Política de Segurança da Informação

CEDAE

SUMÁRIO

1. INTRODUÇÃO

A Companhia Estadual de Águas e Esgotos (CEDAE), com o intuito de instituir a cultura de Segurança da Informação na Companhia, resolve estabelecer a Política de Segurança da Informação (PSI).

2. ABRANGÊNCIA

A Política de Segurança da Informação aplica-se a:

- Todos os ambientes físicos pertencentes ao patrimônio ou sob a tutela da CEDAE;
- Todos os ambientes computacionais e ativos de informação pertencentes ou tutelados pela CEDAE;
- Todos os contratos, convênios, acordos, termos e instrumentos congêneres celebrados pela CEDAE;
- Todos os colaboradores da Companhia, abrangendo os conselheiros, diretores, extraquadro, prestadores de serviços, estagiários e aprendizes, além de consultores, fornecedores e todos os parceiros de negócio, independente da relação contratual com que se apresentem, caso acessem, armazenem, processem ou transmitam informações pertencentes ou sob guarda da CEDAE.
- Esta Política também se aplica, no que couber, ao relacionamento da CEDAE com outros órgãos e entidades públicos ou privados.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

3. OBJETIVO

A Política de Segurança da Informação tem como objetivos:

- Estabelecer diretrizes estratégicas que orientem e apoiem as ações institucionais em segurança, com o intuito de preservar, em qualquer meio, a confidencialidade, integridade, disponibilidade e autenticidade dos dados, informações e conhecimentos produzidos ou guardados pela empresa, em todo seu ciclo de vida;
- Promover práticas de segurança da informação compatíveis com o uso aceitável das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades da Companhia; e
- Promover o alinhamento das diretrizes de segurança com os objetivos estratégicos da CEDAE.

4. TERMOS E DEFINIÇÕES

4.1 Alta administração: Grupo de pessoas que dirige e controla a Companhia: administradores, conselheiros fiscais e comitê de auditoria, etc.

4.2 Ativo de Informação: Meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Para efeito desta Política, denominado como "Ativo".

4.3 Autenticidade: Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física,

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

equipamento, sistema, órgão ou entidade.

4.4 Colaboradores: Empregados, estagiários, extraquadros, terceirizados, aprendizes e aqueles que exercem mandato, cargo, emprego ou função, ainda que transitoriamente e sem remuneração, por eleição, nomeação, convênio, contratação ou qualquer outra forma de investidura ou vínculo.

4.5 Computação em Nuvem: Modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

4.6 Confidencialidade: Propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados.

4.7 Disponibilidade: Propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

4.8 Evento de Segurança: Qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.

4.9 Incidente: Interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

4.10 Incidente de Segurança: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

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

4.12 Informação Classificada: Informação classificada em grau de sigilo nos termos da LAI.

4.13 Integridade: Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.14 Necessidade de Conhecer: Condição segundo a qual o conhecimento da informação é indispensável para o adequado exercício de cargo, função, emprego ou atividade.

4.15 Privilégio Mínimo: Concessão de recursos e autorizações mínimos em um sistema de informação necessários para o adequado exercício de cargo, função, emprego ou atividade.

4.16 Risco de Segurança: Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

4.17 Tratamento de Riscos: Processo de implementação de ações de Segurança da Informação para evitar, reduzir, reter ou transferir um risco.

4.18 RCC: Rede Corporativa CEDAE.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

5. DIRETRIZES

5.1 São princípios desta Política:

5.1.1 Preservação da imagem da empresa e dos seus colaboradores;

5.1.2 Disseminação da cultura de segurança da informação;

5.1.3 Integração das ações de Segurança da Informação com os objetivos do negócio e com as demais ações dos órgãos da administração pública e da sociedade civil;

5.1.4 Incorporação da segurança da informação desde a concepção e por todo o ciclo de vida, em todos os processos e projetos executados na CEDAE.

5.2 Gestão de Segurança da Informação

5.2.1 A gestão de segurança da informação deverá ser institucionalizada na CEDAE com a seguinte composição: Diretoria Administrativa (DAD), Gerência de Tecnologia da Informação (GTI), Departamento de Suporte, Infraestrutura e Segurança da Informação (GTI-7) e a Coordenação da Segurança da Informação (GTI-72).

