POLÍTICA SEI Nº 0024206261/2025 - CAJ.CONSAD

Joinville, 17 de janeiro de 2025.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A segurança da informação é essencial para proteger os ativos da organização e mitigar riscos em um ambiente de constante evolução tecnológica. Esta Política de Segurança da Informação (PSI) estabelece diretrizes práticas e estratégicas para proteger informações, assegurar a continuidade do negócio e garantir a conformidade com leis e regulamentações aplicáveis.

Esta PSI está fundamentada em dois referenciais reconhecidos globalmente: a ISO/IEC 27002:2022, que oferece um conjunto abrangente de práticas para a gestão da segurança da informação, e os CONTROLES CIS 8, que fornecem controles priorizados para enfrentar ameaças cibernéticas modernas.

Combinando abordagens estratégicas e práticas, esta política busca criar um ambiente seguro, resiliente e adaptado às demandas tecnológicas e organizacionais atuais.

2. OBJETIVOS

Esta política tem como objetivo estabelecer diretrizes para a gestão da segurança da informação, permitindo que os usuários de TI da CAJ adotem comportamentos alinhados às necessidades do negócio, à mitigação de riscos cibernéticos e à conformidade com requisitos legais e regulatórios.

Proteger os ativos de informação da CAJ por meio da aplicação de controles que garantam:

I - **Integridade:** Assegurar que as informações sejam mantidas em seu estado original, protegendo-as contra alterações indevidas, intencionais ou acidentais, tanto na guarda quanto na transmissão.

II - **Confidencialidade:** Garantir que o acesso às informações seja restrito a pessoas devidamente autorizadas.

III - **Disponibilidade:** Garantir que os usuários autorizados tenham acesso às informações e ativos correspondentes sempre que necessário, promovendo a continuidade dos negócios.

IV - **Resiliência:** Estabelecer práticas que aumentem a capacidade da organização identificar, prevenir e recuperar-se rapidamente de incidentes, assegurando a continuidade das operações e a proteção dos interesses do negócio.

3. APLICAÇÕES DA PSI

As diretrizes estabelecidas nesta política devem ser seguidas por todos os colaboradores, prestadores de serviço, administradores e terceiros, aplicando-se à informação em qualquer meio ou suporte, físico ou digital. Esta política também informa que os ambientes, sistemas, dispositivos (como computadores, notebooks, smartphones, tablets) e redes da empresa poderão ser monitorados e registrados, sempre com comunicação prévia, em conformidade com as leis e regulamentações brasileiras, visando à proteção dos ativos da organização e à segurança das operações.

4. PRINCÍPIOS DA PSI

I - Toda informação produzida ou recebida pelos colaboradores como resultado de suas atividades profissionais contratadas pela CAJ é de propriedade exclusiva da instituição. Quaisquer exceções a essa regra devem ser explícitas e formalizadas por meio de contrato entre as partes envolvidas.

II - Os equipamentos de informática e comunicação, sistemas e informações fornecidos pela CAJ são destinados exclusivamente à realização das atividades profissionais.

III - O uso pessoal desses recursos é permitido, desde que não afete negativamente o desempenho dos sistemas, a segurança da informação ou a continuidade dos serviços.

IV - A CAJ, por meio da Gerência de Tecnologia da Informação, se reserva o direito de registrar e monitorar o uso de sistemas e serviços, a fim de garantir a disponibilidade, a segurança e a conformidade das

informações e dos recursos tecnológicos utilizados.

5. REQUISITOS DA PSI

Para garantir a uniformidade e a eficácia das ações de segurança da informação, a PSI deverá:

I - Ser comunicada a todos os colaboradores, prestadores de serviço e parceiros da CAJ, garantindo que seja cumprida tanto dentro quanto fora da empresa.

II - A gestão da segurança da informação será responsabilidade de um Comitê de Segurança da Informação e Comunicação, composto por um grupo multidisciplinar, que será encarregado de implementar, revisar e supervisionar a aplicação da PSI.

III - Tanto a PSI quanto as normas de segurança relacionadas deverão ser revisadas e atualizadas periodicamente. Caso eventos relevantes ou incidentes ocorram, a política será revista de forma antecipada, conforme análise e decisão do Comitê de Segurança.

IV - A responsabilidade pela segurança da informação será comunicada durante o processo de contratação de colaboradores, e todos deverão ser orientados sobre os procedimentos de segurança, incluindo o uso adequado dos ativos, com o objetivo de reduzir os riscos.

V - Prestadores de serviço que utilizem sistemas de informação da CAJ também deverão ser orientados sobre as normas de segurança e assinar um termo de responsabilidade, garantindo seu compromisso com as práticas estabelecidas.

