DELIBERAÇÃO Nº 4935/2022

APROVANDO A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA ESPIRITO SANTENSE DE SANEAMENTO – CESAN, usando de atribuições que lhe são conferidas pelo Estatuto,
RESOLVE:

Artigo 1º – Aprovar a Política de Segurança da Informação – INS.027.00.2022.

Artigo 2º – Esta Deliberação entra em vigor nesta data, revogadas as disposições em contrário.

Vitória, 25 de Janeiro de 2021.

RAFAEL GROSSI GONCALVES PACIFICO:05124776633
Assinado de forma digital por RAFAEL GROSSI GONCALVES PACIFICO:05124776633 Dados: 2022.01.26 13:07:15 -03'00'

Rafael Grossi Gonçalves Pacifico
PRESIDENTE DO C.A.

CARLOS AURELIO LINHALIS:72383682772
Assinado de forma digital por CARLOS AURELIO LINHALIS:72383682772 Dados: 2022.01.26 16:18:03 -03'00'

Carlos Aurélio Linhalis
CONSELHEIRO

PEDRO MENEGUETTI:41835484620
Assinado de forma digital por PEDRO MENEGUETTI:41835484620 Dados: 2022.01.25 17:02:55 -03'00'

Pedro Meneguetti
CONSELHEIRO

JOSE ALVES PAIVA:04980034772
Assinado de forma digital por JOSE ALVES PAIVA:04980034772 Dados: 2022.01.26 10:04:47 -03'00'

José Alves Paiva
CONSELHEIRO

MARCELO CAMPOS ANTUNES:03171117797
Assinado de forma digital por MARCELO CAMPOS ANTUNES:03171117797 Dados: 2022.01.25 20:36:17 -03'00'

Marcelo Campos Antunes
CONSELHEIRO

JOSE MARCOS TRAVAGLIA:56063601791
Assinado de forma digital por JOSE MARCOS TRAVAGLIA:56063601791 Dados: 2022.01.26 07:42:06 -03'00'

José Marcos Travaglia
CONSELHEIRO

FABIANO VENTURIM CANAL:05476746781
Assinado de forma digital por FABIANO VENTURIM CANAL:05476746781 Dados: 2022.01.25 16:32:13 -03'00'

Fabiano Venturim Canal
CONSELHEIRO

956ª Reunião do C.A.
Processo nº 2021.022184

COMPANHIA ESPÍRITO SANTENSE DE SANEAMENTO – CESAN

SEGURANÇA DA INFORMAÇÃO

INS.027.00.2022

Revisão:	Proposta:	Processo:	Aprovação:	Páginas:
00	P-CRC	2021.022184	Deliberação 4935/2022	11

SUMÁRIO

1 OBJETIVO

Estabelecer as diretrizes necessárias para assegurar a confidencialidade, integridade e disponibilidade da informação e dos dados pessoais sob responsabilidade da Cesan.

2 CAMPO DE APLICAÇÃO

Aplica-se a todas as Unidades da Cesan.

3 UNIDADE RESPONSÁVEL

A atualização e manutenção desta Norma é responsabilidade da Coordenadoria de Riscos e Conformidade em conjunto com o Comitê de Privacidade.

4 DEFINIÇÕES

4.1 AMEAÇA

Conjunto de fatores externos ou causa potencial de um incidente indesejado, que possa resultar em dano para um sistema ou unidade da estrutura organizacional da Cesan.

4.2 ATIVO

Qualquer recurso que tenha valor para a Cesan.

4.3 RECURSO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (RECURSO DE TIC)

a) Todos os equipamentos e serviços de informática e telecomunicações fornecidos pela área de TI aos usuários para desempenho exclusivo de suas funções relacionadas

a Cesan. Exemplos de equipamentos: computadores, notebooks, tablets, smartphones, telefones celulares, impressoras e servidores; Exemplos de serviços: software, sistemas, rede corporativa de dados, acesso à internet, email, telefonia fixa e móvel.
b) Equipamentos portáteis são aqueles que o usuário leva facilmente para o desempenho de suas atividades. Exemplos: celular, notebook, smartphone, modem 3G/4G e tablet.

