POLÍTICA

Sistema de Gestão Integrado

SEGURANÇA DA INFORMAÇÃO

Referência do Documento | PL03_V10

ÍNDICE

1. Referências 3
2. Documentos associados 3
3. Registos associados 3
4. Lista de distribuição 3
5. Histórico do documento 3
6. Classificação do documento 3
7. Registo da revisão: 3
8. Enquadramento estratégico para o negócio 4
9. Motivação para a segurança da informação 4
10. Significado da segurança da informação 4
11. Âmbito de proteção para a segurança da informação 4
12. Compromisso para a segurança da informação 4
13. Gestão do risco 5
14. Gestão de incidentes e gestão da continuidade de negócio 6
15. Políticas complementares 6
16. Integração com outros sistemas de gestão 6
17. Formação e sensibilização 6
18. Divulgação e publicação 7
19. Compromisso para revisão e melhoria contínua 7
20. Funções e responsabilidade 7
21. Contexto da organização 7
22. Verificação do documento 7

1. Referências	ISO/IEC 27001:2013 | 4.1, 5, A.5.1.1 e A.5.1.2. ISO/IEC 20000:2018 | 8.7.3., 6.3.(c) ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 421 ETSI EN 319 401 Regulamento (UE) N.º 910/2014 Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679 do Parlamento Europeu e do Conselho) Lei nº58/2019, de 8 e agosto – Proteção de dados
2. Documentos Associados	PL05_SGSI – Uso aceitável DS24 – Definição do âmbito PL10_GTS – Política de Privacidade
3. Registos Associados	RG01 – Registo de documentos RG02 – Inventário MA04_GTS - Registo de documentos
4. Lista de Distribuição	Público
5. Histórico do Documento	2013-10-07 **|** Versão 1 2014-02-04 **|** Versão 2 2015-01-12 **|** Versão 3 2015-05-26 **|** Versão 4 2016-12-29 **|** Versão 5 2017-11-02 **|** Versão 6 2019-11-25 **|** Versão 7 2021-01-26 **|** Versão 8 2022-09-07 **|** Versão 9 2023-07-07 **|** Versão 10
6. Classificação do Documento	D | Público

7. Registo da revisão:

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	2023-07-07	**2023-07-07**	
10	**T. Compliance**	**D. compliance**	Revisão anual do documento.
	Sofia Perestrelo	Débora Rodrigues	

8. Enquadramento estratégico para o negócio

As opções estratégicas de negócio da ACIN enquadram-se numa dinâmica de expansão da cobertura de atividades e mercados cada vez mais seletivos, em que fatores diferenciadores de qualidade, segurança, fiabilidade, idoneidade e credibilidade são fundamentais para o sucesso.

Desta forma, elege a ACIN a Segurança da Informação como uma ferramenta de gestão que permitirá suportar a concretização dos seus objetivos de negócio.

9. Motivação para a Segurança da Informação

O mercado onde a ACIN está inserida rege-se por regulamentação nacional e internacional aplicável à sua atividade comercial, em matérias de gestão e segurança da informação que os seus clientes colocam à sua custódia nas plataformas eletrónicas.

A ACIN está determinada em acompanhar sistematicamente a evolução desta envolvente legal e integrá-la nos seus sistemas de gestão, assim como em cumprir e fazer cumprir requisitos e determinações contratuais de e para os seus clientes, diretos ou indiretos.

10. Significado da Segurança da Informação

A informação que os clientes da ACIN colocam sob sua custódia é um bem indispensável para a "sobrevivência do negócio".

A política para a segurança da informação da ACIN é um compromisso assumido pela sua Administração, na garantia da implementação e melhoria contínua de um sistema para a sua gestão, doravante denominado SGSI, assegurando a disponibilização dos recursos que sejam necessários para a sua eficácia e assegurando a sua revisão, de acordo com a periodicidade mínima estabelecida.

O SGSI da ACIN será implementado em conformidade com os requisitos da norma ISO/IEC 27001:2013, sendo ainda que a sua Declaração de Aplicabilidade será definida com base na lista de controlos apresentada pelo Anexo A de tal norma.

11. Âmbito de proteção para a Segurança da Informação

O âmbito de proteção do Sistema de Gestão de Segurança da Informação (SGSI) abrange os produtos e serviços disponibilizados pelas plataformas aplicacionais da ACIN, tendo em conta as exceções apresentadas no DS24 - Definição do âmbito do SGI.

12. Compromisso para a Segurança da Informação

- ✓ Confidencialidade

Garantia de que a informação de clientes que é confiada à custódia das plataformas eletrónicas da ACIN, inseridas no âmbito de proteção, é acedida apenas a quem está formalmente autorizado para esse efeito.

- ✓ Integridade

Garantia de proteção da exatidão da informação recebida, processada, armazenada e transmitida por responsabilidade da ACIN, nas suas plataformas eletrónicas inseridas no âmbito de proteção.

