Política Interna de Segurança da Informação

nosi
we believe in...

Controlo de Documentação

Histórico de Versões

Versão	Data	Autor	Descrição	Classificação
1.0	16/06/2020	Direção de Segurança & Compliance	Criação do documento	Interna

Versão	Implementado por:	Revisto por:	Aprovado por:
1.0	• Ider Andrade • José Mendes	• Adilson Rodrigues	• Conselho de Administração do NOSi, EPE

Informações de Contacto

Nome	Endereço	Email
Direção de Segurança & Compliance	Data Center do Estado, Avenida António Mascarenhas - Achada Grande Frente, Praia	dsc@nosi.cv

/Adilson Rodrigues/

/Diretor de Segurança & Compliance do NOSi, EPE/

/Carlos Tavares Pina/

/Presidente do Conselho de Administração NOSi, EPE/

Índice

1. Introdução

A adoção de políticas, normas e procedimentos que visam garantir a salvaguarda da informação deve ser das principais prioridades de qualquer organização, com o intuito de reduzir os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos pretendidos.

A implementação de uma Política de Segurança da Informação (doravante PSI) mais do que uma atitude estratégica a Organização, é uma ação indispensável, baseada nas finalidades daquela instituição, que de entre outras coisas, seja garantir que no tratamento da informação, a sua segurança seja um fator vital ao êxito do trabalho desenvolvido. Desta feita, as políticas internas de segurança da informação, como uma componente primordial, mas também sensível de uma organização, incluem bases de dados, ambientes informáticos, documentos, arquivos e outras ferramentas tecnológicas e/ou aplicacionais que a envolvam.

As tecnologias de informação “frutos” da Quarta Revolução Industrial, consubstanciam-se numa ferramenta primordial para o crescimento económico, assim como um vetor relevante na melhoria de vida das pessoas. No entanto, os sistemas de informação são cada vez mais postos à prova por diversos tipos de ameaças com origens diversificados, como são as fraudes eletrónicas, os ataques DoS (Denial of Service), a espionagem, fugas de informação, sabotagem, entre outros, que com o passar dos tempos se revelam mais sofisticados e ambiciosos.

A dependência dos sistemas e serviços de informação, leva a crer que as organizações estão cada vez mais vulneráveis às ameaças de segurança. O uso simultâneo de redes públicas e privadas e a partilha de recursos de informação, são fatores que contribuem para o acréscimo da dificuldade de controlo de acessos, e de segurança dos mesmos.

No caso do Núcleo Operacional da Sociedade de Informação – EPE (doravante NOSi), pela posição que ocupa no processo de transformação digital no setor público Cabo-Verdiano, e na promoção da inovação e governação eletrónica,

mais do que essencial, é de necessidade garantir a proteção da informação gerada.

Desta feita, é criada esta PSI, como medida preventiva contra a manipulação da informação e dados gerados e geridos pelo NOSI, adequada aos princípios e valores defendidos pela instituição.

2. OBJETIVO E ÂMBITO

Se por um lado, a informação e os seus processos de apoio, sistemas e redes, são bens essenciais ao negócio de uma organização, por outro há que garantir os 3 (três) princípios fundamentais da segurança da informação, a Confidencialidade, a Integridade e a Disponibilidade, comumente denominados como *tríade CID,* como elementos essenciais para preservar a competitividade, faturação, rentabilidade e a própria imagem de uma organização no mercado.

A PSI como documento que orienta e estabelece as diretrizes corporativas do NOSi, para a proteção dos ativos de informação, deve, portanto, ser cumprida e aplicada em todos os departamentos e áreas funcionais da instituição, e desta feita por técnicos, colaboradores, estagiários, membros da administração e até mesmo terceiros em quaisquer dependências do NOSi.

A aplicação dos princípios e regras enumerados neste documento não inviabiliza a utilização de medidas complementares de Segurança da Informação no NOSI, definidos por órgãos e entidades competentes.

