FARMHOUSE CIÊNCIA & TECNOLOGIA
ISSN: 2959-3409
FARMHOUSE Ciência & Tecnologia
Revista Multidisciplinar do Instituto Superior Politécnico de Ciências e Tecnologia
Ano: 2025 Número: 6 Volume: 4

Análise e Implementação de Políticas de Segurança em Redes de Dados Sensíveis. Caso de Estudo: Instituto Superior Politécnico Internacional de Angola (ISIA)

Analysis and Implementation of Security Policies in Sensitive Data Networks. Case Study: Instituto Superior Politécnico Internacional de Angola (ISIA)

Análisis e Implementación de Políticas de Seguridad en Redes de Datos Sensibles. Caso de Estudio: Instituto Superior Politécnico Internacional de Angola (ISIA)

Autor: António João Fragoso Filipe

Universidade Gregório Semedo

E-mail: af211195@aluno.ugs.ed.ao

Orcid: https://orcid.org/0009-0007-8217-4395

Artigo original

RESUMO

O aumento da interconectividade digital e o avanço das tecnologias de informação impõem desafios significativos à protecção de dados em instituições educacionais. Este estudo visa propor a implementação de políticas de segurança da informação no Instituto Superior Politécnico Internacional de Angola (ISIA), uma instituição académica que enfrenta a necessidade de proteger informações críticas em sua infra-estrutura de rede. Através da análise de vulnerabilidades existentes, buscou-se desenvolver e recomendar medidas de segurança alinhadas às normas nacionais e internacionais, com o objectivo de mitigar riscos e fortalecer a protecção dos dados. Dada a relevância estratégica da segurança da informação no ambiente académico, o trabalho focou na análise das vulnerabilidades e na proposição de medidas de segurança baseadas nas normas ISO/IEC 27001 e ISO/IEC 27002.

Palavras-chave: Políticas de segurança; Redes de dados ISO 27001 e ISO/IEC 27002; Segurança da Informação.

SUMMARY

The increasing digital interconnectivity and advancement of information technologies pose significant challenges to data protection in educational institutions. This study aims to propose the implementation of information security policies at the Institute Polytechnic International de Angola (ISIA), an academic institution facing the need to protect critical information within its network infrastructure. By analyzing existing vulnerabilities, the research sought to develop and recommend security measures aligned with national and international standards, with the goal of mitigating risks and strengthening data protection. Given the strategic relevance of information security in the academic environment, the work focused on analyzing vulnerabilities and proposing security measures based on ISO/IEC 27001 and ISO/IEC 27002 standards.

Keywords: Information Security, Security Policies, Data Networks, ISO 27001 and ISO/IEC 27002.

RESUMEN

El aumento de la interconectividad digital y el avance de las tecnologías de la información plantean desafíos significativos para la protección de datos en instituciones educativas. Este estudio tiene como objetivo proponer la implementación de políticas de seguridad de la información en el Instituto Superior Politécnico Internacional de Angola (ISIA), una institución académica que enfrenta la necesidad de proteger información crítica en su infraestructura de red. Mediante el análisis de las vulnerabilidades existentes, se buscó desarrollar y recomendar medidas de seguridad alineadas con las normas nacionales e internacionales, con el fin de mitigar riesgos y fortalecer la protección de los datos. Dada la relevancia estratégica de la seguridad de la información en el entorno académico, el trabajo se centró en el análisis de las vulnerabilidades y en la propuesta de medidas de seguridad basadas en las normas ISO/IEC 27001 e ISO/IEC 27002.

Palabras-clave: Políticas de seguridad; Redes de dados, ISO 27001 e ISO/IEC 27002; Seguridad de la Información.

INTRODUÇÃO

A segurança da informação é um tema crítico na sociedade actual, especialmente no que se refere a dados sensíveis e confidenciais. Com o aumento exponencial do volume de dados

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

trocados em redes de computadores, a segurança tornou-se uma questão fundamental para organizações e indivíduos. Redes que gerem dados sensíveis, como informações financeiras, médicas e governamentais, estão sujeitas a ataques cibernéticos maliciosos que podem causar danos irreparáveis. A implementação de políticas de segurança adequadas é, portanto, uma medida essencial para garantir a integridade, confidencialidade e disponibilidade desses dados.