5.2.2 Devem ser assegurados recursos financeiros para a implantação e manutenção da Segurança da Informação, sendo previstos no Plano Diretor de Tecnologia da Informação (PDTI).

5.3 Gestão de Riscos

5.3.1 A gestão de riscos de segurança da informação deve ser realizada por meio de um processo contínuo, abrangendo as fases de análise, avaliação e tratamento dos riscos e a definição do escopo desta gestão deverá,

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

preferencialmente, manter correspondência com serviços críticos da CEDAE e estar alinhada à Política de Controles Internos e Gestão de Riscos.

5.4 Segurança Física e do Ambiente

5.4.1 O acesso aos ambientes físicos e computacionais é controlado e concedido apenas a pessoas autorizadas para o desempenho das suas atividades profissionais.

5.4.2 O acesso às instalações físicas consideradas críticas e de acesso restrito pela CEDAE, deve ser registrado de forma a permitir sua rastreabilidade.

5.4.3 As áreas críticas e de acesso restrito deverão ser identificadas para a implantação de barreiras e controles que reduzam a possibilidade de entrada de pessoas não autorizadas.

5.4.4 Os equipamentos de propriedade da CEDAE deverão ser protegidos contra ameaças físicas e ambientais, incluindo aqueles localizados ou utilizados fora de suas instalações físicas.

5.5 Controle de acesso

5.5.1 Credenciais de acesso à rede e aos sistemas de informação devem ser concedidas com base nos princípios da necessidade de conhecer e do privilégio mínimo, devendo ser monitorado, registrado, e o sistema permitirá a rastreabilidade e a identificação do usuário e as ações executadas, podendo o acesso ser revogado sem a obrigatoriedade de aviso prévio na forma do regulamento de controle de acesso.

5.6 Gestão de Ativos

5.6.1 O inventário e o mapeamento de ativos de Informação devem considerar os processos de negócios críticos, as informações classificadas conforme os requisitos legais e deverá identificar os responsáveis por cada ativo de

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

informação.

5.6.2 Os equipamentos de propriedade da CEDAE localizados ou utilizados fora de suas instalações físicas devem ser protegidos com regras de segurança.

5.6.3 Os equipamentos que não são de propriedade da CEDAE que adentrem suas instalações deverão ser protegidos com regras de segurança.

5.7 Gestão do Uso de Recursos de TIC

5.7.1 Para a realização de suas atividades internas, colaboradores e prestadores de serviços devem utilizar apenas, recursos de Tecnologia da Informação e Comunicação (TIC) previamente autorizados pela Gerência de Tecnologia da Informação (GTI).

5.7.2 Mecanismos de segurança da informação devem ser implementados para assegurar a gestão do uso de recursos computacionais, tais como, e-mail, acesso à internet, redes sociais, rede sem fio, computação em nuvem, dentre outros, sob o domínio da infraestrutura tecnológica.

5.7.3 O uso e movimentação de recursos de TIC deve ser realizado apenas quando autorizado pela GTI.

5.8 Uso Aceitável da Internet e Recursos de TIC

5.8.1 A utilização de equipamentos e recursos computacionais, incluindo os pessoais (notebooks, celulares, tablets etc.), conectados à rede da CEDAE ou nas dependências da Companhia, é controlada e está sujeita a monitoração e eventual inspeção local, na forma das normas internas da Companhia.

5.8.2 São vedados:

I. a instalação de softwares não homologados ou licenciados pela GTI;

II. o acesso ou a tentativa de acesso a recurso tecnológico do qual não seja detentor de autorização, em especial àqueles que contenham

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

conteúdo considerado ofensivo, ilegal ou impróprio;

III. a utilização dos recursos tecnológicos da CEDAE para fins estranhos às atividades institucionais;

IV. a prática de quaisquer atos tendentes a tornar indisponível qualquer recurso tecnológico sem autorização;

V. o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente de rede da CEDAE.

5.8.3 O usuário é responsável pela integridade do equipamento computacional que está operando.

5.8.4 O uso do correio eletrônico corporativo é obrigatório como meio de envio e recebimento de informações inerentes às atividades institucionais da CEDAE, vedada a sua utilização para fins particulares.

