1. OBJETIVOS

1.1. Esta política de segurança cibernética e da informação ("Política") estabelece as diretrizes e formaliza o compromisso da alta administração em relação ao tema de segurança cibernética e da informação para a Companhia de Saneamento Básico do Estado de São Paulo – SABESP e suas subsidiárias ("Companhia"), de modo a assegurar a:

a) **Confidencialidade**, com garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

b) **Integridade**, com garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais e;

c) **Disponibilidade**, com garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário, da estrutura de negócios da Companhia.

1.1.1. A presente Política estabelece diretrizes claras para garantir a proteção das informações e dos ativos da Companhia, conforme os princípios e padrões internacionais de segurança, de forma a prevenir, detectar e reduzir a vulnerabilidade a incidentes ou crises cibernéticas.

1.2. Esta Política se aplica a todos administradores, acionistas, empregados, estagiários, menores aprendizes, fornecedores, parceiros e quaisquer outros profissionais que atuam à serviço da Companhia.

2. DIRETRIZES

2.1. A Companhia deve realizar o tratamento de informações nos mais variados formatos para viabilizar o seu negócio, e, portanto, possui um programa estruturado para definir, implementar e monitorar a sua segurança e proteção independente da forma em que ela se encontra, onde é processada, está armazenada ou é descartada.

2.2. Todas as partes atuantes a serviço da Companhia devem estar cientes de suas responsabilidades no tratamento seguro da informação, incluindo o uso de controles de acesso, autenticação forte, criptografia de dados sensíveis e gestão adequada de ativos, respondendo pelo descumprimento desta Política, mesmo após seu desligamento.

2.3. As informações devem ser protegidas tanto no meio digital (notebooks, celulares, tablets etc.), quanto no físico. É de responsabilidade do Colaborador manter estas informações protegidas em qualquer ambiente.

2.4. As informações relevantes da Companhia devem ser armazenadas com redundância, assegurando a disponibilidade e a possibilidade de restauração de dados, arquivos digitais de computadores e sistemas corporativos, em conformidade com as normas aplicáveis.

2.5. É obrigatório realizar treinamentos periódicos de conscientização, aplicar controles físicos e lógicos para proteção dos ambientes, e manter processos de gestão de riscos e resposta a incidentes atualizados.

SEGURANÇA E PROTEÇÃO DAS INFORMAÇÕES

2.6. Todas as informações tratadas para viabilizar as atividades desenvolvidas pela Companhia são de sua propriedade exclusiva e devem ser utilizadas conforme estabelecido nesta Política e demais instrumentos normativos. Qualquer finalidade não explicitamente autorizada é proibida por padrão.

2.7. Deve existir uma metodologia para inventário e classificação das informações de acordo com o nível de confidencialidade para o negócio. Esta classificação deve servir como diretriz para implementar mecanismos de proteção em todo o ciclo de vida do tratamento: criação, coleta, acesso, manuseio, armazenamento, reprodução, transporte e descarte.

2.8. Os ativos de tecnologia da informação e tecnologia da automação, onde as informações da Companhia são tratadas, estão sujeitos a monitoramento sem aviso prévio, seguindo as regras de privacidade e proteção de dados previstas em legislação específica.

ACESSO AS INFORMAÇÕES

2.9. Os acessos aos ativos digitais e físicos e sistemas de tecnologia da informação e tecnologia da automação devem ser controlados de acordo com sua classificação e revisados periodicamente, de forma a estarem acessíveis apenas às pessoas autorizadas. Os privilégios de acesso devem ser configurados a permitir o mínimo necessário para o cumprimento dos objetivos de negócio e impedir conflitos de segregação de função.

SEGREGAÇÃO DE FUNÇÕES

2.10. Deve ser implementada segregação de funções para mitigar o risco de alterações não autorizadas ou uso indevido dos ativos da Companhia, por meio da separação de responsabilidades conflitantes e assegurando que atividades ou funções críticas estejam devidamente segregadas. Quando a segregação não for viável, devem ser adotados controles compensatórios, como monitoramento de atividades, trilhas de auditoria e supervisão gerencial.

2.11. A segregação de funções deve estar presente em todos os processos, em especial para os críticos, garantindo que nenhuma pessoa tenha controle total sobre todas as etapas do ciclo do processo.

2.12. Cada colaborador deve possuir uma identificação única, pessoal e intransferível, que o responsabilize pelas ações realizadas, devendo ser utilizada como assinatura eletrônica, sendo expressamente proibido o seu compartilhamento.

