casal
Nossa água é o futuro

Política de Segurança da Informação

2024

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI) estabelecida pela Companhia de Saneamento de Alagoas tem como objetivo principal proteger os ativos de informação, garantir a confidencialidade, integridade e disponibilidade dos dados, além de promover a conscientização e a adoção de boas práticas de segurança.

Essa política é aplicável a todas as áreas e setores da organização, independentemente de sua localização geográfica ou função desempenhada. Todos os usuários abrangidos por esta política têm a responsabilidade de aderir às diretrizes e procedimentos estabelecidos, bem como de proteger os recursos de TI da empresa.

2. ABRANGÊNCIA

Esta política abrange todos os empregados, contratados, prestadores de serviços e quaisquer indivíduos permitidos a acessar os recursos de Tecnologia da Informação (TI) da Companhia de Saneamento de Alagoas, incluindo usuários externos que utilizam os sistemas e informações da Companhia. Ela engloba todos os ativos de TI da CASAL, como redes, servidores, dispositivos em geral, dispositivos de armazenamento, recursos de nuvem, sistemas contratados que contenham dados da empresa, aplicativos e quaisquer meios de comunicação aplicáveis.

A Política de Segurança da Informação (PSI) deve ser revisada periodicamente para garantir sua relevância contínua, efetividade e aderência às melhores práticas. As revisões devem ser realizadas em intervalos predefinidos, e também em cenários específicos, como mudanças significativas na empresa, evolução tecnológica e novas ameaças à segurança da informação.

As revisões devem ser realizadas de forma sistemática, abrangente e documentada, garantindo que a política se mantenha relevante, envolvendo a participação de partes interessadas relevantes, como a equipe de TI, gestores, especialistas em conformidade e demais profissionais envolvidos no gerenciamento de riscos de TI.

3. OBJETIVOS

3.1 Assegurar o uso apropriado dos recursos de TI: Estabelecer diretrizes claras sobre o uso adequado dos recursos de TI dentro da organização, garantindo que sejam utilizados apenas para fins relacionados ao trabalho e em conformidade com as políticas internas e regulamentações aplicáveis;

3.2 Garantir a conformidade legal e regulatória: Assegurar que a organização cumpra todas as leis, regulamentos e requisitos aplicáveis relacionados à proteção de dados, privacidade, segurança da informação e propriedade intelectual, reduzindo os riscos de não conformidade e possíveis penalidades legais;

3.3 Preservar a segurança da informação: Implementar controles e medidas de segurança adequados para proteger os ativos de TI da organização, incluindo sistemas, redes, dados e informações confidenciais. Isso envolve a prevenção de acesso não autorizado, a detecção de atividades maliciosas, a proteção contra ameaças internas e externas, bem como a implementação de práticas de segurança de dados e backup;

3.4 Promover a eficiência e a produtividade: Estabelecer diretrizes para o uso eficiente dos recursos de TI, incentivando o uso adequado das tecnologias disponíveis, o compartilhamento de informações, a colaboração e a adoção de melhores práticas. Isso visa aumentar a produtividade dos empregados e melhorar os processos de negócios por meio do uso efetivo da tecnologia;

3.5 Fomentar a conscientização e a educação em segurança da informação: Promover a conscientização dos usuários de TI sobre os riscos de segurança e a importância da proteção da informação. Isso inclui a implementação de programas de treinamento, a divulgação de políticas de segurança, a realização de campanhas educativas e a promoção de uma cultura de segurança cibernética dentro da organização.

4. PRINCÍPIOS

4.1 Segurança da Informação: O princípio fundamental desta política de TI é garantir a segurança, confidencialidade, integridade e disponibilidade dos recursos de TI da CASAL. Ela também visa proteger os dados da CASAL contra acesso não autorizado, uso indevido ou divulgação sem o consentimento.