Segundo Tannenbaum e Van Steen (2017), as políticas de segurança em redes de dados sensíveis podem incluir medidas como autenticação de utilizadores, criptografia de dados, controlo de acesso à rede, *firewall*, monitoramento e detecção de intrusos. A implementação dessas políticas exige uma análise aprofundada da rede e dos dados a serem protegidos, a fim de aplicar medidas de segurança adequadas e eficazes. Além disso, é crucial que a equipa responsável pela implementação das políticas de segurança esteja actualizada e treinada para lidar com possíveis ameaças cibernéticas.

Este trabalho tem como objectivo analisar e propor políticas de segurança em redes de dados sensíveis no Instituto Superior Politécnico Internacional de Angola (ISIA), com a finalidade de garantir a protecção adequada dos dados e a prevenção de possíveis ataques cibernéticos.

Os procedimentos metodológicos utilizados abrangeram uma revisão bibliográfica detalhada, permitindo a análise de estudos e pesquisas sobre políticas de segurança em redes de dados sensíveis. A colecta de dados incluiu observação participante, revisão documental, aplicação de questionários e realização de entrevistas, a fim de obter informações sobre a infraestrutura de rede e os dados sensíveis do ISIA.

A análise da infraestrutura procurou identificar vulnerabilidades e necessidades específicas de segurança na rede da instituição. Com base nos resultados dessa análise, foram identificadas e selecionadas políticas de segurança adequadas, considerando a natureza dos dados e as regulamentações aplicáveis.

Por fim, o estudo foi concluído com a proposição e implementação das políticas de segurança definidas, garantindo a protecção efectiva dos activos da instituição.

2.1. Sistemas de Gestão de Segurança da Informação

Os Sistemas de Gestão de Segurança da Informação (SGSI) são estruturas organizacionais que englobam políticas, procedimentos, directrizes e recursos associados para gerir e proteger a informação, como ilustra a Figura 1.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

Figura 1

Estrutura do Sistema de Gestão de Segurança da Informação (SGSI).

Fonte: Adaptado de (Gino, 2023)

A implementação de um SGSI tem como objectivo assegurar a protecção contínua dos activos de informação de uma organização, alinhando a segurança da informação com os objectivos estratégicos da empresa. Este sistema, não necessariamente informatizado, baseia-se nas normas da família ISO/IEC 27000, que incluem toda a abordagem institucional utilizada para proteger a informação, de acordo com os seus princípios e atributos de confidencialidade, disponibilidade, integridade, responsabilidade, autenticidade e criticidade (Culot et al., 2021; SGSI, 2015).

De acordo com as normas técnicas mencionadas, o Sistema de Gestão de Segurança da Informação deve definir políticas, objectivos, processos e procedimentos específicos para a gestão da segurança da informação no seu âmbito. O SGSI engloba os seguintes processos organizacionais (SGSI, 2015):

- Classificação da Informação: organizar e classificar as informações de acordo com a sua confidencialidade e atribuir um proprietário responsável por cada informação.
- Gestão de Riscos de Segurança da Informação: reduzir ao mínimo os riscos associados à informação, implementar as medidas de segurança necessárias e realizar uma avaliação contínua através de análises sistemáticas e periódicas.
- Gestão de Resposta a Incidentes de Segurança da Informação: garantir a continuidade das operações, procurando minimizar a interrupção causada por desastres ou falhas, especialmente nos activos que suportam os processos críticos de informação da organização.
- Controlo de Acesso à Informação: gerir o acesso (lógico e físico) conforme as normas e procedimentos estabelecidos.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Consciencialização e Formação em Segurança da Informação: validar as directrizes da PSI/PJSC e definir a utilização responsável das informações.
- Gestão de Activos de Tecnologia da Informação e Comunicações: inventariar e gerir os activos críticos de tecnologia da informação e comunicação.

2.2. Princípios da Segurança da Informação

Os princípios da segurança da informação são os fundamentos que orientam a protecção dos dados dentro de uma organização. Estes princípios são essenciais para a criação de políticas e procedimentos de segurança eficazes e incluem (Reis et al., 2020):

- Confidencialidade: envolve a protecção de informações sensíveis contra acessos não autorizados. Técnicas como criptografia, controlo de acesso baseado em função (RBAC) e sistemas de gerenciamento de identidade e acesso (IAM) são usadas para garantir que apenas pessoas autorizadas possam aceder às informações (Flowerday & Tuyikeze, 2016).
- Integridade: refere-se à precisão e completude da informação. Mecanismos como *hashing*, assinaturas digitais e controlos de versão são utilizados para garantir que os dados não sejam alterados de maneira não autorizada ou acidental (Flowerday & Tuyikeze, 2016).
- Disponibilidade: assegura que a informação esteja acessível e utilizável quando necessário. Para garantir a disponibilidade, as organizações implementam medidas como *backup* regular, planeamento de continuidade de negócios e sistemas de recuperação de desastres (Flowerday & Tuyikeze, 2016).