5.8.5 O acesso diário à caixa de mensagens eletrônicas corporativa é responsabilidade exclusiva do usuário.

5.8.6 As mensagens produzidas e transmitidas utilizando os recursos de comunicação eletrônica são propriedades da CEDAE.

5.8.7 Os serviços corporativos de correio eletrônico, comunicação unificada, Intranet e Internet devem ter seu uso orientado para as atividades de interesse da CEDAE.

5.8.8 O acesso à Internet no âmbito da CEDAE deve ser realizado com a finalidade exclusiva de executar as atividades de interesse público e aquelas desempenhadas pela Companhia, observando sempre a moralidade administrativa.

5.9 Contratações e Aquisições

5.9.1 Os acordos, convênios, ajustes e instrumentos congêneres sempre que aplicáveis, deverão dispor de especificações de segurança da informação que definam, no mínimo, os direitos de propriedade das informações, a classificação de

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

sigilo, estabeleçam as regras para transferência de informações e os acordos de confidencialidade e de não divulgação. Devem, ainda, prever a concordância com os procedimentos de segurança pelos seus empregados, prepostos ou representantes, sem prejuízo da participação em orientações complementares de segurança da informação que a CEDAE julgar necessárias.

5.9.2 As contratações de tecnologia devem ser precedidas de análise de riscos e da classificação de segurança das informações, nos termos da legislação pertinente em vigor, bem como pela realização de vistoria prévia (due diligence) pela Companhia, de modo a verificar se o parceiro oferece, no mínimo, a mesma segurança da informação que a CEDAE.

5.9.3 As contratações que envolvam a utilização de computação em nuvem devem conter cláusulas que estabeleçam a territorialidade de dados, garantam interoperabilidade, transferência, migração e descarte dos dados após seu encerramento.

5.10 Desenvolvimento Seguro

5.10.1 Os sistemas de informação desenvolvidos, internalizados e mantidos pela CEDAE devem ter sua segurança especificada, analisada e testada, em todo seu ciclo de vida, e estar em conformidade com os requisitos contratuais e a legislação em vigor.

5.10.2 Na ausência de definições contratuais específicas os direitos de propriedade de sistemas de informação bem como todo código-fonte desenvolvido são de propriedade da CEDAE.

5.11 Conformidade

5.11.1 Deve ser realizada a verificação de conformidade das práticas de segurança da informação da CEDAE com esta Política e demais normativos e procedimentos agregados.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

5.11.2 As atividades, produtos e serviços desenvolvidos na CEDAE devem estar em conformidade com as leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes, sejam eles internos, municipais, estaduais ou federais, inclusive os referentes à proteção das informações pessoais, profissionais e de terceiros.

5.11.3 O uso de sistemas, serviços e documentos deve estar em conformidade legal com direitos de propriedade intelectual e, portanto, com termos de licenciamento de instalação e uso.

5.12 Segurança na Gestão de Continuidade do Negócio

5.12.1 A CEDAE deve estabelecer uma estrutura de gerenciamento adequada, planos, procedimentos de recuperação e resposta a desastres que visem a identificação de potenciais ameaças e a manutenção da segurança da informação a níveis predeterminados durante eventos de interrupção.

5.12.2 Todos os sistemas críticos devem ser identificados por meio de metodologias e analisados os seus riscos e possíveis impactos sobre as operações da CEDAE.

5.12.3 Simulações e testes periódicos devem ser realizadas para identificar as vulnerabilidades e o tratamento dos riscos em caso de incidentes ou desastres que impactem na disponibilidade dos serviços críticos da CEDAE.

5.12.4 Planos de contingência devem ser elaborados para mitigar os riscos de indisponibilidade dos serviços críticos da CEDAE.

5.13 Classificação de Segurança e Tratamento da Informação

5.13.1 O tratamento da informação, abrangendo todo o seu ciclo de vida, deve seguir todas as etapas do ciclo da informação que compreende: criação, manipulação, armazenamento, transporte e descarte.