4.2 Uso Responsável: Todos os usuários de recursos de TI devem utilizá-los de forma responsável e em conformidade com as políticas e diretrizes estabelecidas. Isso significa utilizar os recursos de TI exclusivamente para fins autorizados e relacionados ao trabalho, evitando o acesso, armazenamento ou transmissão de conteúdo ilegal, ofensivo ou que viole direitos de propriedade intelectual.

4.3 Conformidade Legal e Regulatória: A política de TI deve estar alinhada às leis, regulamentos e requisitos legais aplicáveis à organização.

4.4 Acessibilidade e Disponibilidade: Os recursos de TI devem ser acessíveis e estar disponíveis para os usuários autorizados de forma confiável e contínua. Isso envolve a implementação de infraestrutura robusta, procedimentos de backup e recuperação de dados, manutenção preventiva e solução rápida de problemas técnicos. A organização deve garantir que os serviços de TI essenciais sejam mantidos em funcionamento, minimizando interrupções e tempo de inatividade, de modo a apoiar as operações e os processos de negócio.

4.5 Melhoria Contínua: A política de TI deve ser revisada periodicamente para garantir sua eficácia e relevância contínuas. A organização deve buscar constantemente melhorar suas práticas e controles de TI, acompanhar as tendências e as melhores práticas do setor, bem como avaliar e responder a novos riscos e desafios de segurança da informação. A colaboração entre as equipes de TI, os usuários e a alta administração é fundamental para identificar oportunidades de melhoria e implementar ações corretivas e preventivas.

5. DIRETRIZES GERAIS

5.1 CLASSIFICAÇÃO DA INFORMAÇÃO

A CASAL reconhece a importância da classificação das informações de acordo com a legislação em vigor e vem implementando medidas com base na confidencialidade, integridade, disponibilidade e requisitos das partes interessadas relevantes.

A classificação da informação será revisada periodicamente para garantir sua relevância e atualização de acordo com as mudanças na legislação, regulamentações e requisitos internos da empresa. Isso assegura que as medidas de segurança sejam consistentes com as necessidades atuais de proteção da informação.

A empresa reconhece a importância de classificar os dados pessoais de acordo com sua sensibilidade e estabelecer diretrizes claras para o tratamento adequado dessas informações.

Dados pessoais são informações relacionadas à pessoa natural. Dados sensíveis são informações 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.

5.2 PRIVACIDADE

A privacidade dos colaboradores, clientes e demais partes interessadas é de extrema importância a Companhia compromete-se a proteger as informações coletadas, armazenadas e processadas, em conformidade com as leis e regulamentações aplicáveis, conforme regulamento na política de privacidade de dados.

A CASAL utilizará as informações pessoais quando necessárias à realização de suas atividades e prestação de serviços.

As informações pessoais coletadas serão utilizadas apenas para os fins aos quais foram fornecidas, de acordo com as finalidades determinadas e legítimas da CASAL.

A CASAL poderá compartilhar informações pessoais com terceiros somente quando necessário para a prestação de serviços, cumprimento de obrigações legais ou mediante consentimento expresso do titular das informações. Esses terceiros estão sujeitos a obrigações contratuais de confidencialidade e segurança das informações compartilhadas.

A CASAL adota medidas técnicas, organizacionais e administrativas adequadas para proteger as informações pessoais contra perda, roubo, uso indevido, acesso não autorizado, divulgação ou alteração não autorizada. Essas medidas incluem controles de acesso, criptografia, firewalls, treinamentos e monitoramento de sistemas regulares.

A CASAL em conformidade com a Legislação em vigor, com foco na LGPD, respeita os direitos dos Titulares de Dados.