Figura 2

Princípios da Segurança da Informação.

Fonte: Adaptado de (Renato Júnior, 2023)

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

2.3. Ameaças à Segurança e Vulnerabilidades

As ameaças à segurança e vulnerabilidades são desafios constantes no campo da segurança da informação. As ameaças podem ser externas ou internas, e as vulnerabilidades podem surgir de falhas no design, implementação ou configuração de sistemas (Ramesh Srinivasan, 2015).

Ameaças:

- *Malware*: Software malicioso, como vírus, *worms*, *trojans* e *ransomware*, que pode danificar ou comprometer sistemas e dados.
- *Phishing*: Técnicas de engenharia social usadas para enganar utilizadores e obter informações sensíveis, como credenciais de login.
- Ataques de Força Bruta: Tentativas de adivinhar senhas por meio da tentativa sistemática de todas as combinações possíveis.
- Ataques de Negação de Serviço (DoS): Tentativas de tornar um serviço indisponível, sobrecarregando o sistema com tráfego excessivo.
- Injecção de SQL: Ataques que exploram vulnerabilidades em aplicativos webs para executar comandos SQL maliciosos.

Vulnerabilidades:

- Software Desactualizado: Falhas de segurança em software que não foram corrigidas por meio de actualizações.
- Configuração Incorrecta: Configurações de segurança inadequadas ou padrão que podem ser exploradas por atacantes.
- Falta de Criptografia: Dados transmitidos ou armazenados sem criptografia são vulneráveis a intercepção e roubo.
- Autenticação Fraca: senhas fracas ou métodos de autenticação ineficazes que podem ser facilmente comprometidos.
- Falhas de Programação: Erros no código do software que podem ser explorados para executar comandos não autorizados ou aceder a dados sensíveis.

A gestão eficaz de ameaças e vulnerabilidades envolve a implementação de uma série de práticas e tecnologias, tais como (Mark S. Merkow, 2012):

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Análise de Vulnerabilidades: Identificação e avaliação contínua de vulnerabilidades em sistemas e redes.
- Gerenciamento de *Patches*: Aplicação regular de *patches* de segurança para corrigir vulnerabilidades conhecidas.
- Monitoramento e Detecção: Implementação de sistemas de monitoramento e detecção de intrusos (IDS/IPS) para identificar actividades suspeitas e responder rapidamente a incidentes.
- Educação e Treinamento**:** Capacitação contínua dos funcionários para reconhecer ameaças como *phishing* e adoptar práticas de segurança adequadas.

2.5. Normas de Segurança da Informação ISO

As normas de segurança da informação ISO são padrões internacionais que fornecem directrizes e boas práticas para a gestão da segurança da informação. As normas mais relevantes incluem (ISO, 2022):