MODELO DE TRÊS LINHAS

2.13. A Companhia adota o modelo de três linhas como referência para segregação de funções e responsabilidades para o tratamento de riscos relacionados à segurança da informação:

a) **Primeira Linha:** é composta pelas funções operacionais e atividades-fim da Companhia, responsáveis por identificar, avaliar, controlar e mitigar riscos inerentes às suas atividades. Essas áreas são responsáveis por assegurar a conformidade com políticas e procedimentos estabelecidos, atuando diretamente na implementação de controles de segurança.

b) **Segunda Linha:** compreende as funções de apoio à gestão de riscos, como controle interno, conformidade e gestão de riscos. É responsável por fornecer suporte, recomendações, monitoramento e orientação à primeira linha, a fim de assegurar que os riscos sejam gerenciados de forma adequada.

c) **Terceira Linha:** é composta pela área de auditoria interna, que de forma independente, atua para avaliar a eficácia dos controles internos, da gestão de riscos e da governança corporativa. Relatórios gerados são direcionados à alta administração e ao conselho de administração, promovendo a supervisão e a melhoria contínua do sistema de gestão da segurança da informação.

FORNECEDORES E PARCEIROS

2.14. Fornecedores e parceiros são fundamentais para viabilizar os negócios da Companhia. O escopo de atuação de cada um deles deve estar formalizado por meio de um contrato de prestação de serviço, contendo cláusulas de confidencialidade, proteção de dados pessoais, de cumprimento a esta Política e procedimentos internos, orientações específicas de atuação ou outras recomendações, além de sanções em caso de seu descumprimento.

2.15. Sempre que necessário, os acessos a informações, ativos, sistemas de tecnologia da informação e tecnologia da automação são permitidos, mas devem ser restrito ao mínimo necessário ao cumprimento do escopo contratual e permanecerem válidos somente durante a vigência do contrato. As áreas contratantes são responsáveis pelas ações dos fornecedores e parceiros, com o apoio e recomendações da área de Segurança da Informação.

RISCOS CIBERNÉTICOS E EXCEÇÕES À POLÍTICA

2.16. A operacionalização dos serviços prestados pela Companhia é fortemente dependente de ativos, sistemas de tecnologia da informação e tecnologia da automação, que têm seus riscos cibernéticos identificados e estão protegidos através de controles processuais, cibernéticos e tecnológicos adequados, continuamente monitorados e melhorados para assegurar que os objetivos do negócio sejam devidamente atendidos, bem como identificados novos riscos a partir da evolução constante da tecnologia.

2.17. Esta Política deve ser cumprida integralmente e as exceções devem ser revisadas e monitoradas pela Comissão de Segurança da Informação, conforme estabelecido pelo seu regimento interno.

RESILIÊNCIA CIBERNÉTICA E TECNOLÓGICA

2.18. A resiliência cibernética, tecnológica e operacional, deve garantir a continuidade dos serviços prestados mediante a ocorrência de incidentes na sua operação, permitindo que a Companhia possa responder, se adaptar e se recuperar em caso de ocorrência de incidentes ou crises cibernéticas.

CLASSIFICAÇÃO E PROTEÇÃO DA INFORMAÇÃO

2.19. A Companhia deve classificar e proteger informações conforme sua sensibilidade, com base nos princípios de confidencialidade, integridade e disponibilidade, visando mitigar riscos, garantir rastreabilidade e apoiar a conformidade legal e regulatória.

PROPRIEDADE, CONFIDENCIALIDADE E USO ADEQUADO DE RECURSOS

2.20. Todos os dados, informações, produtos e recursos tecnológicos desenvolvidos ou utilizados no âmbito da Empresa são de sua propriedade e devem ser protegidos contra uso indevido, acesso não autorizado ou divulgação indevida. O uso de bens, equipamentos e serviços deve respeitar as diretrizes internas, conforme estabelecido no Código de Conduta e Integridade, sendo vedado o aproveitamento para fins pessoais ou contrários aos interesses da Companhia.

RELATO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

2.21. A Companhia deve manter canais formais, seguros e acessíveis para o registro imediato de incidentes, eventos suspeitos ou situações que possam comprometer a Segurança da informação:

a) O canal de comunicação e relatos de eventos de segurança da informação é: segurancadainformacao@sabesp.com.br

CONTATO COM AUTORIDADES

2.22. A Companhia deve estabelecer procedimentos claros para manter contatos apropriados com autoridades relevantes, assegurando a comunicação tempestiva de incidentes de segurança da informação, o cumprimento de obrigações legais e regulatórias, e a definição precisa de quando e quais entidades devem ser acionadas.

