POLÍTICA de SEGURANÇA da INFORMAÇÃO

Cibersegurança

Elaboração:	CISO	**Validação:**	CISO/CSI	**Aprovação:**	CE

ÍNDICE

Acrónimos

- AdP – Águas de Portugal
- CISO – *Chief Information Security Officer*
- CSI – Comité para a Segurança da Informação
- DPO – *Data Protection Officer*
- DRP - *Disaster Recovery Plan*
- JUR – Departamento Jurídico
- RGPD – Regulamento Geral de Proteção de Dados
- SI – Segurança da Informação
- SSE – Departamento de Segurança e Sustentabilidade Empresarial
- STI – Departamento de Sistemas e Tecnologias de Informação

1. Objetivo

A Águas do Tejo Atlântico, S. A., doravante identificada por Tejo Atlântico, é responsável pela gestão e exploração do sistema multimunicipal de saneamento de águas residuais da Grande Lisboa e Oeste, e durante o desempenho da sua atividade procede à criação, recolha, tratamento e gestão de informação, onde se incluem dados pessoais, para a realização dos seus objetivos em sintonia com a sua missão e visão.

A Tejo Atlântico visa, com a presente política, constituir uma base comum à organização para a implementação de uma cultura de segurança da informação garantindo a adoção de boas práticas em matéria de segurança da informação, nomeadamente com o previsto na Norma ISO/IEC 27001:2013, de modo a estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação; em cumprimento da Lei n.º 46/2018, de 13 de Agosto, que aprova o Regime Jurídico de Segurança do Ciberespaço e do Decreto – Lei n.º 65/2021, de 30 de julho, que regulamenta a Lei n.º 46/2018, de 13 de agosto e executa na ordem jurídica nacional, as obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, permitindo a implementação de um quadro nacional de certificação da cibersegurança, bem como com a Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

Com a referida cultura enraizada de forma transversal e fluente, uma organização torna-se mais resistente a incidentes de segurança da informação, assim como também permitirá o estabelecimento de relações de confiança nos intercâmbios com outras organizações.

2. Âmbito

A presente política aplica-se a todos os que, de alguma forma, colaboram, interagem, ou possuam uma relação com a Tejo Atlântico, assim como também aos ativos físicos e lógicos que armazenem, processem ou transmitam informação na ou com a empresa, sendo responsabilidade de todos cumprir e fazer cumprir as obrigações, políticas e procedimentos estabelecidos para o cumprimento da presente política, e entender a importância da segurança da informação nas suas atividades diárias.

3. Política de Segurança da Informação do Grupo AdP

A presente política materializa e complementa, de forma adaptativa a realidade e especificidades da Tejo Atlântico, a política de Segurança da Informação do Grupo AdP.

4. Responsabilidades

A segurança da informação é da responsabilidade da Administração da Tejo Atlântico, que age de forma prudente, fazendo uma gestão adequada da segurança da informação com base no conhecimento transmitido, traduzindo assim o compromisso formal da Tejo Atlântico e a relevância da segurança da informação na presente política.

Foi criado, na Tejo Atlântico, o Comité para a Segurança da Informação (CSI), que é responsável por:

- Análise e parecer sobre políticas, procedimentos, manuais e regulamentos de sistemas de informação e de segurança da informação, objetivos de segurança da informação, segurança física, *Disaster Recovery Plan* (DRP), plano de continuidade de negócio e plano de segurança, assegurando o respeito pelos requisitos estatuários, regulamentares e legislativos aplicáveis;

- Análise dos relatórios periódicos de incidentes de segurança física e lógica;

- Aprovação dos planos anuais de exercícios de avaliação de segurança, DRP e continuidade de negócio;

- Análise e parecer sobre a atribuição de acessos;
- Análise e parecer sobre a atribuição de responsabilidades de segurança;
- Análise e parecer sobre o inventário de ativos, a análise de risco, plano de tratamento do risco e decisão e priorização de implementação de iniciativas/projetos para melhoria dos sistemas de segurança, em função dos riscos identificados;
- Análise das métricas e indicadores de avaliação dos sistemas de segurança e propostas de melhoria;
- Análise e parecer sobre temas de segurança da informação submetidos ao CSI.