Além desta PSI, serão criadas outras políticas, normas e procedimentos de caráter mais específicos, que permitirão maior nível de proteção da informação.

A presente PSI além de basear-se nas recomendações propostas pela norma ISO/27001 e ISO/27002, reconhecida mundialmente como um standard de prática para a gestão de segurança da informação, está também em conformidade com as leis nacionais vigentes e as melhores práticas internacionais de segurança da informação.

Salvo se explicitamente definida o contrário, esta política e os regulamentos a ela associadas, são aplicáveis à totalidade da informação gerida pelo NOSi, EPE.

3. Política de Segurança da Informação

3.1 Declaração de Objetivos

A missão, a visão, os valores e a política do NOSI, bem como o bem-estar, a segurança das pessoas e a segurança de informação, dos ativos e das instalações são fatores chave para atingir as metas e o sucesso do seu negócio.

O NOSi está consciente de que a informação, nomeadamente informação sensível dos colaboradores, cidadãos, clientes, parceiros e do negócio, deve ser tratada de forma a assegurar a sua credibilidade, e que para tal é necessário:

a) Manter o comprometimento com a Segurança de Informação;
b) Garantir e reforçar a conformidade com a regulamentação e exigências legais em vigor;
c) Assegurar a Integridade, a Confidencialidade e a Disponibilidade da Informação;
d) Estabelecer um padrão de qualidade consistente com a dimensão e importância da organização.

Tendo em conta o *supra* exposto, o NOSi desenvolveu esta política, alinhada com as melhores práticas, e que serve de base a um sistema de gestão e organização de Segurança da Informação. Neste sentido, compromete-se, a:

a) Seguir e implementar os princípios descritos nesta Política e normas associadas;

b) Criar a infraestrutura organizacional de suporte, garantindo a sustentabilidade e as evidências necessárias;
c) Definir a estratégia e as normas que devem ser aplicadas no âmbito da gestão de Segurança de Informação;
d) Traduzir as normas numa *Framework* de controlos, que devem ser executados ao nível dos processos e procedimentos;
e) Proceder ao relato regular e transparente do seu desempenho na matéria da Segurança de Informação.

Os princípios aqui descritos refletem a cultura do NOSi e devem ser considerados como princípios gerais de orientação da Segurança de Informação.

A Política agora criada e todos os documentos a eles associados no âmbito da Gestão da Segurança de Informação, deverão ser sujeitos a um processo de revisão e melhoria contínua baseado no modelo PDCA (*Plan* – Planear, *Do* – Executar, *Check* – Verificar, *Act* – Agir), que permita mitigar os riscos subjacentes à proteção de Informação e consequentemente à segurança nos processos para se alcançar os objetivos da empresa.

Esta PSI deve ser monitorizada, analisada e revista em intervalos regulares, de pelo menos uma vez por ano, ou sempre que ocorram situações internas que o justifiquem, bem como alterações legais, para assegurar a adequação e eficácia da mesma.

3.2 Diretrizes de Segurança da Informação

A informação é um bem tão importante como qualquer outro de índole material, pelo que tem de ser protegida da forma mais conveniente possível. Como já foi aqui dado a entender, a segurança da informação protege a informação contra uma multiplicidade de ameaças, visando designadamente, garantir os princípios da tríade CID, assegurar a continuidade do negócio, minimizar os efeitos negativos no mesmo, maximizar a rentabilização dos investimentos e melhorar a qualidade do

serviço prestado. O NOSi considera que a Informação é um ativo crítico da organização, considerado essencial, de modo a que tudo fará para que esse bem inestimável se mantenha intacta, disponível/acessível somente às pessoas autorizadas. São igualmente considerados ativos da organização, todos os recursos informáticos de software e hardware utilizados na administração e gestão da Informação.