5.3 USO DE DISPOSITIVOS PESSOAIS NA EMPRESA

5.3.1 Dispositivos Pessoais

5.3.1.1 Permissão de Uso

5.3.1.1.1 O uso de dispositivos pessoais na rede da empresa, incluindo redes cabeadas e wireless, é permitido desde que os funcionários sigam as diretrizes de segurança estabelecidas nesta política;

5.3.1.1.2 Os dispositivos pessoais devem ser registrados e autorizados antes de serem conectados à rede wireless e cabeada. Isso pode ser feito por meio de um processo de solicitação de acesso e aprovação pela equipe de TI;

5.3.1.1.3 Os dispositivos pessoais devem apresentar configurações mínimas de segurança, incluindo software antivírus, sistema operacional licenciado e atualizado.

5.3.1.1.4 Os dispositivos pessoais conectados às redes devem ser segregados da rede corporativa principal, com acesso restrito a recursos e sistemas críticos.

5.3.1.1.5 Os empregados são responsáveis por garantir a integridade e a segurança de seus dispositivos pessoais, incluindo o uso de senhas fortes e a proteção contra perda ou roubo;

5.3.1.1.6 Os empregados são exclusivamente responsáveis pela verificação, atualização e manutenção adequada dos softwares existentes em seus dispositivos pessoais. A empresa não se responsabiliza por quaisquer danos ou prejuízos causados por ações irregulares decorrentes de softwares desatualizados ou não autorizados.

5.4 RECURSOS DE TI

5.4.1 Computadores, equipamentos e recursos de informática

A Companhia disponibilizará sempre que possível, estes recursos para realizar suas atividades. Esses dispositivos serão configurados de acordo com os padrões e requisitos da empresa.

5.4.2 Ambiente On-Premises

A empresa pode optar por hospedar servidores em seu próprio local físico, o que significa que os servidores e infraestrutura de TI serão instalados e mantidos internamente.

5.4.3 Ambiente de nuvem

A empresa pode optar por hospedar servidores em um ambiente de nuvem, utilizando provedores de serviços em nuvem confiáveis e seguros.

5.4.4 Dispositivos móveis

A empresa pode fornecer aos empregados dispositivos móveis, como smartphones ou tablets, para facilitar o acesso às informações e permitir a comunicação em tempo real.

5.4.5 Softwares

A Casal utilizará softwares licenciados assegurando o cumprimento das obrigações legais, evitando riscos relacionados a violações de direitos autorais e segurança da informação.

5.4.6 Contas de E-mails

5.4.6.1 Todos os empregados devem possuir contas de e-mails corporativos para comunicação profissional e acesso aos sistemas disponíveis no âmbito da empresa;

5.4.6.2 As contas de e-mail setoriais existentes no organograma são de responsabilidade dos gestores de cada setor, que são responsáveis por administrar e controlar o acesso às contas de e-mail. A CASAL não cria contas de e-mail para estagiários, jovens aprendizes ou prestadores de serviços. Entretanto, permitirá a criação de nomes personalizados de e-mail no formato de aliás, de caráter temporário.

5.4.6.3 A CASAL poderá permitir a criação de contas de e-mail ou alias para prestadores de serviços que trabalhem diretamente na área de TI. Essa permissão será concedida com o único objetivo de garantir a segurança dos dados trafegados e assegurar um gerenciamento eficaz dos recursos de TI. A criação de contas de e-mail ou alias para prestadores de serviços na área de TI será autorizada e monitorada pela Gerência responsável pela gestão de TI da CASAL.

5.4.6.4 É obrigatório o uso de autenticação em dois fatores para acesso às contas de e-mails.

5.4.6.5 A Gerência de TI deve implementar medidas de proteção para prevenir o acesso não autorizado às contas de e-mails, como a detecção de atividades suspeitas e o monitoramento de logs;

5.4.6.6 As contas de e-mails setoriais extintos ou de empregados com vínculo de trabalho extinto ou suspenso, devem ser desabilitadas ou removidas.

5.4.6.7 Será permitida a transferência de backup de dados da conta setorial extinta para outra conta, conforme solicitação do gestor responsável pelo novo setor.