2.23. Caso seja detectado um incidente de segurança da informação, a Companhia avaliará a necessidade de divulgações ao mercado, nos termos da legislação e regulamentação a ela aplicáveis.

CONTATO COM GRUPOS DE INTERESSES (Interação com Entidades Especializadas em Segurança da Informação)

2.24. A Companhia deve manter contato com grupos especializados e fóruns de segurança da informação para promover atualização contínua, troca de conhecimentos e cooperação em ações preventivas e corretivas. Este relacionamento será realizado conforme orientações das áreas específicas, preservando segredos de negócio e assuntos confidenciais.

DISPOSIÇÕES GERAIS

2.25. O Descumprimento das diretrizes estabelecidas nesta Política será tratado com a devida seriedade e poderá resultar na aplicação de sanções disciplinares, administrativas e/ou legais, conforme a gravidade da infração e a legislação vigente.

a) As sanções podem incluir, mas não se limitam a:

- Advertência verbal ou escrita;
- Suspensão temporária de acessos a sistemas e recursos tecnológicos;
- Medidas disciplinares previstas em regulamentos internos da organização;
- Responsabilização civil e/ou criminal, quando aplicável.

b) A aplicação das sanções observará sempre os princípios da proporcionalidade, razoabilidade e do devido processo, garantindo ao colaborador o direito à ampla defesa e ao contraditório.

c) A Política será revisada regularmente para assegurar sua eficácia e alinhamento com as mudanças tecnológicas, regulatórias e organizacionais.

3. REFERÊNCIAS

3.1. Esta Política está fundamentada em boas práticas de mercado, legislações aplicáveis e documentos normativos internos da Companhia que suportam sua implementação e aplicação. São referências:

3.1.1. Referências Técnicas Externas

a) ISO/IEC 27001:2022 – Sistema de Gestão da Segurança da Informação;

b) NIST Cybersecurity Framework – Estrutura de referência para Cibersegurança;

c) Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.

3.1.2. Documentos da Companhia

a) Estatuto Social;

b) Código de Conduta e Integridade; e

c) Política de Privacidade, Proteção de Dados Pessoais e Uso Responsável de Inteligência Artificial.

1. **Conselho de Administração**
   a) deliberar e aprovar a Política de Segurança Cibernética e da Informação, assegurando sua integração ao planejamento estratégico e à gestão de riscos da Companhia, bem como acompanhar a efetividade e os resultados da política implementada.

2. **Alta Administração**
   a) assegurar os recursos e a estrutura necessários para a plena implementação da Política de Segurança da Informação, bem como realizar seu monitoramento e acompanhamento, alinhando a execução às diretrizes do plano estratégico aprovado.

3. **Diretoria Executiva de Clientes e Tecnologia**
   a) garantir que objetivos da Política de Segurança Cibernética e da Informação estejam compatíveis com a estratégia da Companhia, assegurando sua aplicação técnica e operacional conforme os recursos e estrutura definidos pela Alta Administração; e
   b) aprovar exceções à esta política, quando necessário.

4. **Gerência de Segurança da Informação**
   a) criar e manter atualizado uma Política de Segurança Cibernética e da Informação com as diretrizes executivas sobre o tema, bem como procedimentos para apoiar a sua operacionalização;
   b) atuar como agente responsável pelas ações estratégicas, táticas e operacionais sobre segurança cibernética e da informação, apoiando as áreas de negócio no momento da concepção de novos produtos e serviços;
   c) promover a cultura de segurança cibernética e da informação dentro da Companhia, além de realizar anualmente iniciativas de treinamento e conscientização sobre o tema para todos os colaboradores;
   d) identificar, gerenciar e monitorar riscos de segurança cibernética e da informação, bem como definir e implementar estratégias para contenção, mitigação e eliminação dos riscos;
   e) criar e gerir indicadores de performance do ambiente de segurança cibernética e da informação;
   f) estabelecer e coordenar a Comissão de Segurança Cibernética; e
   g) apoiar as áreas quanto a assuntos não previstos nessa Política.

5. **Colaboradores**
   a) conhecer e cumprir as diretrizes estabelecidas na Política de Segurança Cibernética e da Informação e das normas vigentes e correlacionadas;
   b) atuar de forma engajada e proativa em relação a segurança da informação, incluindo, mas não se limitando ao cumprimento das diretrizes da Política de Segurança Cibernética e da Informação; e
   c) comunicar ameaças digitais e possíveis incidentes cibernéticos por meio dos canais de comunicação disponíveis.