A Informação, no sentido mais lato do termo, e independentemente do seu suporte (digital, magnético, documental, etc.), constitui uma componente fundamental estratégica, pelo que o seu correto tratamento gera vantagens acrescidas, em termos de inovação, imagem institucional e prestação de um serviço de qualidade aos clientes e parceiros.

Adicionalmente considera-se de importância estratégica a existência de uma "cultura de segurança", que propicie a todos os colaboradores, uma perspetiva clara das suas responsabilidades no âmbito da Segurança da Informação.

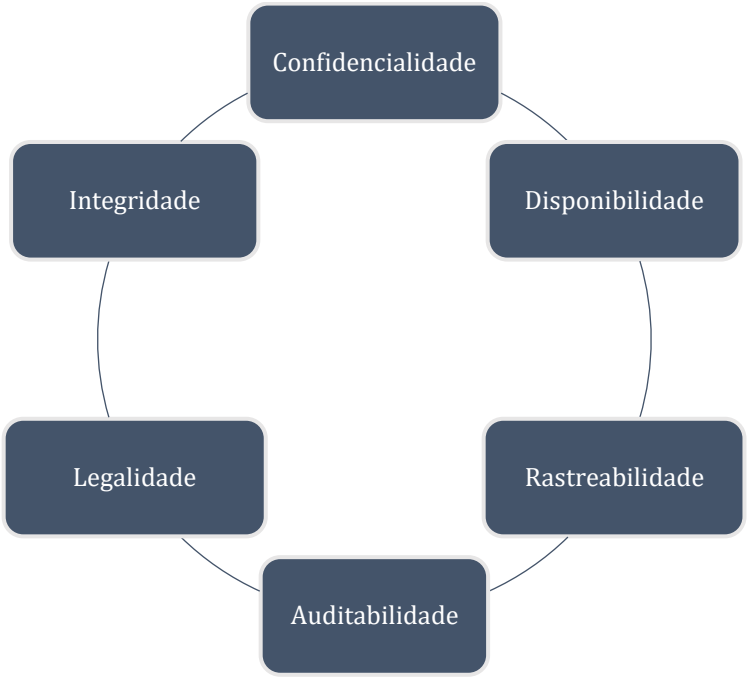
De modo a garantir o correto desempenho das funções para a organização, é indispensável assegurar a todos os colaboradores, estagiários e entidades externas, independentemente do seu nível hierárquico, função e/ou vínculo contratual, o acesso à Informação necessária ao desempenho das respetivas atividades, mas exigindo destes o respeito pelos controlos de Segurança de Informação implementados, e o comprometimento com os princípios da:

a) **Confidencialidade:** A garantia de que a Informação não é divulgada e/ou acedida, de modo acidental ou não, por terceiros ou pessoas sem autorização.
b) **Integridade:** O comprometimento da prevenção contra a modificação e/ou destruição não autorizada da Informação.
c) **Disponibilidade:** Assegurar a acessibilidade da Informação onde e quando necessária e sem demora indevida, para pessoas com autorização para o efeito.

d) **Rastreabilidade:** A garantia das evidências para assegurar a capacidade de recuperação do histórico das ações concretizadas, através de um registo que deverá estar atualizado e disponível em qualquer momento.

e) **Legalidade:** O respeito pelas leis civis e criminais, regulamentações ou obrigações contratuais e requisitos de Segurança de Informação.

f) **Auditabilidade:** A garantia de auditabilidade dos dados e informação corporativa e/ou de negócio são registados, compilados, analisados, e revelados de modo a permitir que auditores internos ou provedores de garantia externos possam testar a sua veracidade.