5.13.2 As diretrizes estabelecidas no processamento da informação devem

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

assegurar a adoção dos níveis de proteção adequados que garantam a disponibilidade, integridade e confidencialidade das informações, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

5.13.3 Deverão ser estabelecidos controles de segurança, softwares ou outros recursos tecnológicos que garantam a proteção da informação na tramitação de documentos sigilosos ou classificados de propriedade da CEDAE.

5.14 Governança Segura de Dados

5.14.1 Devem ser implementados processos e controles adequados para assegurar que os dados sob responsabilidade da CEDAE sejam tratados apenas para as finalidades para as quais foram coletados.

5.14.2 Todos os processos de trabalho e de atividades essenciais, que tenham processamento de informação, devem ser mapeados e modelados para fins de identificação, análise, avaliação e tratamento dos riscos.

5.14.3 O tratamento de informações em ambiente de nuvem deve ser precedido de análises de risco de segurança da informação.

5.15 Educação e Conscientização

5.15.1 Esta Política e seus documentos agregados devem ser divulgados para disseminar a cultura corporativa em Segurança da Informação.

5.15.2 De forma a reduzir os riscos à segurança da informação, todos os alcançados por esta Política devem ser informados quanto ao uso adequado e seguro dos ativos e das informações da CEDAE a que tenham acesso.

5.15.3 É responsabilidade de todos conhecer e cumprir as diretrizes, regras e ações definidas por esta Política, assim como pelas suas normas e procedimentos agregados.

5.16 Implica em violação desta Política qualquer ato que:

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

I. Exponha a Companhia ou seus colaboradores a uma perda efetiva ou potencial por meio do comprometimento da segurança dos dados, informações, imagem institucional, ou ainda da perda de equipamento;

II. Envolva a divulgação indevida de dados confidenciais ou uso não autorizado de dados corporativos;

III. Envolva o uso de dados, informações, equipamentos, softwares ou outros recursos tecnológicos para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou dispositivo legal; e

IV. A não comunicação imediata a área responsável de quaisquer descumprimentos da Política, normas ou procedimentos de segurança da informação, que porventura venha a tomar conhecimento ou presencie.

5.16.1 O não cumprimento das disposições constantes nesta Política de Segurança da Informação e suas normas internas, caracteriza infração a ser apurada, sujeitando o infrator às penalidades previstas em lei e na Política de Consequências da CEDAE.

6. ATRIBUIÇÕES E RESPONSABILIDADES

6.1 A Alta Direção e todos os Colaboradores, bem como todos aqueles que, de alguma forma, executem atividades vinculadas à CEDAE são corresponsáveis pela proteção e salvaguarda das informações a que tenham acesso em razão da execução de suas atividades, independente das medidas de segurança.

6.2 Cabe a todos garantir o tratamento seguro das informações a que tenham acesso.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

6.3 As credenciais de acesso à rede e aos sistemas de informação são pessoais e intransferíveis, sendo o usuário o responsável exclusivo pela proteção de sua identidade.

6.4 A Alta Direção e os Colaboradores da CEDAE têm a obrigação de reportar, imediatamente, qualquer evento ou incidente de segurança que tenham conhecimento, aos canais oficiais da Companhia.

6.5 Os incidentes de segurança notificados ou detectados devem ser registrados, avaliados e tratados pela Coordenação de Segurança da Informação.

6.6 Os incidentes que envolvam exposição de dados devem ser comunicados às partes interessadas, imediatamente após o conhecimento do fato, nos termos das normas da Companhia.

6.7 Os incidentes de infraestrutura computacional devem ser solucionados pela GTI (Gerência de Tecnologia da Informação).

6.8 O Gestor de segurança da informação deve definir o modelo de Prevenção, Tratamento e Respostas a Incidentes de Segurança da Informação que melhor se adeque às necessidades da CEDAE, deve também modelar o processo de gestão de incidentes, mantendo a conformidade com a legislação correspondente.