2.5.1. ISO/IEC 27001

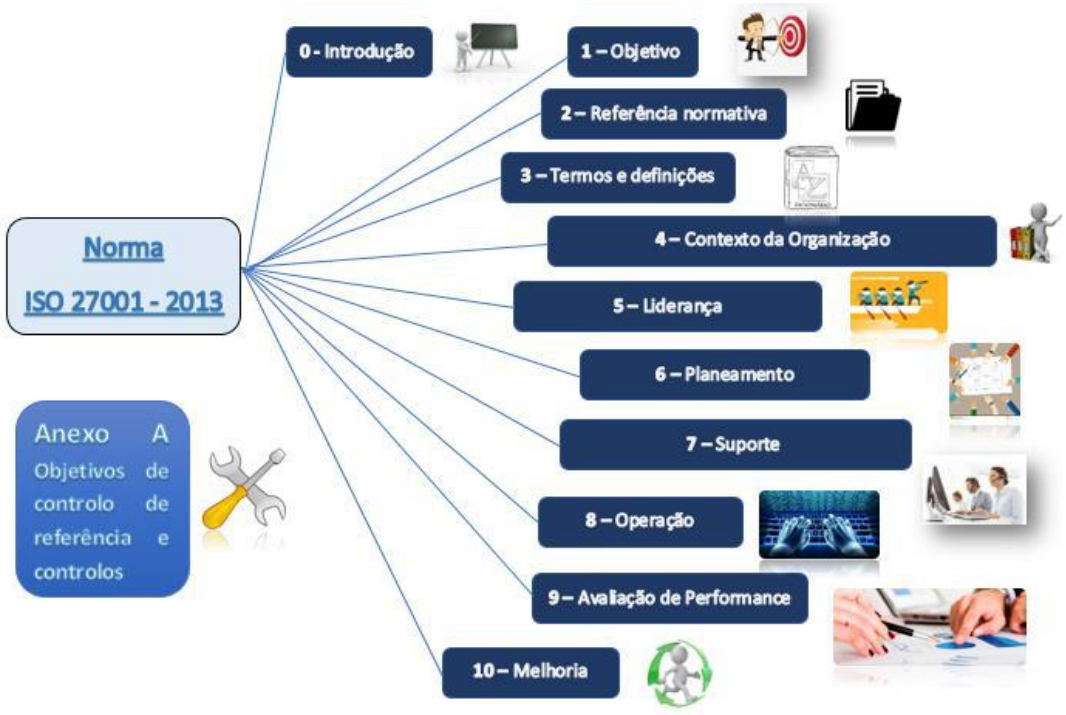
A ISO/IEC 27001 é a norma internacional que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI**)**, utilizando o ciclo PDCA (*Planear, Implementar, Monitorizar e Ajustar*) para a implementação de controlos de segurança. A norma exige que as organizações realizem uma avaliação contínua dos riscos e implementem controlos adequados para mitigá-los (ISO, 2022).

A estrutura da versão mais recente da norma ISO/IEC 27001 – 2013 é apresentada na Figura 3.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

Figura 3

Estrutura geral da norma ISO/IEC 27001.



Fonte: Adaptado de (F. Palma, 2024)

A extensão da ISO/IEC 27001 e 27002 inclui requisitos e orientações específicas para a gestão da privacidade da informação. Este padrão é particularmente relevante para organizações que precisam estar em conformidade com regulamentos de privacidade de dados, como o GDPR (*General Data Protection Regulation*) (Fenz et al., 2016; ISO, 2022).

Benefícios da Conformidade com Normas ISO:

- Melhoria da Segurança: Implementação de controlos robustos e boas práticas que aprimoram a segurança global da informação.
- Conformidade regulamentar: ajuda as organizações a cumprir leis e regulamentos de protecção de dados.
- Confiança dos *Stakeholders*: A certificação ISO/IEC 27001 pode aumentar a confiança de clientes e parceiros de negócios na capacidade da organização de proteger dados sensíveis.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Melhoria Contínua: O ciclo PDCA promove a melhoria contínua dos processos de segurança da informação.

Figura 4

Benefícios da Norma ISO 27001.

Fonte: (Anderson, 2023)

2.6. Importância da Política de Segurança da Informação

A política de segurança da informação é fundamental para garantir a protecção adequada dos activos informacionais de uma organização. Esta política estabelece directrizes claras e procedimentos específicos para mitigar riscos de segurança, proteger dados sensíveis e assegurar a continuidade operacional. Ao adoptar uma abordagem profissional na sua implementação, a política de segurança promove a conformidade com regulamentos e normas vigentes, como o Regulamento Geral sobre a Protecção de Dados (RGPD), mitigando potenciais impactos legais e financeiros associados a violações de segurança. Além disso, a aplicação de práticas baseadas em evidências científicas permite uma gestão mais eficaz dos recursos de segurança, promovendo a consciencialização e o treinamento contínuo dos colaboradores. Em suma, uma política de segurança da informação não apenas protege a organização contra ameaças externas e internas, mas também fortalece a confiança dos clientes

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

e *stakeholders*, contribuindo para a sustentabilidade e crescimento da empresa (Jureńczyk, 2023).

2.7. Situação Actual do ISIA

A estrutura organizacional do ISIA, com as suas diferentes áreas de actuação (académica, administrativa, financeira, técnica e social), resulta numa vasta diversidade e um grande volume de informação em circulação, predominantemente em formato digital. A rede do ISIA está distribuída por três edifícios geograficamente separados, o que cria um cenário complexo para sistemas de comunicação e segurança da informação entre eles.

