesso aos equipamentos será inativado até que nova senha seja cadastrada. Caso se verifique inviabilidade de solicitação automática do sistema, compete ao colaborador realizar a alteração a cada 90 dias.

11. Política de Controle de Acesso

11.1. O Controle de Acesso envolve o acesso lógico, aos recursos de tecnologia, e o acesso físico às instalações da CETESB.

11.2. O Controle de Acesso à informação, bem como a quaisquer bens e equipamentos ou qualquer suporte físico que contenha informações, deve considerar os seguintes aspectos:

a) Todo uso de informação deve observar as normas desta Política de SI, devendo ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário;

b) É obrigatória a prévia autorização da Área proprietária dos dados, caso seja necessário o

acesso a dados complementares não originalmente pertinentes à área de atuação do colaborador, o que deverá ocorrer mediante identificação única e intransferível do usuário;

c) Sempre que houver a admissão ou mudança das atribuições do usuário, o acesso a novas informações deve ser autorizado pelo superior imediato, para que a unidade organizacional responsável pela tecnologia da informação e comunicação providencie as permissões de acesso compatíveis, bem como demais providências necessárias;

d) Sempre que houver mudança de alocação do usuário, o acesso às informações da área de origem deverá ser automaticamente bloqueado pela unidade organizacional responsável pela tecnologia da informação e comunicação. O acesso às novas informações na área de destino deve ser autorizado pelo superior imediato, para que a unidade organizacional responsável pela tecnologia da informação e comunicação providencie as permissões de acesso compatíveis, bem como demais providências necessárias;

d.1) A unidade organizacional responsável pela administração de pessoal comunicará a unidade organizacional responsável pela tecnologia da informação e comunicação sempre que houver movimentação de funcionários para o respectivo bloqueio.

e) Sempre que houver desligamento de colaboradores, a unidade organizacional responsável pela tecnologia da informação e comunicação deverá imediatamente recolher os equipamentos, observado o item "f" abaixo, bens e quaisquer informações utilizadas pelo colaborador e remover imediatamente o acesso do usuário aos sistemas da CETESB;

f) Caso o colaborador utilize equipamentos próprios, deverá entregá-los à unidade organizacional responsável pela tecnologia da informação e comunicação, para remoção das informações pertinentes à CETESB;

g) A unidade organizacional responsável pela administração de pessoal deverá providenciar a notificação à unidade organizacional responsável pela tecnologia da informação e comunicação quanto aos ajustes necessários dos privilégios de acesso aos sistemas e equipamentos, bem como a adequação em relação aos acessos físicos.

11.3. O Controle de Acesso Físico às instalações da CETESB é monitorado, apenas sendo autorizada a entrada de colaboradores, prestadores de serviço e usuários dos serviços, podendo, conforme o caso, ser autorizada a entrada de acompanhante dos usuários e, ainda:

a) A entrada e permanência de usuários e respectivos acompanhantes deve ser sempre acompanhada por colaborador da CETESB da área onde atuará o prestador de serviço;

b) A entrada e permanência de prestadores de serviços eventuais deve ser sempre supervisionada por colaborador da CETESB da área onde atuará o prestador de serviço;

c) Os colaboradores devem evitar acessar áreas da CETESB às quais o acesso não seja necessário ao desempenho de suas atividades.

11.4. O Controle de Acesso Lógico aos equipamentos e computadores da CETESB, bem como à rede interna e aos seus sistemas de dados, é realizado por intermédio de senhas que garantam acesso adequado a cada perfil de acesso e respectivos privilégios, e cuja definição e utilização devem observar a Política de Senhas descrita na Cláusula 9 desta Política de SI.

12. Acesso Remoto (VPN)

12.1. O acesso remoto de uma rede externa às estações de trabalho e servidores CETESB deverá ser monitorado, autorizado e somente feito utilizando VPN.

12.2. Somente será fornecido acesso a VPN para colaboradores ou prestadores de serviço em regime de trabalho remoto ou cujas atividades possam demandar acesso à rede interna da CETESB quando estejam fora das instalações físicas da organização, ou ainda em casos específicos, a colaboradores que utilizem dispositivos próprios.

12.3. O acesso remoto deve ser solicitado através de chamado a ser enviado para a unidade organizacional responsável pela tecnologia da informação e comunicação, com aprovação do gerente imediato ou, em caso de fornecedores ou prestadores de serviço, pelo Gestor do contrato, mediante justificativa fundamentada.