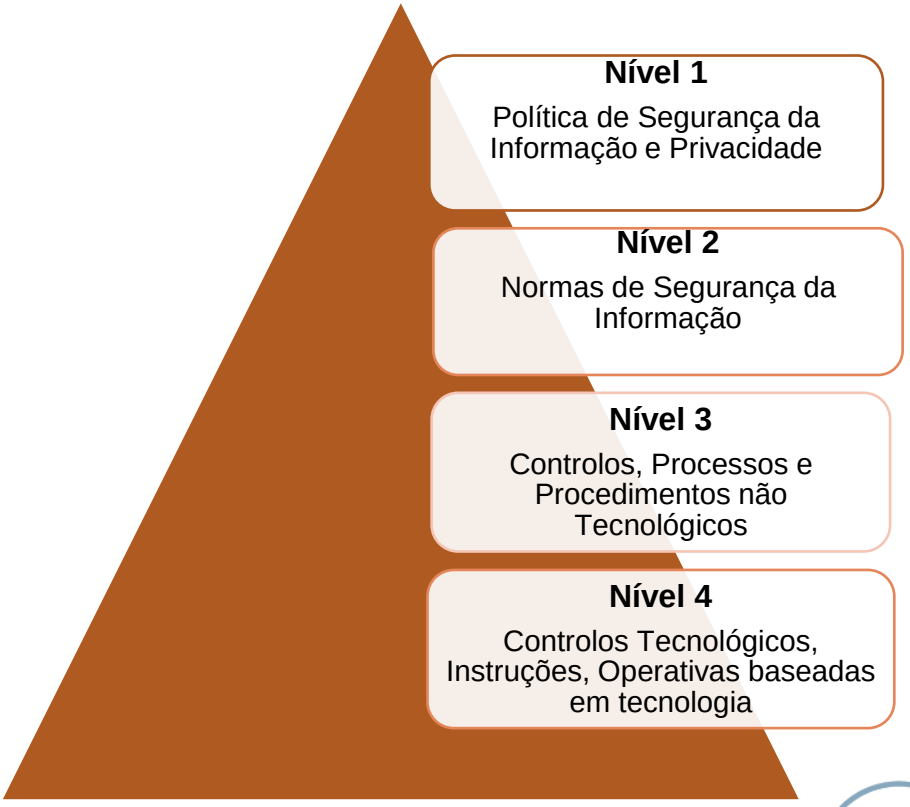


O NOSi assume como sendo sua obrigação garantir os princípios acima referidos junto de entidades com a qual é mantido qualquer tipo de relacionamento, nomeadamente clientes, parceiros, fornecedores, e entidades oficiais competentes.

Esta Política é aplicável de igual modo a todos os ativos geridos pelo NOSi uma vez que estes são partilhados, visando garantir um controlo adequado ao nível das infraestruturas de processamento da informação.

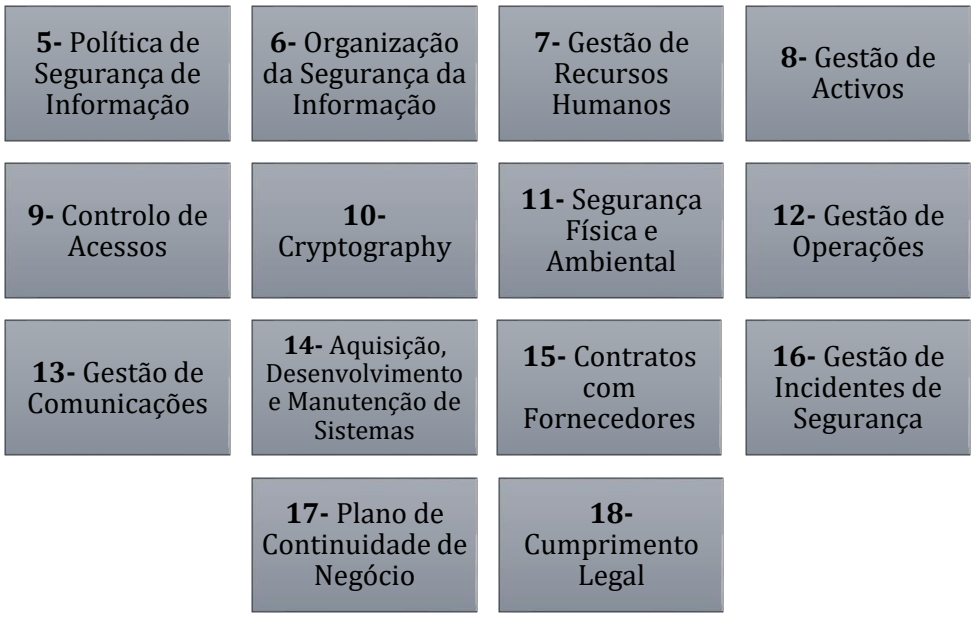
Estes requisitos devem "estar presentes" em todos os processos do ciclo de vida da Informação (criação, utilização, atualização, conservação, distribuição e destruição) e do respetivo sistema de suporte (processamento, armazenamento e transmissão), quer este seja manual ou automatizado.