Para compreender melhor a segurança da rede do ISIA, foram realizadas entrevistas estruturadas e semiestruturadas com os responsáveis pela gestão da rede, além da consulta de documentos institucionais. Esse processo permitiu identificar rapidamente os principais desafios e problemas críticos de segurança da rede do ISIA.

As questões elaboradas para as entrevistas foram baseadas em referências bibliográficas relevantes e inquéritos. A recolha de informação da rede do ISIA, após a obtenção das respostas, foi agrupada com foco especial nos seguintes contextos:

- Segurança Organizacional: abordaram-se aspectos relacionados à política de segurança e às funções e responsabilidades sobre os activos da organização.
- Segurança Física e Ambiental: avaliaram-se as condições de segurança física das instalações da instituição, bem como das áreas onde estão localizados os equipamentos de rede e onde ocorre o tratamento e armazenamento das informações.
- Segurança de Equipamentos e Serviços: identificaram-se e avaliaram-se todos os equipamentos existentes, incluindo servidores, máquinas e dispositivos, considerando quem os utiliza e as medidas de segurança aplicadas. Os serviços também foram analisados quanto à sua segurança.
- Segurança da Rede de Dados: A análise focou na segurança das comunicações dentro da rede, garantindo a protecção contra acessos não autorizados e ataques cibernéticos.
- Segurança Aplicacional: levantaram-se informações sobre todos os programas e aplicações desenvolvidos e/ou utilizados, incluindo como é feito o armazenamento e registos de informações, monitoramento e análise das mesmas.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Segurança de Recursos Humanos: analisaram-se as funções e responsabilidades dos colaboradores em relação à segurança, desde o início até o término do contracto, incluindo a formação técnica oferecida.
- Conformidade: avaliou-se o cumprimento dos requisitos legais e contratuais, incluindo o Regulamento Geral de Protecção de Dados (RGPD) e outras leis relacionadas à protecção de dados pessoais, conforme as regulamentações vigentes.

  Essa abordagem estruturada permitiu uma análise abrangente da segurança da rede do ISIA, identificando áreas críticas que exigem melhorias e fornecendo uma base sólida para o desenvolvimento e implementação de políticas de segurança mais eficazes e adaptadas às necessidades específicas da instituição.

2.7.1. Lista dos Problemas Relevantes do ISIA

Nesta secção, são listados os problemas do ISIA que foram identificados para serem tratados e mitigados:

- Falta de um documento formal de política de segurança.
- Desconhecimento do estado actual da segurança da informação devido à falta de formação entre utilizadores, investigadores, técnicos, funcionários, docentes e não docentes, etc.
- Ausência de auditorias regulares para verificar o estado da segurança da informação na rede e em toda a instituição, apesar da realização de auditorias específicas em curso.
- Falta de um documento que atribua responsabilidades e funções claras.
- Presença de máquinas com Windows 7 (um sistema operativo desactualizado), pelo menos entre os docentes, com pastas partilhadas, representando um potencial risco se um computador infectado se ligar à rede interna.
- Falta de um processo de revogação para ex-alunos, mantendo-os como "utilizadores activos".
- Implementação insuficiente de medidas de segurança física nas salas que contêm material sensível.
- Ausência de registos de acesso às salas com material sensível, onde o acesso é feito por chaves tradicionais, sem controlo de entrada e saída.
- Utilização de chaves mestras para acesso às salas com material sensível.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Algumas salas com equipamento sensível são utilizadas como arrumos, afectando a qualidade do ambiente.
- Falta de suporte técnico ou política para ajudar estudantes ou professores a cifrar os seus dados ou proteger informações mais confidenciais.

2.8. Proposta do Documento de Políticas de Segurança

Nesta secção, são apresentadas as políticas propostas para mitigar os riscos identificados através da análise e avaliação dos problemas e desafios da rede do ISIA.

1. Política de Segurança da Informação

Documento de Política de Segurança - ISIA

Data	Versão	Autor	Comentários	Status
18/02/2025	1.0	António João Fragoso Filipe	Elaboração do Documento	Por se aprovar.