12.4. Os usuários que tiverem direito ao acesso remoto devem estar cientes de que:

a) A proteção da confidencialidade das informações nos equipamentos utilizados para acesso ao VPN é de responsabilidade do próprio usuário.

b) Os recursos de tecnologia da informação disponibilizados têm como objetivo a realização de atividades profissionais, respeitando o horário normal de expediente e as prorrogações de jornada autorizadas.

c) O usuário com acesso remoto autorizado, acessa os mesmos ambientes que visualiza internamente, ou seja, manterá o mesmo perfil de acesso que detém quanto dentro das instalações físicas da CETESB.

12.5. Os usuários autorizados ao acesso remoto, devem garantir que seu perfil de acesso remoto não seja utilizado por outras pessoas, protegendo suas credenciais e, em nenhum momento, devem disponibilizar seu login e senha VPN, ou qualquer informação de acesso a terceiros.

13. Teletrabalho

13.1. Os colaboradores em regime de teletrabalho ou que sejam autorizados a realizar todas as atividades à distância assumem o compromisso de:

a) Manter sempre instalados e atualizados softwares de segurança como antivírus e firewalls, bem como utilizar mecanismos de criptografia validados pela CETESB;

b) Realizar verificação por antivírus em todo arquivo em mídia proveniente de entidade externa e/ou recebido/obtido pela internet;

c) Não conectar seu dispositivo a redes Wi-Fi não criptografadas;

d) Não enviar documentos da organização para sua conta de e-mail pessoal, tampouco realizar quaisquer tipos de cópias dos documentos, devendo solicitar autorização para imprimir quaisquer materiais, mediante justificativa quanto à necessidade;

e) Não publicar fotos do ambiente de trabalho remoto em rede sociais expondo dados e sistemas da organização;

f) Dedicar o máximo cuidado com a segurança física do equipamento utilizado, seja pessoal, seja fornecido pela CETESB, bem como ao acesso ou visualização de informações por terceiros;

g) Autorizar que a unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB realize revisões periódicas nos equipamentos utilizados, de modo a garantir a atualização de sistemas de segurança, inclusive antivírus e firewalls, bem como para fins de auditoria referente à adequada utilização dos sistemas da CETESB, com vistas a assegurar o mesmo nível de segurança aplicado aos equipamentos utilizados dentro das instalações da CETESB.

14. "*Bring your own device*" (BYOD) ou traga seu próprio dispositivo

14.1. A utilização de dispositivos de propriedade pessoal (BYOD), inclusive dispositivos móveis como smartphone, ultrabook, notebook, tablet etc., é permitida, nos seguintes termos:

a) O acesso exclusivo à Internet, inclusive por prestadores de serviços e usuários dos serviços CETESB, bem como acompanhantes, poderá ser feito sem o cadastro prévio do dispositivo BYOD através de redes sem fio configuradas com restrições de segurança e que não permitirão o acesso aos demais serviços de TIC (por exemplo: VoIP, Impressão, sistemas internos, etc), mediante a utilização de credencial de acesso específica para visitantes.

b) A unidade organizacional responsável pela tecnologia da informação e comunicação poderá,

sem aviso prévio, suspender o acesso em caso de suspeita de Incidentes de Segurança da Informação. Nesses casos, o dispositivo estará sujeito à coleta de informações de hardware e software exclusivamente através da coleta de tráfego da rede interna ou externa, ressalvada a privacidade do usuário.

c) Em casos de comprovação de Incidentes de Segurança da Informação envolvendo dispositivo BYOD, o acesso será revogado e serão tomadas as devidas providências administrativas para apuração da responsabilidade.

d) Os softwares utilizados nos dispositivos BYOD deverão possuir licenças válidas, estando o usuário ciente de que a violação de direito autoral relacionado a softwares configura crime tipificado pela legislação brasileira.

e) O usuário será o único responsável pela manutenção e atualização das licenças dos softwares instalados no seu dispositivo e responderá por qualquer incidente ou demanda sobre o uso de software não licenciado em seu dispositivo.

f) É responsabilidade do usuário, a guarda e manutenção adequada do dispositivo BYOD, bem como a segurança dos dados armazenados no dispositivo, sendo o proprietário responsável por eventuais vazamentos de informações ou perda de dados. Recomenda-se a utilização de criptografia nos dados do dispositivo e backup frequente dos dados, bem como o uso de software de Antivírus/Firewall.

