POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DATA: 11.05.2022

Destinatários:	Todos/as os/as trabalhadores/as, a gestão de topo e outras partes interessadas nomeadamente colaboradores/as externos, estagiários/as, fornecedores ou qualquer outra entidade que de alguma forma interaja com os ativos de informação da organização.

Objetivo: Definir os princípios e as regras básicas da gestão da Segurança da Informação

No cumprimento da sua Missão e Visão, suportando-se nos seus Valores e Ética, a EPAL/AdVT efetua o tratamento de um conjunto relevante de informação e de dados, incluindo dados pessoais, nomeadamente de trabalhadores/as, fornecedores e de clientes. Esta informação representa um ativo crítico para a atividade da EPAL/AdVT, 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.

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, as cidadãs e a continuidade da atividade normal da Empresa ou a sua reputação, estabelecem-se os seguintes compromissos, 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, assegurando simultaneamente perfis de acordo com as necessidades operacionais da Empresa, as funções e competências, a realização de ações de formação e sensibilização dos/as utilizadores/as e 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, 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. **Proteção da Informação** – Implementar todas as medidas, físicas ou digitais, adequadas a garantir a segurança da informação, a sua classificação e manuseamento 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. **Envolvimento e consciencialização dos/as Trabalhadores/as** – Divulgar e comunicar junto de todos/as os/as trabalhadores/as 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 e as trabalhadoras devem estar comprometidos/as, cumprir e fazer cumprir os princípios e os documentos normativos internos ou legais aplicáveis neste âmbito.

6. **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.

7. **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.

8. **Eventos de Segurança** – Reportar ao CISO e ao EPD 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.

9. **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.

10. **Continuidade de Negócio** - Assegurar mecanismos de continuidade de negócio, incluindo as 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.