5.4.7 Ambiente colaborativo

A CASAL oferece diversas ferramentas e aplicativos que facilitam a comunicação, colaboração e compartilhamento de informações entre os membros da equipe.

5.4.8 Redes

A infraestrutura de rede disponível para conexão dos dispositivos entre si e à internet consiste em um conjunto de redes, incluindo uma rede cabeada e uma rede sem fio.

5.4.9 Armazenamento

Os usuários devem utilizar os servidores de arquivos designados pela empresa para armazenar e compartilhar seus dados de trabalho. Além disso, quando necessário, a empresa pode fazer uso de ambientes contratados para o armazenamento de dados, seguindo os procedimentos e políticas de segurança estabelecidos.

5.4.10 Backup

Os backups devem ser programados e executados de forma regular, com a definição de horários, frequência e métodos apropriados.

Os usuários são responsáveis pela preservação e conservação dos dados armazenados nos equipamentos e sistemas de TI de sua utilização ou responsabilidade.

5.4.11 Internet

A empresa monitora o uso da Internet através dos serviços de firewall e bloqueio de conteúdo duvidoso. Esse monitoramento é realizado para proteger a segurança das informações, prevenir atividades prejudiciais e garantir a conformidade com as políticas estabelecidas.

5.4.12 Sistemas

5.4.12.1 Os usuários têm a responsabilidade de utilizar os sistemas da empresa, em conformidade com as diretrizes estabelecidas. Essas responsabilidades incluem:

5.4.12.2 Utilizar os sistemas exclusivamente para fins relacionados ao trabalho e de acordo com as políticas estabelecidas pela empresa;

5.4.12.3 Ser responsável pelo acesso, modificação, cópia ou distribuição de informações confidenciais ou restritas, respeitando os níveis apropriados de autorização;

5.4.12.4 Não compartilhar senhas e/ou credenciais de acesso com terceiros, garantindo a confidencialidade e segurança dos sistemas;

5.4.12.5 Abster-se de realizar atividades que possam comprometer a segurança dos sistemas, como introduzir vírus ou realizar tentativas de invasão.

5.4.12.6 Informar imediatamente a equipe de TI sobre qualquer problema ou incidente relacionado aos sistemas, a fim de agir prontamente e mitigar possíveis danos.

5.4.12.7 Para preservar a segurança e confidencialidade das informações, é estritamente proibido compartilhar com terceiros quaisquer conteúdos, como fotos ou capturas de tela, dos sistemas utilizados pela CASAL.

5.5 SEGURANÇA

Essas medidas são fundamentais para proteger os sistemas, dados e informações da CASAL contra ameaças internas e externas.

5.5.1 Senhas Fortes e Complexas

Os empregados devem utilizar senhas fortes e complexas para proteger suas contas e os sistemas da empresa. Isso inclui o uso de senhas com uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais e uma extensão adequada.

5.5.2 Alteração Regular de Senhas

Para garantir a segurança contínua, os empregados devem alterar suas senhas regularmente.

5.5.3 Firewall e Controle de Acesso

A Companhia mantém um firewall atualizado para monitorar e controlar o tráfego de rede.

5.5.4 Monitoramento de Acesso e Atividades

A empresa realizará monitoramento contínuo das atividades de acesso aos sistemas e redes.

5.5.5 Conscientização e Treinamento

A empresa fornecerá treinamento quando necessário sobre boas práticas de segurança.

5.6 HELPDESK

A CASAL disponibilizará ferramentas para registro de chamados de suporte e manutenção de equipamentos.