g) A CETESB não se responsabiliza por acessos indevidos ao dispositivo ou danos de hardware e/ou software que possam ocorrer, mesmo quando o dispositivo for utilizado para acesso à rede CETESB ou execução das atividades do usuário.

h) Em caso de perda, roubo ou furto do dispositivo credenciado, a unidade organizacional responsável pela tecnologia da informação e comunicação deverá ser informada imediatamente, via sistema de chamado, para que sejam tomadas as medidas de segurança cabíveis, com o descredenciamento objetivando evitar o uso indevido do dispositivo extraviado por terceiros dentro do ambiente da CETESB.

i) Qualquer utilização de dispositivos BYOD para atividades além do exclusivo acesso à rede destinada a visitantes estará sujeita às demais regras previstas nesta Política de SI.

15. Utilização de Computador/Notebook da CETESB

15.1. O uso dos computadores e notebooks é restrito às atividades profissionais do usuário, observado o horário normal de expediente e as prorrogações de jornada autorizadas.

15.2. Somente funcionários ou prestadores de serviços com usuário e senha válidos podem

acessar os computadores CETESB.

15.3. Para o acesso a sistemas da organização é obrigatória a utilização de senha pessoal do colaborador.

15.4. Nenhum usuário deverá possuir perfis e privilégios de acesso diferente da área em que atua.

15.5. A unidade organizacional responsável pela tecnologia da informação e comunicação deve ser imediatamente comunicada pelos Coordenadores e/ou unidade organizacional responsável pela administração de pessoal sempre que houver alteração do perfil de acesso dos usuários ou sua retirada em caso de desligamento.

15.6. A utilização de notebooks da CETESB está condicionada a que o colaborador assine o Termo de Responsabilidade para Uso de Aparelhos.

a) A CETESB poderá, a seu exclusivo critério e a qualquer tempo, mesmo durante a vigência do contrato que estabeleça o vínculo com o colaborador, suspender, interromper ou cessar o fornecimento dos equipamentos, seus acessórios e serviços agregados, independentemente de qualquer motivação ou justificativa prévia, sem direito a qualquer reparação por parte do usuário.

b) Finda a relação contratual entre a CETESB e o colaborador, os equipamentos e seus acessórios deverão ser devolvidos à CETESB no exato estado em que foram cedidos ao usuário, com exceção do desgaste natural decorrente do uso, sob pena de ressarcimento pelo usuário à CETESB do valor correspondente aos danos causados.

15.7. Os equipamentos disponibilizados para o uso dos colaboradores são de propriedade ou de responsabilidade da organização, cabendo aos colaboradores utilizá-los e manuseá-los corretamente para as atividades de interesse da CETESB e exercício de suas atividades e, portanto, é obrigação de cada usuário:

a) Utilizar o equipamento com zelo e manter a boa conservação do aparelho, responsabilizando-se pela perda e eventuais avarias que o equipamento venha a sofrer;

b) Responsabilizar-se pelos equipamentos que esteja autorizado a utilizar e seus respectivos acessórios, de modo que não poderá trocá-los, permutá-los ou emprestá-los a outros usuários, sem prévia e expressa autorização da CETESB;

c) Suportar integralmente os danos de qualquer natureza causados ao equipamento e seus

acessórios, em decorrência de mau uso;

d) Reportar à unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB quaisquer comportamentos suspeitos do equipamento ou dos sistemas, para que possíveis falhas ou incidentes, inclusive vírus, possam ser identificados no menor tempo possível;

e) Informar à equipe da unidade organizacional responsável pela tecnologia da informação e comunicação qualquer identificação de dispositivo estranho conectado ao seu computador.

15.8. É proibida e, sempre que possível, será barrada pelos sistemas, podendo sujeitar o usuário a medidas de responsabilização e reparação de danos:

a) Utilização de todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos sistemas dos computadores e notebooks, sem o conhecimento prévio e o acompanhamento da unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB;

b) Realização de reparo de computadores/notebook ou outros equipamentos de informática por qualquer pessoa que não seja da unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB ou terceiro devidamente contratado para o serviço;

c) Instalação ou uso de software nos equipamentos sem a expressa autorização e acompanhamento da unidade organizacional responsável pela tecnologia da informação e comunicação;

d) Utilização de pen-drive, devendo o usuário solicitar à unidade organizacional responsável pela tecnologia da informação e comunicação a cópia do conteúdo para uma pasta de rede exclusivamente nas hipóteses em que a cópia seja autorizada pelo titular da unidade organizacional correspondente, devendo ser adequadamente motivada;

e) Utilização de pastas públicas ou outras cujo acesso não seja restrito, para armazenamento de arquivos que contenham Informação Confidencial ou Informação Restrita.