O CSI é constituído por um elemento em representação das seguintes áreas funcionais/pelouros da Tejo Atlântico:

- Cibersegurança
- Gestão do Risco
- Proteção de Dados
- Departamento Jurídico (JUR)
- Departamento de Sistemas e Tecnologias de informação (STI)
- Departamento de Segurança e Sustentabilidade Empresarial (SSE)

O CSI pode convidar à participação outras áreas funcionais/pelouros, para apreciação de temas que envolvam diretamente a área funcional em questão.

É da responsabilidade do CISO da Tejo Atlântico, em articulação com o STI e com o DPO, garantir a conformidade da presente Política de Segurança da Informação com os requisitos estatuários, regulamentares e legislativos aplicáveis, bem como acompanhar e avaliar a aplicação da mesma, assegurar a sua melhoria contínua com revisões regulares e extraordinárias, quando necessário, a submeter ao CSI, e comunicar à gestão de topo o seu desempenho.

Perante a existência de um incidente de segurança que envolva a violação das obrigações decorrentes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

desses dados, executado através da Lei n.º 58/2019, de 8 de agosto, designado de ora em diante por Regulamento Geral de Proteção de Dados (RGPD), as competências e responsabilidades pertencem ao DPO da Tejo Atlântico.

5. Segurança da Informação

A Tejo Atlântico cria, trata e gere informação, a qual pode adotar diversos formatos ou meios de suporte (impressa ou escrita em papel, armazenada eletronicamente, entre outros) e ser transmitida por correio, meios eletrónicos ou verbalmente, devendo ser adequadamente protegida independentemente do seu formato, utilização ou transmissão.

Sendo essa informação considerada um ativo crítico à atividade da Empresa, esta assume, através da presente política, a responsabilidade e o compromisso de uma proteção e tratamento adequados da mesma, através de meios apropriados, fundamentados nos seguintes princípios:

- Disponibilidade da Informação - Garantir o acesso à informação sempre que necessário, unicamente a pessoas autorizadas para o efeito;
- Integridade da Informação – Assegurar a exatidão, consistência e a confiança da informação, salvaguardando que a mesma é alterada unicamente por pessoas devidamente autorizadas;
- Confidencialidade da Informação – Impedir acesso à informação por pessoas sem a devida autorização;
- Rastreabilidade da Informação – Assegurar a capacidade de registo das atividades relacionadas com o tratamento de dados, sempre que tecnicamente possível, de forma recuperar o histórico das ações concretizadas, que deverá estar atualizado e disponível em qualquer momento.

Simultaneamente pretende-se assegurar as necessidades operacionais da Tejo Atlântico, a formação e sensibilização dos utilizadores e a relação com os seus *stakeholders*.

6. Proteção de Dados Pessoais

Quando a informação contém dados pessoais, o seu tratamento deve cumprir o determinado no RGPD nos termos da legislação em vigor e da Política de Proteção de Dados Pessoais.

A Tejo Atlântico deve garantir a proteção dos dados pessoais, 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 RGPD.

6.1 Privacidade por Defeito

Todos os procedimentos implementados ou a implementar na Tejo Atlântico, que incluam o tratamento de dados pessoais, devem ser submetidos ao conceito de privacidade por defeito, devendo, em consequência, ser implementadas 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 pessoais 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.

7. Gestão da Segurança da Informação

De modo a assegurar que o tratamento de informação na Tejo Atlântico encontra-se devidamente protegido, devem ser adotados processos nesse sentido.

7.1 Gestão de Ativos

Os ativos físicos e lógicos que armazenem, processem ou transmitam informação devem ser identificados, inventariados e protegidos contra acessos indevidos e possuírem documentação e planos de manutenção atualizados.