- ✓ Disponibilidade

Garantia de que a informação tratada no âmbito de proteção está acessível, e quando necessário, para realizar uma atividade de um processo de negócio, dentro dos níveis de serviço definidos formalmente, e respeitando o compromisso de confidencialidade e integridade.

- ✓ Privacidade de Dados

Garantia da privacidade e a confiança dos seus titulares e parceiros, promovendo a total proteção sobre a privacidade e segurança dos dados pessoais.

- ✓ Não Repúdio

Garantir que o autor não negue ter criado e assinado o documento.

- ✓ Autenticidade

Garantir que a validade da transmissão, da mensagem e do seu remetente. O objetivo é que o destinatário possa comprovar a origem e autoria de um determinado documento.

13. Gestão do Risco

Com o objetivo de assegurar prontidão e conformidade do seu SGSI, a ACIN assume o compromisso de identificar, analisar, qualificar e tratar o risco decorrente de várias fontes de ameaças para os seus compromissos.

Todos os riscos de segurança da informação são devidamente avaliados e documentados em intervalos planeados.

A política de gestão do risco da ACIN define a metodologia adotada para tratamento dos riscos assim identificados, sendo baseada nas melhores práticas definidas em normas internacionais de referência, e constitui-se como uma ferramenta de gestão da empresa.

14. Gestão de Incidentes e Gestão da Continuidade de Negócio

Todos os eventos que coloquem em causa os compromissos de segurança da informação serão tratados como possíveis incidentes de segurança e, como tal, inseridos no processo de gestão de incidentes da ACIN.

O respetivo diagnóstico de causas, consequências, medidas de controlo e mitigação do risco decorrentes serão tratadas segundo as melhores práticas, estando previsto a ativação de processos disciplinares e ações judiciais para matérias que revelem dolo ou violação de responsabilidades assumidas por terceiras partes.

A disponibilidade da informação, não descurando a responsabilidade dos restantes compromissos de segurança da informação, será assegurada pela implementação de respostas a incidentes disruptivos e que se integram no âmbito do Plano de Continuidade de Negócio da ACIN.

15. Políticas complementares

Sempre que considerado relevante para a eficácia do SGSI, a ACIN definirá políticas temáticas que descrevem as práticas executadas em diversas matérias no âmbito de proteção, assim como a implementação de controlos decorrentes da necessidade de tratamento do risco.

Estas políticas temáticas serão aprovadas pela Liderança do SGSI, por proposta do seu coordenador.

16. Integração com outros sistemas de gestão

A ACIN assegura que o SGSI será sempre o sistema de gestão que assegura o tratamento de temas relacionados com a Segurança da Informação, seja quais forem os sistemas de gestão implementados e mantendo uma abordagem de sistema de gestão integrado.

Em função da atual implementação do Sistema de Gestão da Norma ISO/IEC 20000-1:2018, compromete-se a ACIN a alinhar os interesses e âmbitos de ambos sistemas, tendo em vista um futuro sistema integrado.

17. Formação e sensibilização

A sensibilização, treino e formação sistemática dos colaboradores da ACIN em matérias de segurança da informação é uma forte aposta decorrente do compromisso da empresa para a eficácia do SGSI.

Estas iniciativas são incluídas num Plano de Formação anual que será auditado na eficácia da sua execução.

18. Divulgação e publicação

A divulgação da formalização das decisões da Liderança do SGSI é assegurada através de um processo de comunicação interna.

A publicação interna de documentos relevantes para a operacionalização da segurança da informação é considerada essencial para que os colaboradores da empresa se sintam corresponsáveis, cumpram e façam cumprir as determinações do SGSI, e sustentam ações de formação integradas no Plano de Formação anual.

A presença de entidades em subcontratação para prestação de serviços leva a que a ACIN integre os respetivos colaboradores nas ações que forem consideradas pertinentes, havendo a acrescentar o compromisso em promover a divulgação de políticas e práticas junto destas entidades, tendo por base acordos devidamente formalizados para esse efeito.

19. Compromisso para revisão e melhoria contínua

A Liderança da ACIN compromete-se a assegurar a revisão pela gestão do SGSI em intervalos planeados, ou sempre que alterações significativas ocorram na empresa, com o objetivo de assegurar a sua adequação e eficácia, certificando nesse ato a evidência do compromisso para a melhoria contínua do SGSI.

20. Funções e responsabilidade

Ciente da importância de assegurar a implementação, operacionalidade, revisão e melhoria contínua do SGSI, a gerência da ACIN atribui a um dos seus elementos a função de Liderança deste sistema.

Com as respetivas atribuições e responsabilidades detalhadas no *Manual de Funções e Responsabilidades* da ACIN, a Liderança nomeia um colaborador responsável pela coordenação do SGSI.

21. Contexto da Organização

Foram determinadas as seguintes questões externas e internas que considera a ACIN relevante para poder atingir os resultados e objetivos esperados, que se encontram espelhados no DS24-Definição do Âmbito.

22. Verificação do documento

Pelo menos uma vez ao ano, ou quando aplicável, a política deverá ser revista, assim como a sua aplicabilidade.