15.9. A CETESB respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da entidade. Portanto, é terminantemente proibido o uso de programas ilegais (sem licenciamento) ou não autorizados pela CETESB.

a) A instalação de quaisquer softwares, drivers e/ou programas apenas poderá ser realizada pela unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB, desde que alinhados à Política de SI e que não representem risco ao SGSI da CETESB.

b) A unidade organizacional responsável pela tecnologia da informação e comunicação fará verificações periódicas nos dados dos servidores e/ou computadores e notebook dos usuários, visando garantir a correta aplicação dessa diretriz.

c) Caso sejam encontrados programas não autorizados, estes deverão ser removidos imediatamente, e o usuário será devidamente responsabilizado.

d) Os sistemas de tecnologia da informação e comunicação deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer terceiro.

e) Aqueles que instalarem tais programas não autorizados nos computadores ou violarem direitos de propriedade intelectual se responsabilizarão perante a CETESB por quaisquer problemas ou prejuízos causados em decorrência desta ação.

15.10. Os computadores/notebooks deverão conter versões do software antivírus instaladas, ativadas e atualizadas permanentemente.

a) A atualização do antivírus será automática, agendada pela unidade organizacional responsável pela tecnologia da informação e comunicação.

b) É expressamente proibido desabilitar o programa antivírus instalado nos equipamentos.

c) Todo arquivo em mídia proveniente de entidade externa a CETESB deve ser verificado por programa antivírus, bem como todo arquivo recebido/obtido pela Internet.

15.11. Todos os computadores/notebooks utilizados para acessar sistemas da CETESB poderão:

a) Ser acessados remotamente somente pela unidade organizacional responsável pela tecnologia da informação e comunicação.

b) Passar por auditorias interna/externa realizadas pela unidade organizacional responsável pela tecnologia da informação e comunicação ou terceiro contratado pela CETESB.

c) Ter as informações do seu registro de log do Sistema Operacional examinadas, para fins de acompanhamento, monitoramento e controle de sua utilização, visando, inclusive, à proteção do colaborador contra invasões indevidas.

16. Acesso à Internet

16.1. A internet deve ser utilizada para fins de complemento às atividades profissionais, para o enriquecimento intelectual dos colaboradores ou, no caso dos pesquisadores, como ferramenta para busca por informações que venham contribuir para o desenvolvimento de

seus trabalhos.

16.2. É expressamente vedada a utilização para realização de trabalhos de terceiros ou de atividades que tenham finalidade diversa daquela para qual o usuário foi contratado.

16.3. Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a unidade organizacional responsável pela tecnologia da informação e comunicação com prévia autorização do titular da unidade organizacional.

16.4. O uso da internet será auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

16.5. As seguintes atividades são proibidas:

a) Baixar arquivos como vídeos, imagens e executáveis da Internet que não foram aprovados pela unidade organizacional responsável pela tecnologia da informação e comunicação;

b) Acessar sites com conteúdo pornográfico, webproxys, jogos, bate-papo, apostas e assemelhados. Tais conteúdos estarão bloqueados e serão monitorados, sujeitando o infrator que os acessar às penalidades cabíveis;

c) Acessar softwares P2P que realizam buscas e baixem arquivos (download) de conteúdo de áudio, vídeo, programas etc. (por exemplo, torrents); e,

d) Acessar jogos online, rádio e TV online.

16.6. Todo o acesso à internet por meio de equipamentos da CETESB será monitorado através de log contendo MAC, IP, URL acessada, data e horário, possibilitando a o rastreio da atividade.

16.7. A internet terá seu acesso concedido conforme os seguintes tipos de acesso: 1) Básico sem streaming, rede sociais e armazenamento em nuvem; 2) Acesso pleno.

16.8. O acesso à Internet através da rede Sem Fio (WIFI) será monitorado pela CETESB e disponibilizado conforme Acesso visitantes, mobile, consultores e funcionários.

17. Uso de E-mail

17.1. A ferramenta de e-mail será fornecida de forma individual a cada novo colaborador, a quem se atribui total responsabilidade sobre o seu uso, para uso exclusivo em suas atividades profissionais.