VI - Qualquer incidente que afete a segurança da informação deve ser comunicado imediatamente à Gerência de Tecnologia da Informação, que, se necessário, encaminhará o caso ao Comitê de Segurança da Informação e Comunicação para análise e medidas corretivas.

VII - A PSI aplica-se a todos os ambientes de TI, tanto os administrativos, voltados para os recursos e sistemas de apoio e acesso aos dados (como gestão de pessoal, financeiros, e-mails, sistema comercial, etc.), bem como aos sistemas operacionais, voltados para os recursos da produção e operações, como sistemas de automação, telemetria e outros sistemas críticos. Ambos os ambientes devem ser tratados com a mesma prioridade em termos de segurança.

VIII - Um plano de contingência e as práticas de continuidade dos negócios devem ser implementados e testados anualmente, a fim de minimizar os riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

IX - Todos os requisitos de segurança, incluindo a necessidade de planos de contingência, deverão ser identificados na fase de levantamento de escopo de projetos ou sistemas, sendo formalmente acordados, documentados e implementados durante a execução.

X - A CAJ implementará controles apropriados, como trilhas de auditoria e registros de atividades, em todos os pontos críticos, incluindo estações de trabalho, notebooks, acessos à internet, e-mails e sistemas comerciais ou financeiros desenvolvidos pela própria CAJ ou por terceiros.

XI - Ambientes de produção deverão ser segregados de forma rigorosa e controlada, garantindo isolamento adequado em relação aos ambientes de desenvolvimento, testes e homologação, minimizando riscos de falhas ou acessos não autorizados.

XII - A CAJ isenta-se de responsabilidade por uso indevido, negligente ou imprudente dos recursos e serviços disponibilizados aos colaboradores. A instituição se reserva o direito de realizar investigações, incluindo análise de dados e evidências, para coleta de provas a serem utilizadas em processos investigatórios e adotar as medidas legais cabíveis.

XIII - A implementação desta PSI será obrigatória para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, e também se aplica a prestadores de serviço ou parceiros. A não conformidade com os requisitos estabelecidos nesta PSI e nas normas de segurança acarretará em medidas disciplinares e legais, conforme as políticas internas da CAJ.

6. USUÁRIOS DE INFORMÁTICA

São reconhecidos como usuários da infraestrutura de TI da CAJ todos os colaboradores, administradores, profissionais autônomos, temporários ou prestadores de serviços que obtiverem a devida aprovação do gestor responsável e da área de TI para o acesso aos recursos computacionais da empresa. Esta aprovação inclui a prescrição de senhas de acesso, que deverão ser gerenciadas conforme as políticas e boas práticas de segurança da informação.

7. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

O Comitê de Segurança da Informação e Comunicação (CSI) deve ser formalmente constituído por colaboradores designados para integrar o grupo. A composição mínima do CSI deverá incluir representantes das seguintes áreas: Tecnologia da Informação, Governança e Jurídico.

O CSI deverá reunir-se formalmente pelo menos uma vez a cada seis meses para revisar as práticas de segurança da informação, avaliar riscos e definir estratégias de proteção. Reuniões adicionais poderão ser convocadas sempre que necessário para deliberar sobre incidentes graves, questões críticas ou decisões estratégicas relevantes para a segurança da CAJ.

Além disso, o CSI poderá contar com o apoio de especialistas internos ou externos para assuntos que demandem conhecimentos técnicos específicos, garantindo uma abordagem adequada e eficaz em situações

complexas.

8. DAS RESPONSABILIDADES ESPECÍFICAS

São responsabilidades:

8.1 – DOS USUÁRIOS DE INFORMÁTICA

I - Respeitar e cumprir integralmente a Política de Segurança da Informação (PSI) da CAJ, bem como as normas e procedimentos relacionados.

II - Garantir a proteção e guarda dos recursos computacionais, como dispositivos, sistemas e redes, colocados à sua disposição para a execução de suas atividades profissionais.

III - Utilizar as senhas de acesso de forma exclusiva e intransferível, sendo responsável por sua confidencialidade e segurança.

IV - Buscar continuamente conhecimento e capacitação para o uso correto e seguro dos recursos de hardware e software da CAJ, em conformidade com as normas internas.

V - Relatar imediatamente à área de TI qualquer incidente ou ameaça à segurança dos recursos, como falhas de segurança, vulnerabilidades, mau funcionamento de sistemas, presença de vírus ou qualquer outro risco.

VI - Assegurar que as informações e dados de propriedade da CAJ sejam protegidos e não disponibilizados a terceiros, exceto com autorização por escrito do responsável hierárquico.

VII - Informar ao responsável hierárquico e à Gerência de TI sempre que houver a necessidade de novos softwares ou ferramentas para suas atividades, garantindo a avaliação prévia de segurança e compatibilidade.