4.4 AUTENTICIDADE

A informação será proveniente de sua fonte, sem sofrer alteração no decorrer do processo.

4.4 COMITÊ DE PRIVACIDADE

Comitê designado pela Diretoria da Cesan que tem como principal atribuição debater os temas relativos à segurança, proteção e privacidade dos dados.

4.5 CONFIDENCIALIDADE

A informação será acessada e utilizada somente pelos usuários cuja permissão lhe tenha sido concedida previamente em razão de sua função, para atender às exigências do exercício de suas atividades profissionais.

4.6 CONTROLE DE ACESSO

Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.7 DADOS

Parte elementar da estrutura do conhecimento incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis.

4.8 DADO PESSOAL

Informação relacionada a pessoa natural identificada ou identificável, como por exemplo: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet), cookies.

4.9 DISPONIBILIDADE

A informação será para o uso legítimo dos usuários autorizados.

4.10 COOKIES

Na terminologia da informática, pequenos arquivos de texto depositados por um site no computador do usuário para “memorizar” algumas informações relativas àquela navegação.

4.11 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Ocorrência identificada de sistema, dados, informações, serviço ou rede, ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

4.12 INFORMAÇÃO

Informação é o conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento.

4.13 INTEGRIDADE

A informação será correta, verdadeira e não corrompida.

4.14 LEGALIDADE

A informação deve atender a requisitos legais e em conformidade com a legislação vigente.

4.15 RISCO

Combinação da probabilidade de um evento e de suas consequências que podem causar danos a uma organização, perda de informações, perda financeira, parada de um serviço.

4.16 SEGURANÇA DA INFORMAÇÃO

Visa preservar os princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade, de modo a proteger a informação dos diversos tipos de ameaças.

4.17 USUÁRIO

Empregados, estagiários, adolescentes aprendizes e contratados autorizados a utilizar os recursos de TIC da Cesan.

4.18 VIOLAÇÃO DE DADOS PESSOAIS

É um incidente de segurança envolvendo dados pessoais.

4.19 VULNERABILIDADE

Fragilidade de um ativo ou um grupo de ativos que pode vir a ser explorada por uma ou mais ameaças.

5 DISPOSIÇÕES GERAIS

Esta Política deve ser interpretada de forma restritiva, ou seja, o que não estiver expressamente permitido somente deve ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

A violação a qualquer dispositivo desta Política está sujeita a aplicação das penalidades cabíveis de acordo com os normativos internos da CESAN, sem prejuízo das demais penalidades previstas na legislação e regulamentação aplicável.

Esta Política deverá servir de orientação para a elaboração de demais normativos sobre assuntos que venham a tangenciar o uso de informações (incluindo dados pessoais) e consequentemente a necessidade de observar a sua proteção, garantindo os atributos de Disponibilidade, Integridade, Confidencialidade, Autenticidade e Legalidade.

Deverão ser observadas as seguintes diretrizes:

a) Esta Política será divulgada no sítio eletrônico da Cesan.
b) As informações (incluindo dados pessoais) geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos usuários, bem como os demais ativos disponibilizados, são de propriedade ou de responsabilidade da Cesan e devem ser empregados unicamente para fins profissionais.

c) É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, da Cesan em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto, até mesmo no âmbito acadêmico.

d) Os usuários devem garantir a proteção dos dados que manipulam em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte;

e) Os recursos de TIC de propriedade da Cesan devem ser utilizados para fins profissionais e aprovado administrativamente.

f) Os recursos de TIC portáteis são utilizados somente quando fornecidos ou autorizados pela Cesan. Além disso, são diretamente relacionados a uma justificativa do negócio, com motivo profissional, no âmbito das atribuições do usuário.