17.2. Os usuários devem:

a) Adotar o e-mail como recurso preferencial para comunicações oficiais internas que não necessitam ser circuladas por meio físico escrito, com vistas a reduzir o risco de exposição de papeis a terceiros, bem como o custo com impressão, aumentando a agilidade na entrega e leitura da informação;

b) Cuidar para que sua senha de acesso ao equipamento e ao e-mail não sejam acessadas por terceiros e bloquear os equipamentos quando não estiverem em uso, sendo o responsável direto pelas mensagens enviadas por seu endereço de e-mail;

c) Realizar a manutenção da caixa de e-mail, apagando mensagens inúteis e evitando acúmulo de informações desnecessárias.

17.3. Os usuários não devem:

a) Abrir e-mails de remetentes com os quais não estejam familiarizados;

b) Abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela unidade organizacional responsável pela tecnologia da informação e comunicação, caso não tenha certeza absoluta de que solicitou o conteúdo;

c) Clicar em links, exceto quando tenha certeza absoluta de que solicitou o conteúdo ou quando confirmado com a unidade organizacional responsável pela tecnologia da informação e comunicação que se trata de link confiável;

d) Abrir e-mails com assuntos estranhos, potencialmente nocivos e/ou em inglês, tendo em vista a gravidade de vírus circulados nos últimos anos por e-mails que continham assuntos maliciosos;

e) Utilizar o e-mail fornecido pela CETESB para assuntos pessoais;

f) Utilizar o seu e-mail pessoal para enviar correntes para e-mails da CETESB;

g) Enviar anexos (arquivos) muito grandes, exceto quando estritamente necessário ao desempenho de suas atividades.

17.4. É proibido o envio de grande quantidade de mensagens de e-mail (spam), o que inclui mala direta, correntes, anúncios, propaganda política etc.

18. Uso de aplicativos de mensagens (WhatsApp, Telegram etc.)

18.1. Quando for necessário utilizar aplicativos de mensagens, como WhatsApp, Telegram ou equivalentes, para tratar assuntos que envolvam as atividades profissionais, os

colaboradores:

a) Devem ter habilitado a autenticação em dois fatores para acesso ao aplicativo a ser utilizado;

b) São obrigados a conferir às informações exatamente o mesmo nível de cuidado e de confidencialidade empregado dentro das instalações e por meio dos sistemas e equipamentos da CETESB;

c) São proibidos de criar grupos com o nome ou logo CETESB, exceto quando expressamente autorizado pelo titular da unidade organizacional à qual o colaborador está vinculado, mediante justificativa quanto à necessidade do grupo;

d) Não devem postar mensagens com conteúdo humorístico, pornográfico, religioso, racista ou que expresse preconceito de qualquer natureza, correntes, ou ativismo político, bem como qualquer outro tipo de conteúdo que viole o Código de Conduta e Integridade da CETESB;

e) São proibidos disponibilizar qualquer tipo de documento de quaisquer usuários dos serviços da CETESB, tampouco de qualquer colaborador da organização ou prestador de serviço.

19. Política Mesa Limpa e Tela Protegida

19.1. Os colaboradores e todos que tenham acesso físico ou lógico à CETESB devem adotar a política “Mesa limpa e Tela Protegida”, para minimizar os riscos de acesso não autorizado, perda ou corrompimento de informações durante e fora do horário de expediente.

19.2. A política de “Mesa Limpa” é aplicada no ambiente de trabalho, em relação a papéis e mídias de armazenamento removíveis expostos sobre a mesa. Ao terminar o trabalho ou quando o colaborador não estiver fisicamente em seu posto de trabalho, nenhum documento, relatório e/ou mídia, confidencial e/ou restrito, deverá se deixado sobre sua mesa.

19.3. Os documentos com informações sensíveis ou críticas, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro.

19.4. A política de “Tela Protegida” é aplicada à sessão e ao ambiente de trabalho do colaborador em seu computador/notebook, evitando, por exemplo, que sua sessão de trabalho autenticada/registrada permaneça aberta quando estiver ausente de seu ambiente de trabalho.

19.5. Quando o computador permanecer sem uso pelo período de 15 minutos, o sistema irá bloquear a tela automaticamente.

19.6. A política de Mesa Limpa e Tela Protegida resguarda a CETESB, bem como o próprio colaborador, contra o acesso não autorizado a informações, evitando a visualização de informações expostas sobre a mesa ou na tela do computador.