VIII - Assumir total responsabilidade por qualquer prejuízo ou dano causado à CAJ ou a terceiros decorrente do não cumprimento das diretrizes e normas estabelecidas nesta PSI.

8.2 – DOS GESTORES DE PESSOAS E/OU PROCESSOS

I - Exercer uma postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão e assegurando o cumprimento das diretrizes da PSI.

II - Incluir a responsabilidade pelo cumprimento da PSI da CAJ durante a fase de contratação e na formalização de contratos de trabalho, prestação de serviços ou parcerias, garantindo que todos os envolvidos estejam cientes de suas obrigações em relação à segurança da informação.

III - Exigir a assinatura do Termo de Compromisso e Ciência por parte dos colaboradores, compromissando-os a seguir as normas de segurança da informação e a manter sigilo e confidencialidade, mesmo após o desligamento da empresa, sobre todos os ativos de informação da CAJ.

IV - Exigir a assinatura do Acordo de Confidencialidade de colaboradores temporários, casuais e prestadores de serviços que não possuam um contrato específico, especialmente durante atividades como levantamento de informações para propostas comerciais ou outros processos sensíveis.

V - Autorizar o acesso e definir o perfil de usuário junto à área de TI, garantindo que os acessos sejam concedidos de forma adequada e com base na necessidade para o desempenho das funções do colaborador.

VI - Notificar imediatamente à área de TI sobre qualquer vulnerabilidade, ameaça ou incidente de segurança que comprometa a integridade, confidencialidade ou disponibilidade dos recursos da instituição.

VII - Advertir formalmente qualquer colaborador que viole os princípios ou procedimentos de segurança, aplicando as sanções cabíveis e relatando o ocorrido à área de TI para análise e ações corretivas.

VIII - Adaptar processos, normas e sistemas sob sua responsabilidade para garantir que estejam alinhados e em conformidade com os requisitos da PSI, promovendo uma cultura de segurança da informação em todas as áreas de atuação.

8.3 – DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

I - Testar a eficácia dos controles de segurança implementados e fornecer relatórios aos gestores sobre os riscos residuais, a fim de garantir que a infraestrutura de TI esteja protegida contra ameaças.

II - Acordar com os gestores o nível de serviço a ser prestado e os procedimentos de resposta a incidentes de segurança, garantindo que todos os envolvidos estejam alinhados sobre como agir em caso de incidentes.

III - Configurar e proteger os equipamentos, ferramentas e sistemas utilizados pelos colaboradores, implementando todos os controles necessários para garantir a segurança conforme os requisitos da PSI e das normas complementares.

IV - Gerenciar os privilégios de administradores e operadores de sistemas, garantindo que o acesso a dados sensíveis e arquivos de outros usuários seja restrito ao necessário para a execução de atividades operacionais, como manutenção, cópias de segurança, auditorias ou testes.

V - Segregar funções administrativas e operacionais para minimizar o risco de abuso de privilégios e garantir que nenhuma pessoa tenha capacidade de excluir ou modificar logs e trilhas de auditoria relacionados às suas próprias ações.

VI - Implementar controles de segurança especiais para sistemas com acesso público, garantindo que

evidências sejam coletadas e armazenadas de forma adequada para auditoria e investigação.

VII - Gerar e manter trilhas de auditoria detalhadas o suficiente para rastrear falhas, fraudes e outras atividades suspeitas, assegurando que essas trilhas, quando armazenadas em formato eletrônico, possuam controles de integridade para serem válidas como evidências legais.

VIII - Administrar, proteger e testar cópias de segurança de dados e programas relacionados a processos críticos, garantindo a continuidade e segurança das operações da CAJ.

IX - Implantar controles para registros auditáveis durante a retirada e transporte de mídias contendo informações sensíveis, assegurando que esses processos ocorram em ambientes controlados e conforme as políticas de segurança.

X - Notificar o gestor da informação sobre o fim do prazo de retenção de dados, permitindo que este determine o destino da informação antes de seu descarte.

XI - Planejar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão de dados necessária para garantir a segurança e o desempenho das operações, atendendo às necessidades das áreas de negócio.

XII - Atribuir responsabilidades claras para cada conta ou dispositivo de acesso, identificando os responsáveis por usuários de sistemas e ativos de informação, e garantindo que:

a. Os logins de colaboradores sejam de responsabilidade exclusiva do colaborador.

b. Os logins de terceiros sejam responsabilidade do gestor da área contratante.

XIII - Proteger continuamente os ativos de informação contra códigos maliciosos (vírus, trojans, etc.), realizando varreduras antes de permitir a inclusão de novos ativos no ambiente de produção.