g) É vedado aos usuários o uso de repositórios digitais não homologados pela área de Tecnologia da Informação, para armazenar e publicar informações ou dados pessoais de propriedade ou sob a responsabilidade da Cesan.

h) A Cesan possui documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus ativos e recursos de TIC.

i) A Cesan mantém processo de salvaguarda e restauração das informações e de sistemas, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

j) A Cesan analisa, em intervalos regulares, seus processos e recursos de TIC, visando assegurar que estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

k) A Cesan mantém uma equipe de resposta a incidentes em segurança cibernética, segurança da informação e de privacidade, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança.

l) O planejamento, desenvolvimento e revisão de processos, sistemas e novos projetos são executados considerando a segurança da informação e privacidade.

5.1 DOS PAPÉIS E RESPONSABILIDADES

5.1.1 Dos Gestores

a) Fazer cumprir e gerenciar o cumprimento desta Política por parte dos usuários sob sua gestão.
b) Gerenciar os controles de segurança da informação e privacidade específicos dos processos de sua Unidade, especialmente daquelas atividades que não sejam dependentes de recursos de TIC.
c) Implementar ou solicitar os controles adicionais de segurança necessários e capazes de garantir a continuidade do negócio da sua Unidade.
d) Identificar eventos de segurança de informação e privacidade ou qualquer ação duvidosa praticada por seus usuários, adotando medidas corretivas e disciplinares apropriadas.
e) Analisar a concessão de acesso, validar e fiscalizar o uso da informação e definir controles.

5.1.2 Dos Usuários

a) Cumprir e manter-se atualizado com esta Política.
b) Conhecer e assinar o Termo de Confidencialidade, quando aplicável.
c) Utilizar de forma responsável, profissional, ética e legal as informações e os recursos de TIC institucionais homologados, respeitando os direitos e as permissões de uso concedidas pela Cesan.
d) Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações e dados pessoais acessados ou manipulados, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia.
e) Não revelar qualquer informação ou dado pessoal de propriedade ou sob a responsabilidade da Cesan sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico.

f) Responder pela segurança das informações as quais tem acesso em meio físico ou digital.
g) Evitar a exposição desnecessária de informações as quais tem acesso, ainda que seja objeto de sua função.
h) Zelar pelo recurso de tecnologia da informação disponibilizado pela Cia.

5.1.3 Da Unidade de Tecnologia da Informação

a) Prover condições técnicas adequadas para o cumprimento das diretrizes de segurança da informação.
b) Coordenar a gestão da continuidade de negócio, garantindo, no âmbito de sua atuação, a utilização de metodologias, técnicas e ferramentas de segurança da informação.
c) Realizar a gestão, inclusive da segurança da informação e privacidade, dos Recursos de TIC de propriedade da Cesan ou que estão sob sua responsabilidade.
d) Apoiar as Unidades Organizacionais na definição de controles adequados de segurança da informação e privacidade.
e) Identificar e avaliar os riscos relacionados aos Recursos de TIC e propor melhorias, quando couber.
f) Garantir que todos os Recursos de TIC em uso no ambiente corporativo da Cesan atendam as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança;
g) Mapear e inventariar os Recursos de TIC da Cesan.
h) Realizar o monitoramento dos ambientes lógicos visando à eficácia dos controles implantados, a proteção de seu patrimônio e a reputação da Cesan.

6 DOCUMENTOS DE REFERÊNCIA

LEI Nº 13.709/18: Lei Geral de Proteção de Dados Pessoais (LGPD);

ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;

ABNT NBR ISO/IEC 27032:2015: Tecnologia da Informação — Técnicas de Segurança — Diretrizes para Segurança Cibernética;

ABNT NBR ISO/IEC 27701:2019: Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes;

7 CONSIDERAÇÕES FINAIS

Os casos omissos serão resolvidos a critério do Conselho de Administração.