20. Política de Impressão

20.1. O serviço de Impressão destina-se exclusivamente a atividades de cunho institucional.

20.2. Documentos que contenham informação classificada como confidencial ou restrita, nos termos da Cláusula 6 desta Política, bem como dados de usuários de serviços da CETESB, devem ser removidos da impressora imediatamente.

20.3. O colaborador deve imprimir somente documentos relacionados às suas atividades institucionais.

20.4. A sustentabilidade ambiental é elemento chave na utilização do serviço, a impressão de documentos e deve ser evitada sempre que possível.

a) Deve-se sempre que possível usar impressão em face dupla.

b) Deve-se buscar a tramitação de documentos de forma eletrônica.

21. Backup de Dados e Cópias

21.1. Todos os dados deverão ser protegidos através de rotinas de “backup”. Cópias de segurança dos sistemas serão executadas de forma automática, sendo o processo acompanhado pela unidade organizacional responsável pela tecnologia da informação e comunicação.

21.2. É de responsabilidade dos usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos usuários, que não sejam considerados importantes às atividades da organização.

21.3. No caso das informações consideradas importantes às atividades da organização, o usuário tem obrigação de salvá-las na pasta de rede da sua área. Estas informações serão incluídas na rotina diária de “backup” automático.

21.4. Não é permitida a cópia, reprodução ou transferência (para e-mail pessoal ou transferência digital ou física a terceiros) de informações a que os usuários tenham acesso em decorrência do exercício de suas atividades, exceto quanto previamente autorizado pelo titular da unidade

organizacional. A não observância dessa regra caracterizará a quebra da obrigação de confidencialidade a que o usuário está comprometido em razão de sua função na organização, podendo acarretar sua responsabilização civil ou criminal, conforme o caso.

22. Política de Descarte de Documentos Físicos e Eletrônicos

22.1. Todo e qualquer documento, seja físico, seja eletrônico, apenas poderá ser descartado depois de encerrado o prazo mínimo previsto para sua guarda, em conformidade com a legislação e normativa infralegal aplicável às atividades da CETESB e/ou em conformidade com o quanto pactuado em contrato ou, ainda, quando a informação nele contida esteja preservada por outro meio que garanta a observação das obrigações de guarda.

22.2. No contexto desta Política, a mídia é um mecanismo de armazenamento ou tecnicamente um suporte para informação, incluindo desde discos rígidos a mídias removíveis (Pen-drive/CD ou DVD).

a) Todos os CDs, DVDs, blue-rays deverão ser descartadas por meio de processo físico de destruição, preferencialmente, através de equipamentos específicos (Fragmentadora de papel e CD/DVD) sediados na CETESB, devendo ser documentada a realização do descarte por meio de fotografias e registros de data e hora, para evidenciar a destruição da informação;

b) Todas as fitas de back-up deverão ser destruídas (após encerramento de sua vida útil) sendo picotadas, devendo ser documentada a realização do descarte por meio de fotografias e registros de data e hora, para evidenciar a destruição da informação;

c) Todos os pen-drives, HDs, SSDs ou SSHDs devem ser encaminhados a unidade organizacional responsável pela tecnologia da informação e comunicação da CETESB para sua destruição lógica. Tendo em vista que a formatação por software convencional não é suficiente para eliminar informação em tais mídias, deve-se utilizar software específico que permita a remoção da informação de forma íntegra, antes do descarte. No caso de o equipamento não estar funcional, a unidade magnética deve ser retirada para ser limpa em outro equipamento compatível com uso de software específico. Caso a unidade não esteja funcional, ela poderá ser destruída mecanicamente.

22.3. Os documentos físicos serão descartados através de equipamentos específicos (Fragmentadora de papel e CD/DVD) sediados na CETESB, devendo ser documentada a realização do descarte por meio de fotografias e registros de data e hora, para evidenciar a destruição da informação.

23. Vigência e controle de revisões

23.1. Sem prejuízo da revisão a qualquer tempo, quando constatada sua necessidade para garantir a segurança da informação, esse documento terá validade de 24 (vinte e quatro) meses a partir da data de sua última revisão, quando necessariamente terá de ser revisto e revalidado.

Versão	Autor	Descrição	Data
01	AI/PMC	Criação	23/12/2021