XIV - Evitar introdução de vulnerabilidades ou fragilidades nos ambientes de produção durante processos de mudança, realizando auditoria de código e implementando cláusulas contratuais com terceiros para controle e responsabilização.

XV - Definir regras formais para instalação de software e hardware, garantindo que todos os componentes adicionados aos ambientes de produção ou educacional estejam de acordo com as políticas da CAJ.

XVI - Realizar auditorias periódicas de configurações técnicas e análise de riscos, com reporte detalhado à área de Controle Interno.

XVII - Garantir o bloqueio imediato de acessos de colaboradores desligados ou quando identificado incidente de segurança, garantindo que os acessos sejam restritos de forma rápida e eficiente para proteger os ativos da empresa.

XVIII - Manter sincronização do relógio de servidores e dispositivos com servidores de tempo oficiais do governo brasileiro para garantir a precisão das trilhas de auditoria e a integridade dos registros.

XIX - Monitorar constantemente o ambiente de TI, gerando indicadores de:

a. Uso de capacidade de rede e equipamentos.

b. Tempo de resposta aos sistemas críticos da CAJ.

c. Períodos de indisponibilidade dos sistemas e da rede.

d. Incidentes de segurança (vírus, acessos indevidos, etc.).

e. Atividade dos colaboradores, incluindo acessos à internet e e-mails.

XX - Propor metodologias e processos de segurança para avaliação de riscos e classificação de informações, promovendo uma cultura de segurança e proteção de dados.

XXI - Propor e apoiar iniciativas de segurança da informação, visando o fortalecimento das práticas de proteção de ativos críticos da CAJ.

XXII - Publicar e promover versões da PSI e das Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação e Comunicação.

XXIII - Conscientizar os colaboradores sobre a importância da segurança da informação para o sucesso da CAJ, utilizando campanhas educativas, treinamentos e outras iniciativas de endomarketing.

XXIV - Apoiar a avaliação e adequação de controles específicos de segurança para novos sistemas ou serviços que sejam incorporados ao ambiente da CAJ.

XXV - Analisar e avaliar incidentes de segurança, trabalhando em conjunto com o Comitê de Segurança da Informação e Comunicação para identificar falhas e implementar melhorias.

XXVI - Apresentar relatórios e atas das reuniões do Comitê de Segurança da Informação, destacando os pontos que requerem ações imediatas ou discussão mais profunda por parte da alta gestão.

XXVII - Manter comunicação efetiva com o Comitê de Segurança, assegurando que questões críticas relacionadas à segurança da informação sejam discutidas e tratadas com a devida urgência e prioridade.

XXVIII - Buscar constante alinhamento com as diretrizes corporativas da CAJ, garantindo que a segurança da informação esteja integrada ao planejamento e objetivos estratégicos da instituição.

8.4 – DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

I - Propor investimentos relacionados à segurança da informação, com foco na mitigação de riscos e na implementação de tecnologias e controles que fortaleçam a proteção de dados, incluindo sistemas críticos de operação (TO), como automação e telemetria.

II - Propor alterações nas versões da PSI e revisar continuamente as normas complementares, considerando a evolução das ameaças, os requisitos de conformidade e a necessidade de integração com as operações de TI e TO da CAJ.

III - Avaliar incidentes de segurança, determinando suas causas e propondo ações corretivas, preventivas ou de mitigação, levando em consideração o impacto tanto nos sistemas de TI quanto nas operações de tecnologia e produção da empresa.

IV - Definir as medidas cabíveis em casos de descumprimento da PSI e das Normas de Segurança da Informação complementares, avaliando as consequências para os responsáveis, com foco na preservação da segurança da informação e integridade dos processos.

V - Avaliar e aprovar pedidos de acesso aos sistemas e dados da CAJ, seja para terceiros ou em solicitações internas, especialmente quando envolvem dados sensíveis ou operações críticas, considerando os impactos na segurança da informação e nas operações de TI e TO.

VI - Monitorar a implementação das decisões do Comitê em relação à segurança da informação, assegurando que todas as ações sejam alinhadas às políticas corporativas e cumpram com os requisitos de segurança, tanto nos ambientes administrativos quanto nos de operação.

9 – MONITORAMENTO E AUDITORIA DO AMBIENTE

A CAJ deve garantir a eficácia das regras estabelecidas nesta PSI por meio da implementação de controles de monitoramento e auditoria contínuos, incluindo os seguintes aspectos:

9.1 - MONITORAMENTO CONTÍNUO

I - Implantar sistemas de monitoramento em estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis, redes wireless e outros componentes críticos da infraestrutura da CAJ.

II - O monitoramento deve ser realizado para rastrear atividades de usuários, acessos realizados, e o tratamento de informações sensíveis ou críticas, com ênfase na identificação e prevenção de incidentes de segurança.