A Segurança da Informação é obtida através da implementação de um conjunto de controlos que podem ser: políticas, normas, procedimentos, estruturas organizacionais e funções de software.



Estes controlos necessitam de ser estabelecidos para assegurar que os objetivos específicos de segurança de informação do NOSi sejam atingidos, sendo baseados no *standard* ISO 27002, composta pelos seguintes

domínios:



4. Âmbito da Política

Por Informação entende-se todo e qualquer dado independentemente da sua natureza, desde que relativos às atividades do NOSi, ou de terceiros com quem se relacione, que a organização coloque à disposição dos seus colaboradores e de entidades externas, ou que estes possam vir a ter conhecimento ou acesso no exercício das suas funções.

Esta Política e todas as normas e procedimentos que dela derivem abrangem a totalidade da Informação gerida, independentemente do seu suporte ou via de transmissão, devendo assegurar-se o seu conhecimento e divulgação por todos os colaboradores e entidades externas, que se obrigam ao seu cumprimento na totalidade.

5. Responsabilidades

5.1 Conselho de Administração

A aprovação desta política bem como outros princípios, políticas, regras e procedimentos de segurança de informação derivadas desta, é da inteira responsabilidade do Conselho de Administração.

Pensando na efetividade desta PSI, é fundamental o comprometimento por parte dos Órgãos Administrativos da instituição, como aqueles que têm o poder de representação, mas também de decisão e vinculação da instituição. Na prática este comprometimento se materializa no respeito rigoroso e na aplicação da PSI, em todos os atos da empresa. Havendo tal envolvimento por parte destes, influenciará no cumprimento e dedicação por parte dos colaboradores.

O conjunto de normas elaborados define, com maior detalhe, qual a estrutura organizacional que suporta a Segurança da Informação e quais as responsabilidades de cada interveniente dentro da estrutura, nomeadamente no que diz respeito à Segurança da Informação. No entanto, nos parágrafos seguintes, são apresentadas as responsabilidades essenciais de cada um desses intervenientes.

5.2 COLABORADORES

É imprescindível a responsabilidade de todos os colaboradores, técnicos e estagiários do NOSi, pelo que de nada adiantaria a imposição de controles e medidas técnicas de segurança da informação, se os funcionários com acesso à informação confidencial ou restrita, divulgá-las, intencionalmente ou não. Assim, deverá haver uma sintonia entre o comportamento ético-profissional dos colaboradores adequando-se as medidas e controles técnicos de segurança da informação. Pelo que é da responsabilidade dos colaboradores, nomeadamente:

a) Cumprir fielmente as Políticas, as Normas e os Procedimentos de Segurança da Informação do NOSi;

b) Proteger as informações contra o acesso, a divulgação, modificação ou destruição não autorizados pelo NOSi;

c) Garantir que os equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades às quais

foram aprovadas;

d) Comunicar prontamente ao superior hierárquico, qualquer violação a esta política, suas normas e procedimentos.