6.9 A Política de Segurança da Informação deve ser revisada sempre que necessário ou em um intervalo não superior a 04 (quatro) anos. Cabendo a Gerência de Tecnologia da Informação (GTI) a atualização desta política.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

7. DOCUMENTOS RELACIONADOS

7.1 Lei do Software- Lei n° 9.609, de 19 de fevereiro de 1998;

7.2 ABNT NBR ISO/I EC 27000- Tecnologia da Informação- Técnicas de Segurança;

7.3 Marco Civil da Internet- Lei n° 12.965, de 23 de abril de 2014;

7.4 Política de Segurança da Informação e Comunicações da Dataprev- POSIC;

7.5 Código de Ética e Conduta da CEDAE;

7.6 Política de Porta-Vozes;

7.7 Política de Consequências;

7.8 Política de Relacionamento com Agentes Públicos;

7.9 Política de Controles Internos

7.10 Política de Gestão de Riscos;

7.11 Política de Compliance;

7.12 Política de Divulgação de Atos ou Fatos Relevantes e Preservação de Sigilo;

7.13 Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021;

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

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

7.15 As normas internas estabelecem os padrões e regras a serem seguidos na CEDAE, contendo as diretrizes para execução das atividades, proibições e dá outras providências.

7.15.1 IN001 – Rede Corporativa CEDAE

7.15.1.1 Estabelece procedimentos relativos à disponibilização e utilização dos recursos de informática.

7.15.2 IN002 - Segurança da Informação

7.15.2.1 Detalha como garantir a integridade, confidencialidade, e disponibilidade das informações digitais processadas pela empresa.

7.15.3 IN003 - Serviços de Acesso Computadores e Periféricos

7.15.3.1 Orienta o usuário e gerente como proceder para a solicitação de computadores, instalação de softwares, atualizações no sistema operacional, entre outros, como também regras para a utilização e transferência de máquinas ou software.

7.15.4 IN004 - Serviços de Mensageria Digital

7.15.4.1 Detalha procedimento quanto a utilização do Correio eletrônico no envio e recebimento de mensagens, limites de tamanho de arquivo anexo, configuração de rodapé no padrão exigido pela empresa.

7.15.5 IN005 - Serviços de Acesso à Internet

7.15.5.1 Orienta como desenvolver um comportamento ético e profissional no uso da internet, guiando os usuários nos tipos permitidos de acessos e transmissão.

7.15.6 IN006 - Serviços de Acesso a Dispositivos Móveis

7.15.6.1 Estabelece critérios de manuseio e responsabilidades sobre os dispositivos móveis usados dentro ou fora das instalações físicas da CEDAE à serviço da empresa, tais como, notebook, smartphones, entre outros. Bem como

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

define permissões de acesso à Rede Corporativa CEDAE por dispositivos móveis.

7.15.7 IN007 - Solicitação de Informações Corporativas Personalizadas

7.15.7.1 Instrui na elaboração de solicitação e autorização para a preparação de consultas personalizadas ao acervo de dados corporativos armazenados em meio digital, quando as informações desejadas não estiverem disponíveis em funcionalidades dos Sistemas corporativos existentes.

8. DISPOSIÇÕES FINAIS

8.1 O detalhamento necessário à implementação desta Política está contido em instruções normativas internas de segurança específicos, descrito no item 7.15 desta Política.

8.2 Os casos omissos, as situações especiais e demais diretrizes necessárias à implantação desta Política devem ser analisadas e deliberadas pelo setor responsável pela segurança da informação na CEDAE.

8.3 Esta Política dá ciência a todos que as ações executadas nos ambientes físicos, nos ambientes computacionais, nos ativos e nos recursos computacionais da CEDAE poderão ser monitoradas, registradas e auditadas, conforme previsto na legislação brasileira.

8.4 Esta política entra em vigor na data de sua aprovação pelo Conselho de Administração.

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br

9. INFORMAÇÕES DE CONTROLE

9.1 Etapas de Aprovação

Responsável	Área	Assinatura
Elaboração	Assessoria de Privacidade e Proteção de Dados	
Revisão	Gerência de *Compliance*	
	Assessoria de Governança Corporativa	
Aprovação	Conselho de Administração	

9.2 Controle de Alterações

N° da Alteração	Data do documento	Descrição da alteração
V. 1	07/06/2022	Primeira versão

Av. Pres. Vargas, 2655. Cidade Nova. Rio de Janeiro. CEP 20.210-030
www.cedae.com.br


CEDAE