9.2 - AUDITORIA E RASTREABILIDADE

I - Garantir que todos os sistemas críticos gerem trilhas de auditoria detalhadas, que possibilitem a rastreabilidade completa das ações dos usuários. Essas trilhas devem ser protegidas contra alterações e devem ser armazenadas conforme as políticas internas de retenção de dados.

II - As informações geradas pelos sistemas de monitoramento poderão ser utilizadas para identificar e analisar comportamentos anômalos ou ações que possam comprometer a segurança da informação, sempre em conformidade com as normas legais.

9.3 - ACESSO ÀS INFORMAÇÕES DE MONITORAMENTO

I - As informações obtidas pelos sistemas de monitoramento e auditoria podem ser tornadas públicas ou compartilhadas, conforme exigências judiciais, solicitação de superiores hierárquicos ou por determinação do Comitê de Segurança da Informação e Comunicação.

II - Realizar inspeções físicas nas estações de trabalho e outros equipamentos sob sua propriedade sempre que necessário para garantir que não haja riscos à segurança física ou lógica.

III - Instalar sistemas de proteção preventiva e detectável, como firewalls e ferramentas de detecção de intrusão, para garantir a segurança das informações, a integridade dos sistemas e dos perímetros de acesso da CAJ.

9.4 - RESPOSTA A INCIDENTES

I - Em caso de incidente, a área de TI deve tomar as medidas necessárias para mitigar os impactos, proteger os ativos de informação e restaurar os serviços o mais rapidamente possível. Isso inclui o uso de ferramentas de monitoramento para detectar e investigar qualquer violação.

10 – DOS SERVIÇOS E RECURSOS DE TIC

10.1 - GESTÃO E CONTROLE DE ATIVOS

10.1.1 - GESTÃO DE ATIVOS E INVENTÁRIO

I - Todos os ativos de tecnologia da informação (TI) e operacionais (TO), como servidores, computadores, dispositivos móveis, sistemas e licenças de software e sistemas de automação (controladores lógicos programáveis e interface homem máquina) devem ser registrados e atualizados em um inventário centralizado.

II - O inventário deve conter informações como proprietário, localização, configuração, data de aquisição e estado operacional do ativo.

III - A Gerência de Tecnologia da Informação é responsável por manter o inventário atualizado e auditar periodicamente os ativos para identificar possíveis discrepâncias ou riscos.

10.1.2 - GESTÃO DE SERVIÇOS E RECURSOS EM NUVEM

I - Todos os serviços e recursos de nuvem utilizados pela CAJ devem ser formalmente aprovados e registrados, garantindo alinhamento com os requisitos de segurança da PSI.

II - O uso de soluções em nuvem deve atender aos padrões de proteção de dados sensíveis e respeitar as leis brasileiras, como a LGPD.

III - A Gerência de Tecnologia da Informação deve garantir que contratos com provedores de serviços em nuvem incluam cláusulas sobre segurança, disponibilidade e recuperação de dados.

10.1.3 - DATACENTER

I - O Datacenter deve ser um local físico destinado exclusivamente à acomodação de equipamentos críticos, como servidores, sistemas de telefonia e armazenamento.

II - O ambiente deve ser controlado para atender padrões de temperatura, umidade e fornecimento de energia elétrica, com proteção contra falhas (nobreaks e geradores).

III - Deve contar com sistemas de segurança física, incluindo autenticação forte (biometria, cartão magnético, etc.), detecção de incêndios e acesso restrito a pessoas autorizadas.

Nota geral: Os requisitos e padrões relacionados ao inventário e gestão de ativos, infraestrutura física e Datacenter, bem como controle de acessos aos ativos, devem ser claramente definidos e documentados em procedimentos internos atualizados. A responsabilidade pela elaboração, implementação e manutenção desses documentos é da Gerência de Tecnologia da Informação, em conjunto com as áreas responsáveis pelos respectivos ativos e operações.

10.2 - PROTEÇÃO E MONITORAMENTO

10.2.1 - MONITORAMENTO CONTÍNUO

I - A infraestrutura de tecnologia da informação e operação deve ser monitorada continuamente para detectar e responder a incidentes, falhas ou atividades anômalas que possam comprometer a segurança, integridade ou disponibilidade dos sistemas e ativos. O monitoramento deve gerar registros centralizados (logs) contendo informações detalhadas, como data, hora, origem, destino e contexto das ações realizadas. Esses registros devem ser protegidos contra alterações e mantidos conforme normas de retenção aplicáveis.

10.2.2 - GESTÃO DE VULNERABILIDADES

I - Os ativos de TI e TO devem ser regularmente avaliados quanto à presença de vulnerabilidades conhecidas. Devem ser realizados testes periódicos de segurança, como varreduras de vulnerabilidades e testes de penetração, com a aplicação de correções (patches) priorizando ativos críticos. Os resultados e planos de mitigação devem ser reportados ao Comitê de Segurança da Informação e Comunicação para acompanhamento.