Glossário

- **PSI:** Política de Segurança da Informação
- **ISO:** *International Organization for Standardization*
- **IEC:** *International Electrotechnic Commission*
- **ISIA:** Instituto Superior Politécnico Internacional de Angola

Índice

1. Introdução
2. Âmbito
3. Objectivos
4. Princípios
5. Referências Normativas
6. Termos e Definições
7. Revisão da Política

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

8. Directrizes Gerais
9. Responsabilidades
10. Violação e Penalidades
11. Vigência
12. Referências

1. Introdução

Actualmente, a informação, os processos e os sistemas relacionados, bem como as redes e as pessoas envolvidas no seu manuseamento, são essenciais para o funcionamento de empresas, instituições e organizações. Tal como outros activos, necessitam de protecção contra diversos riscos aos quais podem estar expostos. No ISIA, observa-se uma crescente dependência dos sistemas de informação e infra-estruturas de comunicação para o normal funcionamento da instituição, tornando as ameaças informáticas uma preocupação regular.

Tanto a informação quanto os demais activos do ISIA estão sujeitos a ameaças deliberadas e acidentais. Os processos, sistemas, redes e pessoas envolvidas possuem vulnerabilidades, o que implica que os riscos à segurança da informação sejam uma constante. A implementação de uma política de segurança da informação visa minimizar esses riscos, protegendo o ISIA contra ameaças e vulnerabilidades, e reduzindo o impacto sobre seus activos.

Assim, a segurança da informação pode ser assegurada através da aplicação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos, estruturas organizacionais, *software* e *hardware*. Estes controlos devem ser estabelecidos, implementados, monitorizados, revistos e aprimorados conforme necessário, garantindo que os objectivos específicos de segurança e de negócios da instituição sejam alcançados.

Para mitigar a probabilidade de ameaças afectarem a confidencialidade, integridade e disponibilidade dos activos de informação, como, por exemplo, fraudes, vandalismo e sabotagem, o ISIA dedica-se à segurança da informação. Dessa forma, através de esforços contínuos e bem geridos, foram estabelecidos os fundamentos para proteger os activos de informação, reduzindo riscos, custos e cumprindo requisitos legais, ao mesmo tempo que preserva a imagem e reputação do ISIA.

2. Âmbito

Esta PSI é aplicável a toda a instituição, ou seja, a todos os que directa ou indirectamente possuam acesso ao ISIA.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

3. Objectivos

O principal objectivo desta política de segurança é a definição dos princípios e regras básicas de gestão de segurança da informação no ISIA. Além disso, visa:

- Contribuir com iniciativas relativas à segurança da informação;
- Auxiliar na salvaguarda dos activos do ISIA – pessoas, propriedade, finanças e reputação;
- Prestar assistência e melhorar a qualidade da tomada de decisões no ISIA;
- Atender aos requisitos legais e/ou estatutários.

4. Princípios

A segurança da informação deve ser entendida como uma responsabilidade colectiva. Assim sendo, o conjunto de regras desta PSI guiar-se-á pelos seguintes princípios:

a) Confidencialidade: Garantia de que a informação não esteja disponível ou seja revelada a pessoas, sistemas, órgãos ou entidades não autorizadas pelo ISIA.

b) Integridade: Garantia de que a informação não foi modificada ou destruída de forma não autorizada ou acidental, quer na origem, no transporte e/ou no seu destino.

c) Disponibilidade: Garantia de que a informação esteja acessível a pessoas, sistemas, órgãos ou entidades autorizadas pelo ISIA, sempre que for necessário.

d) Autenticidade: Garantia de que a informação é construída por pessoas, sistemas, órgãos ou entidades com permissão para tal.

e) Não repúdio: Garantia de que o emissor da informação não negue posteriormente a autoria da mesma.

f) Conhecimento: Garantia de que todos os funcionários, colaboradores, docentes, não docentes e entidades prestadoras de serviço tenham formação e competências que permitam a execução das suas funções, e também formação em segurança da informação.

g) Responsabilidade: Todos os indivíduos, sem excepção, que participam de alguma forma na produção, manuseamento, transporte e destruição da informação, devem ser responsáveis pela mesma.

h**)** Privacidade: Garantia ao direito colectivo e pessoal à intimidade e ao sigilo da correspondência e comunicações individuais.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

5. Referências Normativas

A presente Política de Segurança da Informação (PSI) baseia-se nas recomendações da norma ISO/IEC 27001:2013 e da norma ISO/IEC 27002:2013, amplamente reconhecidas internacionalmente como a norma para sistemas de gestão de segurança da informação e como o código de práticas para a gestão da segurança da informação, respectivamente. Esta política também está em conformidade com o Regulamento Geral de Protecção de Dados (RGPD) e outras leis aplicáveis.