5.3 Comunicação da Política

As Políticas, normas, processos e procedimentos relativos à Segurança da Informação devem ser de conhecimento de todos os colaboradores, e estagiários, independentemente do seu vínculo contratual com o NOSi, e das entidades externas relevantes.

É da responsabilidade do NOSI divulgar esta política junto dos seus colaboradores garantindo a sua aceitação e compromisso de cumprimento por todos.

Uma vez divulgada a presente PSI e todos as outras políticas, normas, processos e diretivas a ela associadas para o conhecimento de todos os seus destinatários, esses não podem incumpri-las alegando o seu desconhecimento.

5.4 Estrutura Funcional

A estrutura funcional do NOSi responsável pela segurança da informação é a Direção de Segurança & Compliance (DSC), sendo uma das suas principais atribuições, é a de garantir a Segurança e Proteção da Informação gerida no NOSi e na Rede Tecnológica Privativa do Estado (RTPE), cuja gestão está a cargo do NOSI.

Neste sentido, é da responsabilidade da DSC garantir a atualização e a conformidade da PSI, tendo em conta as melhores práticas internacionais, as políticas, diretrizes e regulamentos internos e as leis nacionais em vigor.

5.5 Destinatários

De uma forma geral todos os destinatários desta PSI, ou seja, tanto os funcionários, colaboradores, e estagiários, como entidades externas com acesso à Informação, são responsáveis pela proteção da Informação que manipulam e devem conhecer e respeitar esta política, normas e procedimentos de Segurança de Informação que se encontram definidas e aprovadas para o NOSi.

É da responsabilidade de todos assegurar o nível de segurança fixado no sentido de proteger os interesses do NOSi e permitir o funcionamento adequado, seguro e eficaz, de todas as áreas de atividades.

A quebra destes compromissos por qualquer colaborador interno ou de entidades externas pode levar à aplicação de sanções disciplinares, administrativas, civis e penais ou outras, de acordo com as leis, e normas aplicáveis.

5.6 Normas de Segurança da Informação

A Política de Segurança de Informação é fixada nas presentes regras e noutros documentos específicos sobre a matéria que, em conjunto, constituem as “Normas de Segurança de Informação”. Estas são baseados nas melhores práticas de mercado e encontram-se alinhadas com as necessidades específicas do NOSI.

Estas normas serão dadas a conhecer aos respetivos destinatários conforme forem progressivamente criadas e implementadas.

6. Informações Pessoais

Quando tenha lugar o tratamento de dados pessoais no seio da instituição, será feito com total respeito às regras constitucionais e leis nacionais vigentes, em especial o Regime Jurídico de Proteção de Dados das Pessoas Singulares.

6.1 Informação Sensível (Especial)

O NOSi é ciente da proibição de tratamento de informação sensível (dados

especiais nos termos da Lei de Proteção de Dados), nomeadamente informação respeitante às convicções políticas, filosóficas ou ideológicas, origem racial, dados genéticos, opção ou filiação partidária e/ou sindical, saúde e vida sexual, a vida privada no geral.

No entanto, a Lei de Proteção de Dados das Pessoas Singulares, excetua essa regra em três (3) situações distintas. Sendo assim o NOSI é consciente que só poderá efetuar o tratamento de dados sensíveis, nestas situações específicas, nomeadamente:

a) Situações em que o próprio titular dos dados ou da informação dá o seu consentimento, permitindo tal tratamento;

b) Nas situações em que a própria lei permite explicitamente que tal pessoa ou entidade faça esse tratamento;

c) Quando o tratamento se destina a processamento de dados estatísticos;

d) E por último, mediante prévia autorização da Comissão Nacional de Proteção de Dados (CNPD).

7. Avaliação de Risco de Segurança da Informação

Os requisitos de segurança de informação são definidos através de uma avaliação precisa. A realização de uma análise de risco ajuda a determinar qual o nível de risco a que a informação está exposta e, consequentemente, efetuar uma priorização dos Riscos mais relevantes, permitindo identificar as ações de mitigação adequadas e os controlos apropriados.