7.2 Classificação da Informação

A informação deve ser classificada de acordo com o nível de confidencialidade necessária, considerando as necessidades relacionadas com o negócio, a partilha, restrições de acesso e os impactos inerentes à utilização indevida. Deverá igualmente ser considerada cada etapa do seu ciclo de vida, ou seja, a criação, o armazenamento, a utilização, a transferência e a destruição.

A metodologia para a classificação da informação encontra-se detalhada no procedimento P.001 Controlo de Documentos Internos e Registos.

Devem ser promovidos todos os esforços necessários para evitar acessos de pessoas não autorizadas à informação classificada.

7.3 Transferência da Informação

A consulta, tratamento, ou outro, de informação em locais públicos podem originar fugas de informação indesejadas. Assim, não se deve discutir ou comentar assuntos relacionados com informações da Tejo Atlântico, seja em conversa presencial ou por outro meio, em locais públicos, assim como também deve-se evitar a utilização de postos de trabalho ou dispositivos móveis, quando não é possível evitar que terceiros visualizem o conteúdo desses.

Todos os esforços necessários devem ser realizados por forma a garantir que toda e qualquer transferência de informação será realizada por forma a garantir o cumprimento da sua classificação.

7.4 Gestão de Acessos

As atribuições, revisões e revogações de acessos utilizam as ferramentas e os processos da Tejo Atlântico.

Os acessos são concedidos única e exclusivamente para o cumprimento das funções a realizar, assentes no princípio do mínimo acesso necessário. Todos os acessos desnecessários ou em excesso, devem ser prontamente revogados.

Os proprietários dos acessos concedidos são responsáveis pelos mesmos, assim como das ações desencadeadas pela sua utilização. Também são responsáveis por notificar prontamente quando detetem um acesso concedido que seja desnecessário ou em excesso.

Os acessos concedidos à informação da Tejo Atlântico somente podem ser utilizados em dispositivos confiáveis, disponibilizados, ou autorizados pela Tejo Atlântico.

Os acessos devem ser registados por forma a permitirem a rastreabilidade e identificação dos mesmos.

Os acessos concedidos são revistos periodicamente.

7.5 Proteção da informação e Gestão de Riscos

Os riscos de segurança da informação dos ativos que garantem a continuidade do funcionamento das redes e dos sistemas de informação da Tejo Atlântico, devem ser identificados, analisados e avaliados, com

periodicidade mínima anual, para se determinar a exposição ao risco e priorizar e aplicar medidas técnicas e organizativas para evitar, mitigar ou transferir esse risco de forma a eliminá-lo ou minimizá-lo para um nível aceitável, protegendo assim a informação.

7.6 Incidentes de Segurança da Informação e Cibersegurança

Todo e qualquer evento que configure um comportamento desviante do funcionamento padrão, que seja suspeito de colocar em causa a confidencialidade, disponibilidade ou a integridade da informação, ou que represente uma violação à presente política, deve ser prontamente reportado à equipa do Departamento de STI da Tejo Atlântico.

Para os casos que configurem incidentes de segurança da informação, as medidas corretivas necessárias serão adotadas, em tempo útil pela Tejo Atlântico, assim como a colaboração ativa com as autoridades competentes, seguindo as boas práticas e os requisitos legais em vigor.

7.7 Consciencialização em Segurança da Informação

A base para uma cultura de segurança da informação forte, na Tejo Atlântico, é a aposta na consciencialização e capacitação de todas as unidades orgânicas da Empresa, para que juntos e em uníssono configurem um ambiente mais resistente à ocorrência de incidentes.

De forma a concretizar uma cultura forte, a Empresa promove regularmente a disseminação de princípios, diretrizes e boas práticas em segurança da informação, através de programas de consciencialização e capacitação adequados à responsabilidade pelo cumprimento da presente política.

7.8 Avaliação e Auditoria

São efetuadas avaliações à efetividade das políticas procedimentos, manuais e regulamentos de segurança da informação, através da realização de auditorias internas com periodicidade mínima anual.