10.2.3 - ANTIVÍRUS

I - Todos os dispositivos, como servidores, computadores, notebooks, tablets e smartphones, devem possuir sistemas de proteção contra vírus e outras ameaças. Esses sistemas devem ser licenciados, atualizados automaticamente e configurados para detectar, bloquear e reportar incidentes de segurança.

II - No caso de trabalho remoto com acesso a recursos internos, é obrigatória a disponibilização de antivírus licenciado. O uso do sistema antivírus deve seguir as melhores práticas de proteção e estar alinhado aos padrões definidos pela Gerência de Tecnologia da Informação.

10.2.4 - FIREWALL

I - Os ambientes computacionais internos devem ser protegidos por sistemas de firewall que possam identificar, bloquear acessos não autorizados e analisar arquivos para prevenir ameaças, como arquivos infectados. A administração dos firewalls deve ser restrita à equipe da Gerência de Tecnologia da Informação ou à empresa contratada, devidamente capacitada para esta atividade.

II - Os registros de acessos e eventos devem ser armazenados em sistemas centralizados, contendo data, hora, origem, destino, usuário e contexto. Devem ser utilizadas tecnologias modernas e métodos atualizados para garantir a segurança, integridade e disponibilidade dos ambientes, acompanhando a evolução das técnicas de intrusão.

Nota Geral: A proteção e monitoramento dos ativos de TI e TO devem ser realizados de forma integrada, garantindo a identificação e resposta a ameaças, a correção de vulnerabilidades e a aplicação de medidas preventivas. Todos os controles e sistemas relacionados à proteção, como monitoramento contínuo, antivírus e firewalls, devem ser documentados em procedimentos internos, com responsabilidade de implementação e atualização atribuída à Gerência de Tecnologia da Informação. Os registros de eventos e análises devem estar disponíveis para auditorias internas e ações de resposta a incidentes.

10.3 - ACESSO E PERMISSÕES

10.3.1 - IDENTIFICAÇÃO

I - O uso de equipamentos e sistemas corporativos será permitido apenas mediante a identificação individual de cada usuário.

II - Os acessos realizados devem ser registrados em sistema centralizado de eventos, contendo data, hora, usuário e recurso acessado.

III - Credenciais específicas, como números de registro, crachás, certificados digitais, dados biométricos e logins de sistemas, devem ser atribuídas a cada colaborador, garantindo sua vinculação a uma pessoa física identificável.

IV - Todos os dispositivos de identificação e técnicas de segurança aplicadas devem atender aos padrões definidos pela Gerência de Tecnologia da Informação.

10.3.2 - PERFIL DE ACESSO

I - O controle de acesso às funcionalidades de sistemas será realizado por perfis associados a cargos ou funções, e não por usuários individuais.

II - Alterações nos perfis de acesso devem ser formalmente autorizadas pelo gestor do processo ou da funcionalidade impactada.

III - Os critérios e padrões para gestão de perfis de acesso devem ser definidos e revisados periodicamente pela Gerência de Tecnologia da Informação.

10.3.2.1 Acesso para Terceiros e Visitantes

I - A conectividade de rede para usuários externos, como terceiros e visitantes, será disponibilizada apenas em ambientes segregados, sem acesso direto aos sistemas internos de produção.

II - O acesso concedido deve ser restrito a serviços específicos, como a internet, e todos os eventos devem ser registrados em sistema centralizado.

III - As permissões, técnicas de segurança e controles associados devem ser documentados e gerenciados conforme os padrões estabelecidos pela Gerência de Tecnologia da Informação.

Nota Geral: Todos os acessos aos sistemas e redes da CAJ devem ser rigorosamente controlados e registrados para garantir a segurança e rastreabilidade das ações realizadas. A identificação de usuários, a definição de perfis de acesso e a gestão de acessos para terceiros e visitantes devem estar alinhadas às políticas internas e padrões de segurança, assegurando o cumprimento das diretrizes corporativas e a proteção dos ativos da organização.

10.4 - DISPOSITIVOS E RECURSOS CORPORATIVOS

10.4.1 - COMPUTADORES

I - Computadores serão disponibilizados aos colaboradores para o desempenho de suas atividades, especificados de acordo com as necessidades de cada função.

II - Todos os computadores devem permanecer conectados à rede local e estar sujeitos ao monitoramento de recursos por meio de softwares específicos.

10.4.2 - DISPOSITIVOS MÓVEIS

I - Dispositivos móveis, como notebooks, smartphones, tablets e pendrives, serão disponibilizados conforme a necessidade definida pelo gestor da área para uso em ambientes externos ou internos.