2. Política – Organização de Segurança de Informação

Resumo

Para garantir uma gestão eficaz da segurança da informação, é essencial estabelecer uma estrutura responsável pela orientação, planeamento, implementação, manutenção e melhoria das práticas de segurança da informação. Esta estrutura deve garantir que os processos operacionais protejam a confidencialidade, integridade e disponibilidade da informação, facilitando decisões rápidas sobre riscos e investimentos em conformidade com requisitos externos (legais, regulamentares ou contratuais) e processos internos da instituição. A política define os responsáveis e as suas funções para manter a segurança da informação na instituição, incluindo o contacto com autoridades e cuidados com dispositivos móveis no local de trabalho.

Objectivo

Fornecer um modelo de gestão de referência para iniciar e controlar a implementação e operação da segurança da informação dentro da instituição. Assegurar a segurança no uso de dispositivos móveis.

Âmbito

Esta política aplica-se a todos os funcionários, docentes, não docentes, estagiários e outros intervenientes do ISIA.

Termos e Definições

Os termos e definições fornecidos na política de segurança da informação são aplicáveis para os propósitos deste documento.

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

Política

I. Para o cumprimento eficaz das regras estabelecidas por esta política, são instituídas as seguintes competências e responsabilidades nesta instituição, conforme o organograma a seguir:

A **Gestão de Topo do ISIA** tem a responsabilidade máxima de promover, controlar e monitorizar a segurança da informação do ISIA, nomeadamente através de:

- Liderança e compromisso com o sistema de gestão de segurança da informação;
- Aprovação da política de segurança da informação;
- Identificação e nomeação de responsáveis para as funções relevantes para a segurança da informação, assegurando a conformidade da mesma e o registo do desempenho do sistema de gestão de segurança da informação.

O **Gestor de Segurança da Informação do ISIA** é responsável por:

- Alinhar os objectivos de Segurança da Informação com os objectivos estratégicos do Departamento de Informática, definindo e mantendo actualizadas as políticas de segurança da informação, apoiando e monitorizando a implementação e melhoria contínua dos procedimentos internos de suporte;
- Desenvolver, implementar e melhorar a segurança da informação na instituição.

O **Gestor da Área Organizacional do ISIA** deve ser responsável por:

- Promover, no âmbito das suas competências e valências próprias, o cumprimento das políticas, processos e procedimentos, identificando proactivamente as ameaças e vulnerabilidades que coloquem em risco a segurança da informação do ISIA.

O **Gestor dos Activos do ISIA** é responsável por:

- Garantir que os activos sejam classificados e que sejam definidos e implementados controlos adequados para protegê-los, assegurando a confidencialidade, integridade e disponibilidade dos activos de informação que suportam.

O **Gestor de Riscos do ISIA** é responsável por:

- Garantir a aplicação de medidas adequadas (técnicas, materiais, organizativas e procedimentais) que permitam atenuar, eliminar ou transferir os riscos associados aos activos de informação, reduzindo a probabilidade de uma ameaça específica explorar as vulnerabilidades que comprometam um activo;

ISSN: 2959-3409
Ano: 2025 Número: 6 Volume: 4

- Avaliar o impacto das medidas implementadas e, consequentemente, reavaliar periodicamente a necessidade de implementar medidas complementares.

  É recomendado à **Gestão de Topo da instituição** definir outras responsabilidades e papéis adicionais, de acordo com o modelo institucional e requisitos de conformidade a que seja obrigada. É recomendado à Gestão de Topo da instituição a definição de responsáveis para estabelecer contactos com grupos de interesse especial, associações profissionais ou outros fóruns especializados em segurança da informação.

II. A **Gestão de Topo da instituição** deve designar os responsáveis para estabelecer contactos com autoridades (por exemplo, entidades reguladoras, entidades policiais, autoridades de fiscalização, etc.). Esses responsáveis devem:

a) Manter contactos adequados com as autoridades civis para garantir uma resposta atempada face a incidentes de grandes dimensões; b) Manter uma lista actualizada dos contactos das autoridades relevantes a serem contactadas em caso de necessidade, no âmbito de planos de emergência, incluindo protecção civil, polícia, bombeiros e segurança das instalações físicas.