7.9 Propriedade intelectual

Toda a informação resultante de todos os que, de alguma forma, colaboram, interagem, ou possuam uma relação com a Tejo Atlântico, é propriedade da Empresa, exceto perante a existência de vínculo contratual, protocolo, ou outro, firmado entre as partes, que altera essa propriedade. Em caso de cessação da relação

estabelecida, toda a informação criada e tratada deverá ser restituída à Tejo Atlântico, ou emitida declaração a atestar a sua destruição de forma conveniente.

Marcas, patentes, metodologias, tecnologias e quaisquer informações que pertençam à Tejo Atlântico, não podem ser utilizadas para fins particulares ou outros, nem transmitidas externamente, sem a devida autorização da Tejo Atlântico.

7.10 Política de Segurança da Informação, Legislação e Regulamentos

A presente Política de Segurança da Informação é complementada por documentos do sistema de gestão, nomeadamente políticas, procedimentos, manuais e regulamentos relacionados com segurança da informação, aprovados pela Administração da Tejo Atlântico em conformidade com aspetos legais e regulamentares.

A todos os que, de alguma forma, colaboram, interagem, ou possuam uma relação com a Tejo Atlântico, têm a responsabilidade de conhecer e cumprir com a legislação em vigor e com os requisitos complementares, à presente política, que lhes sejam aplicáveis.

7.11 Utilização de Recursos de Informação

Equipamentos particulares/privados/externos à Empresa, como computadores ou quaisquer outros dispositivos que possam armazenar e/ou processar dados, não devem ser utilizados para aceder, armazenar ou processar informações da Tejo Atlântico, nem ligados às redes da Organização, com exceção das redes criadas para o efeito ou mediante autorização da Tejo Atlântico.

Apenas os equipamentos e *software* disponibilizados e autorizados pela Tejo Atlântico podem ser instalados e ligados à rede da Tejo Atlântico.

Todos os ativos de suporte de informação devem ser devidamente guardados, especialmente documentos em papel. Os documentos não devem ser abandonados após a sua cópia, impressão ou utilização, pelo que devem de ser devidamente guardados ou destruídos.

Todos e quaisquer ativos de suporte e meios de acesso à informação, por exemplo a conta de acesso (nome de utilizador/palavra-chave), são da responsabilidade do seu utilizador, assim como por todos os atos executados pela utilização dos mesmos. Qualquer suspeição de acesso ou utilização indevida dos anteriores, deve ser prontamente reportado à equipa do Departamento de STI da Tejo Atlântico.

8. Medidas aplicáveis Violações das Políticas de Segurança da Informação

A violação ou o incumprimento da presente Política de Segurança de Informação será punida nos termos da legislação aplicável.

9. Manutenção e Divulgação das Políticas de Segurança

A presente política deve ser avaliada e/ou revista pelo CISO e submetida ao CSI para apreciação prévia à aprovação pela Administração da Tejo Atlântico, com uma periodicidade mínima anual, de forma a garantir a sua adequação ao cumprimento da visão e missão da Tejo Atlântico em sintonia com as boas práticas e legislação em vigor, devendo a mesma ser comunicada a todos os que, de alguma forma, colaboram, interagem, ou possuam uma relação com a Tejo Atlântico.

10. Resumo das alterações

Capítulo/secção	Data da revisão	Descrição
-	03/11/2021	Aprovação da Política de Segurança da Informação (Filedoc n.º 103123-202111)
3 e 6.2	22/02/2023	Criação de lista de Acrónimos, criação do novo capítulo "Política de Segurança da Informação do Grupo AdP" (3), alteração significativa ao subcapítulo da Classificação da Informação e ligeiras alterações nos restantes (Filedoc n.º 100386-202302)

Assinado por: **PAULO ALEXANDRE CÁCERES FERREIRA**
Data: 2023.03.13 17:42:01+00'00'