6. DEVERES E RESPONSABILIDADES

6.1 ALTA GESTÃO;

6.1.1 Desempenhar um papel fundamental na política de segurança da informação;

6.1.2 Estabelecer uma cultura de segurança da informação, promovendo a conscientização e a importância da proteção dos ativos de TI;

6.1.3 Designar recursos adequados para implementar e manter a política de TI, incluindo orçamento, pessoal e tecnologias necessárias;

6.1.4 Definir as diretrizes estratégicas e objetivos para a segurança da informação e monitorar sua conformidade;

6.1.5 Assegurar que sejam realizadas avaliações periódicas de riscos e que as medidas apropriadas sejam tomadas para mitigar os riscos identificados;

6.1.6 Apoiar à equipe de TI para implementar e fazer cumprir as políticas de segurança.

6.2 TECNOLOGIA DA INFORMAÇÃO

6.2.1 A Gerência de Tecnologia da Informação (GETIN) é responsável por garantir o planejamento, implementação e gerenciamento efetivo dos recursos de TI da CASAL, incluindo hardware, software e rede;

6.2.2 Estabelecer políticas de segurança da informação e garantir a conformidade com as leis e regulamentações aplicáveis;

6.2.3 Realizar backups regulares dos dados e implementar planos de contingência em caso de interrupções ou falhas;

6.2.4 Fornecer suporte técnico e treinamento aos usuários;

6.2.5 Monitorar regularmente os sistemas de TI para identificar possíveis vulnerabilidades ou violações de segurança;

6.2.6 Implementar e gerenciar controles de segurança para proteger os ativos de TI da organização, incluindo sistemas, redes, dados e infraestrutura;

6.2.7 Realizar avaliações regulares de riscos de segurança e identificar medidas de mitigação apropriadas;

6.2.8 Garantir a conformidade com as políticas e procedimentos de segurança da informação estabelecidos;

6.2.9 Monitorar a infraestrutura de TI, detectar e responder prontamente a incidentes de segurança;

6.2.10 Conduzir investigações quando necessário;

6.2.11 Manter-se atualizado sobre as tendências de segurança da informação e implementar as melhores práticas;

6.2.12 Fornecer treinamento e conscientização em segurança da informação para os empregados;

6.2.13 Estabelecer e manter acordos de níveis de serviço (SLAs) para garantir a disponibilidade e desempenho adequados dos sistemas de TI.

6.3 EMPREGADOS, CONTRATADOS, PRESTADORES DE SERVIÇOS E DEMAIS USUÁRIOS

6.3.1 Cumprir as diretrizes estabelecidas na política de TI e outras políticas relacionadas;

6.3.2 Utilizar os recursos de TI somente para fins autorizados e relacionados ao trabalho;

6.3.3 Proteger suas credenciais de acesso, como senhas e identificações, e não as compartilhar com terceiros;

6.3.4 Relatar prontamente quaisquer incidentes de segurança ou suspeitas de violações de segurança à equipe de TI;

6.3.5 Contribuir para a conscientização em segurança da informação, participando de treinamentos e seguindo as práticas recomendadas;

6.3.6 Compreender e aderir às políticas de uso aceitável dos recursos de TI, incluindo a proibição de atividades não autorizadas ou ilegais;

6.3.7 Colaborar com a equipe de TI na implementação de medidas de segurança e proteção dos ativos de TI da organização.

7. DANOS E PREJUÍZOS

A responsabilidade por quaisquer violações, danos ou prejuízos causados aos ativos de TI será tratada de acordo com as normas internas e legislação vigente.

8. CONSIDERAÇÕES FINAIS

O desconhecimento e compromissos estabelecidos neste documento não exime os usuários de suas responsabilidades no uso dos recursos de TI da empresa.

9. REFERÊNCIAS

Código de Conduta e Integridade da CASAL

Lei Geral de Proteção de Dados - LGPD

A Lei Geral de Proteção de Dados (LGPD), regulamentada pela Lei 13.709/2018, é uma legislação que estabelece diretrizes para o tratamento de dados pessoais, com o objetivo de garantir a privacidade, a segurança e os direitos dos indivíduos em relação às suas informações pessoais.

