POLÍTICA de SEGURANÇA da INFORMAÇÃO

No cumprimento da sua Missão e Visão, suportando-se nos seus Valores e Ética, a Águas do Tejo Atlântico efetua o tratamento de um conjunto relevante de informação e de dados, incluindo dados pessoais, nomeadamente de trabalhadores, fornecedores e de clientes. Esta informação representa um ativo crítico para a atividade da Águas do Tejo Atlântico, pelo que a sua adequada proteção constitui uma necessidade e uma responsabilidade da Empresa, que disponibiliza todos os recursos necessários para a operacionalização dos processos e atividades relacionadas com a Segurança de Informação e com a proteção dos dados pessoais.

Esta política pretende ainda estabelecer as diretrizes para o modelo de referência no que respeita a definição dos objetivos de segurança da informação, detalhados nos demais procedimentos ou instrumentos normativos da Águas do Tejo Atlântico.

Assim, de modo a cumprir com a legislação, instrumentos contratuais, política de segurança de informação do Grupo AdP e demais normativos, em vigor e aplicáveis, almejando prevenir riscos suscetíveis de afetar a informação, os cidadãos e a continuidade da atividade normal da Empresa ou a sua reputação, estabelecem-se os seguintes princípios, que passam a constituir esta Política:

1. Segurança da Informação – Assegurar uma eficaz e adequada proteção da Informação por si detida, através dos meios adequados (automatizados ou não), garantir a sua confidencialidade, integridade e disponibilidade, incluindo nas transferências de informação.

   Assegurar simultaneamente perfis e acessos de acordo com as necessidades operacionais da Empresa, as competências e formação técnica necessária às funções e a realização de ações de formação e sensibilização dos utilizadores em toda a relação com os seus stakeholders.

2. Proteção de Dados Pessoais – Garantir a proteção dos dados pessoais, que são tratados na empresa e pelos seus subcontratantes, com respeito pela licitude, lealdade, proporcionalidade e transparência no seu tratamento, de acordo com os direitos, liberdades e garantias fundamentais das pessoas singulares e no cumprimento das obrigações decorrentes do Regulamento Geral de Proteção de Dados e demais legislação aplicável.

3. Privacidade por Defeito – Submeter todos os procedimentos implementados ou a implementar na Empresa, que incluam o tratamento de dados pessoais e/ou informação ao abrigo do SGSI – Sistema de Gestão de Segurança da Informação, ao conceito de privacidade por defeito, devendo, em consequência, ser implementadas em todos os projetos ou iniciativas medidas técnicas e organizativas adequadas, a que, por regra, só sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento, com consequências na quantidade de dados recolhidos, na extensão do seu tratamento, no prazo de conservação e na sua acessibilidade, de forma a garantir a sua proteção e a privacidade da informação, independentemente do meio e ferramentas utilizadas no tratamento.

4. Gestão e Proteção dos Ativos de Informação – Implementar todas as medidas, físicas ou digitais, adequadas a garantir a segurança da informação em todo o ciclo de vida, a sua classificação, manuseamento e destruição de acordo com o nível de risco, respeitando os requisitos de identificação, autenticação e não repúdio, com verificações do seu cumprimento e eficácia, procurando proceder à mitigação dos riscos que possam colocar em causa a segurança da informação, a proteção dos dados pessoais e a continuidade do negócio.

5. Propriedade Intelectual – Assegurar que toda a informação resultante de processos/atividades que colaborem, interajam, ou possuam uma relação com a Tejo Atlântico, é propriedade da Empresa, exceto definido em aprovação formal entre as partes, garantindo o cumprimento da Política de gestão da propriedade intelectual da Águas do Tejo Atlântico.

6. Envolvimento e consciencialização dos Trabalhadores – Divulgar e comunicar junto de todos os trabalhadores os princípios relativos à segurança da informação e proteção de dados pessoais e promover ações de informação e de consciencialização para o cumprimento desta política. Todos os trabalhadores devem estar comprometidos, cumprir e fazer cumprir os princípios e os documentos normativos internos ou legais aplicáveis neste âmbito.

7. Subcontratos e Prestação de Serviços – Vincular todos os prestadores de serviços, subcontratados e demais entidades que se relacionem com a Empresa, ao cumprimento das obrigações decorrentes da presente Política nas partes aplicáveis, do Regulamento Geral de Proteção de Dados, da legislação e regulamentação relacionadas com a segurança de informação e com a proteção de dados pessoais aplicáveis dos instrumentos contratuais e demais normativos em vigor nesta matéria, através de vínculo contratual adequado.

8. Registos e Evidências – Registar todas as atividades relacionadas com o tratamento de dados pessoais, as medidas de segurança da informação adotadas, os intervenientes e os responsáveis das mesmas, de forma a evidenciar o cumprimento legal, as boas práticas de segurança da informação e de garantia de proteção de dados pessoais.

9. Eventos de Segurança da Informação – Reportar ao CISO e ao DPO qualquer evento de segurança de informação, que possa colocar em causa a confidencialidade, a integridade e/ou a disponibilidade da informação. Colaborar na investigação e na adoção, em tempo útil, de medidas de proteção, mitigação e corretivas, seguindo os procedimentos instituídos na empresa, e se necessário cooperar com as autoridades competentes.

10. Comité de Segurança da Informação (CSI) – Constituído pelo CISO, DPO, CRO e representantes das direções/áreas de Sistemas e Soluções Digitais, Segurança e Sustentabilidade Empresarial, Jurídico. Acompanha e analisa informação e situações inerentes à segurança da informação, reportando e realizando recomendações ao CE da Empresa.

11. Melhoria Contínua - Assegurar a melhoria contínua do Sistema de Gestão de Segurança da Informação, adotando as medidas que se considerem necessárias de forma atingir os objetivos definidos, nomeadamente auditorias internas/externas periódicas.

12. Continuidade de Negócio - Assegurar mecanismos de continuidade de negócio, incluindo a resiliência através de redundâncias necessárias e a continuidade da segurança da informação, de acordo com a sua criticidade e impacto, nomeadamente em forma manual imediata e alternativa à digital, contemplando a perda de sistemas ou informação cuja recuperação se possa prolongar no tempo.

13. Localização e Transferência de Dados – Garantir que os dados pessoais e a informação crítica da Empresa são tratados, armazenados e alojados preferencialmente em território da União Europeia ou do Espaço Económico Europeu, assegurando o cumprimento do Regulamento Geral de Proteção de Dados, da legislação aplicável.

14. Localização, Retenção e Transferência de Dados – Garantir que os prestadores de serviços, subcontratantes e demais entidades que tratem, armazenem ou alojem dados da Empresa asseguram que os dados pessoais e a informação crítica são tratados apenas na União Europeia ou no Espaço Económico Europeu, em cumprimento do Regulamento Geral de Proteção de Dados, da legislação aplicável e dos normativos internos em vigor. Todos os prestadores de serviços e subcontratantes são obrigados a assegurar mecanismos adequados

de segurança, confidencialidade, retenção, arquivo, eliminação segura, controlo de acessos, encriptação, monitorização, backups, continuidade de negócio e recuperação de desastre, de acordo com a criticidade da informação e os requisitos do Sistema de Gestão de Segurança da Informação da AdTA.