II - Esses dispositivos devem ser configurados e utilizados em conformidade com os critérios de segurança aplicáveis, especialmente ao se conectarem à rede local CAJ.

10.4.3 - INTERNET

I - O acesso à internet é um recurso essencial para comunicação, troca de informações e interação com fornecedores, clientes e a sociedade.

II - A conectividade será garantida por links de comunicação específicos, com níveis adequados de qualidade, disponibilidade e segurança que atendam às necessidades do negócio.

10.4.4 - CORREIO ELETRÔNICO

I - Todos os colaboradores terão acesso ao serviço de correio eletrônico corporativo (e-mail), destinado prioritariamente a fins corporativos e atividades relacionadas às suas funções.

II - O uso pessoal do e-mail será permitido, desde que feito com bom senso, não prejudique a organização e não impacte negativamente o tráfego da rede.

Nota Geral: Todos os dispositivos e recursos corporativos devem ser utilizados exclusivamente para atender às demandas institucionais, respeitando as políticas internas e os critérios de segurança estabelecidos. A Gerência de Tecnologia da Informação é responsável por definir padrões e especificações para uso, monitoramento e configuração desses recursos, assegurando alinhamento com as melhores práticas de mercado e as necessidades do negócio.

10.5 - DADOS E RECUPERAÇÃO

10.5.1 - CÓPIA (BACKUP) E RESTAURAÇÃO

I - Deverão ser realizadas cópias de segurança regulares de todos os dados gerados e armazenados pelos sistemas internos da CAJ, garantindo a disponibilidade e integridade dos dados. A frequência das cópias de segurança deve ser definida com base nas necessidades do negócio e nos requisitos legais aplicáveis.

II - As cópias de segurança devem ser armazenadas em local seguro, fisicamente separado do Datacenter, a fim de minimizar riscos em caso de falhas ou incidentes.

III - As tecnologias e métodos utilizados para backup e restauração devem ser adequados para garantir a execução sem impacto significativo no ambiente de produção.

IV - Os gestores de processos devem fornecer informações sobre os dados a serem copiados, incluindo periodicidade, tempo de retenção e tempo de recuperação, para a área responsável pela gestão de TI.

V - A operação do sistema de backup deve ser realizada exclusivamente por profissionais qualificados, que também são responsáveis pela execução de simulações periódicas de cópia e restauração, com a frequência mínima de uma vez a cada 180 dias, para garantir a eficácia do processo.

VI - Os métodos de backup e restauração adotados devem seguir as melhores práticas de segurança, conforme as diretrizes internas de segurança da informação da CAJ.

11 – PROTEÇÃO DE DADOS SENSÍVEIS

A proteção de dados sensíveis, como informações pessoais, financeiras ou confidenciais, deve ser assegurada:

I - Por meio de controles de segurança adequados durante a coleta, armazenamento, transmissão e processamento desses dados.

II - Mecanismos de criptografia e outras tecnologias de proteção devem ser implementados para garantir a confidencialidade, integridade e disponibilidade dos dados sensíveis.

Todos os dados sensíveis devem ser tratados conforme as legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD), e conforme as políticas internas de proteção de dados pessoais e privacidade.

Nota Geral: A gestão de cópias de segurança e a proteção de dados sensíveis são essenciais para assegurar a continuidade dos negócios e garantir a conformidade legal da CAJ. A área de Tecnologia da Informação é responsável por implementar e manter as melhores práticas de segurança em backup e recuperação, assim como proteger os dados sensíveis, adotando medidas como criptografia e segregação de dados, além de garantir a recuperação rápida em caso de incidentes. As práticas e diretrizes específicas para esses processos devem ser estabelecidas em normas internas complementares.

12 - DA CLASSIFICAÇÃO DA INFORMAÇÃO

As informações geradas, processadas ou mantidas nos processos internos devem ser:

I - Classificadas desde o momento de sua criação ou recebimento, considerando seu valor para a organização, a necessidade de proteção e os requisitos legais e regulatórios aplicáveis.

II - A classificação da informação deve ser baseada em critérios de confidencialidade, integridade e disponibilidade, com níveis claros que orientem a proteção adequada dos dados, e deve ser revisada periodicamente para garantir que os controles aplicados sejam eficazes.

III - Os gestores de processos são responsáveis por informar e manter atualizada a classificação das informações relacionadas aos processos sob sua responsabilidade, assegurando que as informações sejam tratadas de acordo com o seu nível de confidencialidade, conforme a política de segurança da informação.

IV - A CAJ adota como base a ISO/IEC 27002:2022 para a definição e aplicação dos critérios de classificação da informação, que devem incluir, entre outros, a categorização de dados sensíveis, pessoais, financeiros, estratégicos, e de interesse público.