Lei de acesso à Informação - LAI

A Lei de Acesso à Informação (Lei 12.527/2011) é uma legislação que regulamenta o acesso dos cidadãos às informações públicas, promovendo a transparência e o controle social. A Política de Segurança da empresa está alinhada com a Lei de Acesso à Informação (LAI) e estabelece diretrizes para assegurar o acesso apropriado e seguro às informações.

Lei das Estatais

A Lei das Estatais (Lei 13.303/2016) estabelece normas para as empresas estatais, visando aprimorar a governança, a transparência e a eficiência na gestão dessas entidades.

Norma Técnica ABNT NBR ISO/IEC 27001:2022

A Norma Técnica ABNT NBR ISO/IEC 27001:2022 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização. Ela oferece diretrizes detalhadas para identificar os riscos de segurança da informação e implementar controles adequados para mitigar esses riscos. A norma também estabelece um processo de melhoria contínua, permitindo que a organização mantenha sua postura de segurança atualizada e eficaz.

Norma Técnica ABNT NBR ISO/IEC 27002:2022

Fornece diretrizes para práticas de gestão de segurança da informação. Ela abrange uma ampla gama de controles de segurança da informação que podem ser implementados pela organização, abordando áreas como política de segurança, gestão de ativos, acesso físico e lógico, criptografia, segurança em redes, gerenciamento de incidentes, entre outros

10. GLOSSÁRIO

On-Premises

On-Premises refere-se a um ambiente de TI em que os servidores, equipamentos de rede e outros recursos de tecnologia estão fisicamente localizados nas instalações da organização, em vez de estarem hospedados em um data center remoto ou na nuvem.

Hardware

Hardware é o conjunto de componentes físicos que compõem um sistema de computador. Incluindo dispositivos como servidores, computadores, roteadores, switches, discos rígidos, memórias, entre outros. Em uma política de segurança de TI, o termo hardware abrange todos os dispositivos físicos que devem ser protegidos contra acessos não autorizados, falhas ou danos.

Cibernética

No contexto da segurança de TI, o termo é frequentemente usado em "segurança cibernética", que se refere à proteção de sistemas de informação contra ataques, acessos não autorizados, e outros tipos de ameaças digitais.

Wireless

Wireless refere-se a uma forma de comunicação sem fio entre dispositivos, utilizando ondas de rádio ou outras tecnologias sem fio, como Wi-Fi ou Bluetooth.

Firewalls

Firewalls são sistemas de segurança que monitoram e controlam o tráfego de rede com base em regras de segurança predefinidas. Eles atuam como uma barreira entre redes confiáveis e não confiáveis, como a internet, impedindo que tráfego malicioso entre na rede interna da organização e protegendo os dados e sistemas de ataques externos.

Helpdesk

Helpdesk é um serviço de suporte técnico oferecido dentro de uma organização para ajudar os usuários a resolver problemas relacionados a TI, como dificuldades com softwares, hardware, acesso a sistemas, e outros.

Backup

É uma cópia de segurança dos dados de um dispositivo de armazenamento ou sistema para outro ambiente a fim de que possam ser restaurados em caso de perda.

Software

É uma sequencia de instruções inscritas para serem interpretadas por um computador para executar tarefas específicas e fornece instruções para o hardware.

Ambiente de nuvem

É o espaço no qual dados, software, aplicativos e serviços são hospedados por provedores

11. HISTÓRICO DE MODIFICAÇÕES

Versões		Data	Resumo Histórico de Revisões (Motivo da Alteração)	Nº. pg.
V. 00		31/10/2024	Emissão Inicial	Todas
Última Revisão	V.01			

Responsável pela Elaboração / Área Pertinente	Responsável pela Revisão/Estruturação: Revisão: GEPLAN/SUDEO
Livia Maria Soares Dias – SUDEO Inaldo José Lourenço- GETIN Marcio Xavier dos Santos - GEGOC	Livia Maria Soares Dias – SUDEO Cynthia Ferreira Calixto de Oliveira – GEPLAN Lais Lima de Souza Leão – SUJUR