III. É assegurada a segurança no uso de dispositivos móveis no local de trabalho do ISIA (Política de Dispositivos Móveis).

IV. É garantido que todos os materiais confidenciais sejam removidos do espaço de trabalho (Política de Mesa Limpa e Ecrã Limpo).

Conformidade

Medição de Conformidade

A equipa do departamento de informática verificará a conformidade com esta política através de vários métodos, incluindo acompanhamento periódico e auditorias internas e externas.

Excepções

Qualquer excepção a esta política deve ser aprovada antecipadamente pela equipa do departamento de informática.

Não Conformidade

Qualquer docente, não docente, funcionário ou colaborador que viole esta política pode estar sujeito a medidas disciplinares, incluindo rescisão de contracto de trabalho.

CONCLUSÕES

A presente pesquisa abordou a análise e proposta de políticas de segurança em redes de dados sensíveis no Instituto Superior Politécnico Internacional de Angola (ISIA), uma instituição académica que enfrenta desafios significativos na protecção de informações num ambiente digital cada vez mais interconectado. Considerando a importância estratégica da segurança da informação para instituições educacionais como o ISIA, este estudo teve como objectivo analisar e propor políticas de segurança na infra-estrutura de rede. A pesquisa evidenciou a importância da consciencialização contínua e do treinamento dos colaboradores, factores essenciais para promover uma cultura de segurança cibernética. O investimento em educação sobre melhores práticas não apenas aumentou a vigilância contra ameaças internas e externas, mas também reforçou a resiliência da infra-estrutura tecnológica da instituição.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, R., & Mendes de Castro, J. (2020). Análise Comportamental das Políticas de Segurança da Informação – Um Estudo de Caso. *Desafio online*, *9*(1). https://doi.org/10.55028/don.v9i1.9926

Anderson. (2023). *O que é Segurança da Informação?* Blogson. https://www.blogson.com.br/o-que-e-seguranca-da-informacao/

Andersson, F., & Karlsson, F. (2022). Standardizing information security – a structurational analysis. *Information and Management*, *59*(3). https://doi.org/10.1016/j.im.2022.103623

Borges, L. (2016). *Gestão da Segurança da Informação*. ISO. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

Culot, G., & Sartor, M. (2021). The ISO/IEC 27001 Information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7). https://doi.org/10.1108/TQM-09-2020-0202

F. Palma. (2024). *Portal GSTI - ISO 27001 em 5 minutos | O que é a ISO 27001* [Vídeo]. YouTube. https://www.youtube.com/watch?v=68cphWTnsmw

Fenz, S., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. *Information and Computer Security*, *24*(5). https://doi.org/10.1108/ICS-07-2015-0030

Flowerday, V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*. https://doi.org/10.1016/j.cose.2016.06.002

Gino, M. (2023). *Sistema de Gestão de Segurança da Informação*. Studocu. https://www.studocu.com/pt-br/document/universidade-de-sorocaba/linguagem-e-tecnologia/sistema-de-gestao-de-seguranca-da-informacao/79684996

ISO. (2018). *Information technology—Security techniques—Information security management systems—Overview and vocabulary* (ISO/IEC 27000:2018(E)). www.iso.org

ISO. (2022). *ISO/IEC 27001 and related standards: Information security management*. ISO.

Jureńczyk, Ł. (2023). Changing the Importance of Poland in the Security Policy of the United States in the Context of the war in Ukraine. *Przegląd Politologiczny*, *1*. https://doi.org/10.14746/pp.2022.28.1.4

Merkow, M. S. (2012). *Information Security: An Approach for Executive Managers* (2nd ed.).

Merkow, M. M. (2018). *Information Security: Principles and Practices* (3rd ed.). Pearson Education.

Paananen, H., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*. https://doi.org/10.1016/j.cose.2019.101608

Reis, J., & Pablo P. (2020). *Classificação da Informação*.

Renato. (2023). *Protiviti - Pilares da Segurança da Informação*. Protiviti. https://www.protiviti.com.br/cybersecurity/pilares-seguranca-da-informacao/

Toro, R. (2015, 28 de julho). *¿Qué es SGSI?* PMG-SSI. https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Tannenbaum, A. S., & Van Steen, M. (2017). *Distributed Systems: Principles and Paradigms* (2nd ed.). Pearson.