V - A classificação das informações deve estar alinhada com a Política de Segurança da Informação da CAJ, considerando também os controles técnicos, operacionais e legais necessários para proteger adequadamente as informações sensíveis e garantir a conformidade com regulamentações, como a Lei Geral de Proteção de Dados (LGPD).

13 - USO DE INTELIGÊNCIA ARTIFICIAL (IA)

A Companhia Águas de Joinville reconhece os benefícios da Inteligência Artificial (IA) no aprimoramento de seus processos e serviços, mas também entende os riscos associados ao seu uso. Portanto, todos os sistemas de IA utilizados ou desenvolvidos pela CAJ devem seguir as diretrizes de segurança, privacidade e governança estabelecidas nesta Política de Segurança da Informação.

A CAJ se compromete a monitorar continuamente a utilização da IA, garantindo que ela seja segura, ética e em conformidade com as regulamentações vigentes, especialmente no que diz respeito à proteção de dados sensíveis e ao impacto nos processos de tomada de decisão.

14 - GOVERNANÇA DOS DADOS

A Companhia Águas de Joinville estabelece a governança dos dados como um componente central da sua Política de Segurança da Informação, com o objetivo de garantir que todos os dados sejam gerenciados de maneira eficiente, segura e em conformidade com as regulamentações aplicáveis. A governança dos dados abrange as seguintes diretrizes:

14.1 - GESTÃO DE DADOS

I - Todos os dados gerados e utilizados nos processos internos devem ser classificados, protegidos e mantidos de acordo com os requisitos de segurança, privacidade e compliance estabelecidos nesta PSI e em normativas relacionadas.

II - A responsabilidade pelo gerenciamento e governança dos dados será atribuída a uma equipe dedicada, com funções e processos claros para assegurar a integridade, qualidade, e segurança dos dados ao longo de seu ciclo de vida.

14.2 - PROTEÇÃO E PRIVACIDADE DE DADOS

I - Todos os dados sensíveis ou pessoais devem ser protegidos conforme as diretrizes de segurança da informação, incluindo a utilização de criptografia, anonimização e controles de acesso rigorosos.

II - O tratamento dos dados deve respeitar as políticas de privacidade, garantindo o consentimento adequado dos titulares de dados e atendendo às exigências das legislações aplicáveis (como LGPD).

14.3 - QUALIDADE DOS DADOS

I - A CAJ deve manter práticas contínuas para garantir a qualidade dos dados, com processos estabelecidos para validação, atualização, e limpeza de dados para evitar a utilização de informações desatualizadas ou incorretas.

II - Devem ser implementados controles para garantir que os dados sejam precisos, completos e acessíveis, e que sejam utilizados de forma eficaz nas decisões empresariais.

14.4 - ACESSO E CONTROLE DE DADOS

I - O acesso aos dados será restrito a usuários autorizados e será concedido de acordo com as necessidades de negócio e os perfis de acesso definidos pela empresa.

II - Todos os acessos aos dados devem ser registrados e monitorados, com auditorias periódicas para garantir a conformidade com as políticas de segurança e privacidade.

14.5 - CICLO DE VIDA DOS DADOS

I - A governança dos dados deve cobrir o ciclo completo de vida dos dados, desde a sua criação até o arquivamento ou eliminação. Todos os dados devem ser armazenados em locais seguros, com cópias de segurança adequadas e políticas claras para retenção e descarte de dados.

II - Todos os colaboradores devem ser treinados regularmente sobre a importância da governança de dados, com ênfase na segurança, privacidade e conformidade com as políticas e regulamentos aplicáveis.

II - A responsabilidade pela governança dos dados será atribuída a gestores e equipes específicas, com autoridade para implementar e monitorar as práticas de governança.

15 - DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da CAJ, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Na hipótese de violação desta PSI ou das normas de segurança da informação, a Diretoria, com o apoio das áreas de Segurança da Informação, Conformidade e Gestão de Pessoas, determinarão as sanções administrativas que serão aplicadas ao infrator, sendo que:

I - Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Matriz de Penalidades.

II - Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo contrato estabelecido violado.

Esta política foi aprovada pelo Conselho de Administração, entra em vigor na data de sua publicação e terá validade indeterminada, podendo ser revisada a qualquer momento.

Revoga-se a Política de Nº 7259676, de 29 de setembro de 2020, da Companhia Águas de Joinville.

Documento assinado eletronicamente por **Sidney Marques de Oliveira Junior**, **Diretor (a) Presidente**, em 22/01/2025, às 14:27, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Fabio Rodrigo Schatzmann**, **Conselheiro (a)**, em 24/01/2025, às 13:35, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **0024206261** e o código CRC **66C94071**.