8. Controlos de Segurança da Informação

Após a avaliação de Risco baseada em critérios de aceitação, tratamento e gestão do Risco e na regulamentação e legislação nacional aplicável, e posterior identificação das medidas mitigadoras devem ser selecionados e implementados

os controlos apropriados para garantir que o Risco é reduzido para um nível aceitável.

A seleção dos controlos depende de decisão da Direção de Segurança & Compliance do NOSi.

Os mecanismos de Segurança de Informação implementados devem ser alvo de revisões periódicas para garantir os níveis de Segurança esperados, com particular enfoque para a salvaguarda da continuidade do Negócio e processos críticos.

9. ENQUADRAMENTO LEGAL

O NOSI compromete-se a respeitar e cumprir as disposições legais e regulamentares nacionais, regionais e internacionais aplicáveis em matéria de Segurança da Informação e dos sistemas que os suportam.

O NOSI compromete-se ainda, no âmbito da definição de políticas, procedimentos e normas de segurança da informação a respeitar o Decreto-Lei nº13/2014 de 25 de Fevereiro, que cria o NOSi, EPE e o Estatuto da empresa que dele faz parte, e o Decreto-Lei nº19/2010 de 14 de Junho, que estabelece as políticas, normas e regras de segurança da informação para a gestão da Rede Tecnológica Privativa do Estado (RTPE).

Qualquer conflito e/ou violação detetada pelos colaboradores e outras pessoas supramencionadas, relativamente à aplicação e/ou cumprimento dos normativos legais aplicáveis em cada momento, deve ser imediatamente reportado ao NOSI.

10. EXCEÇÕES

Qualquer exceção aos princípios enunciados nesta política, ou aos seus procedimentos, quando permitidas, devem ser aprovadas pelo Conselho de Administração, devendo ser posteriormente comunicadas aos demais destinatários desta política.

11. ABREVIATURAS

Abreviaturas	
PSI	Políticas de Segurança da Informação
Framework	Conjunto de elementos e suas interligações constituindo a base de um sistema ou projeto.
ISO	International Standards Organization
IEC	International Electrotechnical Commission
NOSi, EPE	Núcleo Operacional para a Sociedade de Informação, Entidade Pública Empresarial
PDCA	Plan – Planear, Do – Executar, Check – Verificar, Act – Agir
RTPE	Rede Tecnológica Privativa do Estado

12. REFERÊNCIAS

Este documento foi criado com base nas melhores práticas e standards, nomeadamente:

- Norma ISO/IEC 27001, ponto 5.2 e 6.2;
- Norma ISO/IEC 27002, ponto 5.1.

Na sequência das linhas de orientação antes enumeradas foi estabelecido um conjunto de Normas específicas de Segurança de Informação associadas, de aplicação obrigatória e que visam garantir que os

mecanismos de controlo sobre o acesso, processamento e disponibilização da informação gerida pelo NOSi são os adequados face ao seu valor, sensibilidade e criticidade para os objetivos, e finalidades da empresa, como também para o seu negócio.

Essas normas são:

1. Política de Classificação de Informação;
2. Política de Acesso à Internet;
3. Política de Utilização de Correio Eletrónico;
4. Política de Gestão de Passwords;
5. Política de Segurança de rede;
6. Política de Gestão de Acessos;
7. Política de Secretária Limpa, Ecrã Limpo;
8. Politicas de gestão de controlo acesso à RTPE;
9. Politicas de gestão de mudanças e/ou alterações na infraestrutura;
10. Politica de Gestão de equipamentos disponibilizados aos colaboradores;
11. Política de Segurança Física;
12. Política de Resposta a Incidentes;
13. Politica de Continuidade de Negócio, entre outras devidamente definidas e aprovadas para o efeito.