ALBA
ISFIC RESEARCH AND SCIENCE JOURNAL

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

20 - 02 | 2025

# MELHORIA DE POLÍTICAS DE SEGURANÇA INFORMÁTICA NO INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E CRIMINAIS

## Improving security policies at the higher institute of police and criminal sciences

## Mejora de las políticas de seguridad informática en el instituto superior de ciencias policiales y penales

**Pedro João[1] | António Gabriel Mateus[2] | Amoreno Sebastião Calengo[3]**

[1]Licenciado em Engenharia Informática, Mestre em Engenharia Informática com a especialidade de Gestão de Redes de Computadores e Sistema de Comunicação. Docente do Instituto Superior Politécnico de Ndalatando em Angola. ORCID: https://orcid.org/0000-0003-4103-5237, E-mail: petjohnews19@gmail.com.
[2]Licenciado em Engenharia na especialidade de Redes. Docente do Instituto Superior Politécnico de Ndalatando em Angola. https://orcid.org/0009-0006-8278-9317, E-mail: antonio.gabrielmateus001@gmail.com.
3Licenciado em Informática de Gestão. Docente do Instituto Superior Politécnico de Ndalatando em Angola. ORCID: https://orcid.org/0009-0009-7502-3024, E-mail: amorenoamor16@gmail.com.

Autor para correspondência: petjohnews19@gmail.com

*Data de recepção: 03-09-2025*
*Data de aceitação: 05-11-2025*
*Data da Publicação: 24-11-2025*

**Como citar este artigo:** João, P.; Mateus, A. G. e Calengo, A. S. (2025). *Melhoria de políticas de segurança informática no Instituto Superior de Ciências Policiais e Criminais.* ALBA – ISFIC Research and Science Journal, 1(9), pp. 276-206. https://alba.ac.mz/index.php/alba/issue/view/12.

**RESUMO**

A informação tornou-se o activo mais valioso das organizações, sendo, um alvo potencial para ameaças que se pretende explorar suas vulnerabilidades e causar danos consideráveis. Assim sendo, existe a necessidade de melhorar a política de segurança informática na tentativa de reduzir as chances de fraude. Logo, é importante deparar os factores analistas de sucesso para a melhoria de uma política de segurança, bem como avaliar o nível de relevância de qualquer um deles. O melhoramento das boas práticas dentro da instituição advém de uma superior confiabilidade no que toca ao uso dos dados e, naturalmente, o incremento da credibilidade da própria instituição. O estudo apeteceu saber o impacto na incorporação das tecnologias relacionadas a segurança informática no processo de protecção, e as políticas de implementação no progresso do Instituto Superior de Ciências Policiais e Criminais em Angola. Os dados aferidos mostraram que as instituições de ensino enfrentem em meios tecnológicos e capacitem seus efectivos, na utilização das novas tecnologias. Optou-se pela concretização de um caso de estudo nesta instituição. Para recolha dos dados, foi utilizado um questionário, para os efectivos ter a chance de avaliar sobre a benfeitoria de políticas de segurança informática. O resultado que se alcançou foi analisar os riscos existentes na instituição, que foi de acordo ao propósito pelo qual se conseguiu ter em conhecimento a respeito dos tais riscos. O objectivo foi elaborar as políticas de segurança

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

informática, para o impedimento na violação que circulava na instituição.
**Palavras-chave**: Melhoria; Políticas; Segurança Informática; Redes.

**ABSTRACT**

Information has become the most valuable asset of organizations, being a potential target for threats that intend to exploit its vulnerabilities and cause considerable damage. Therefore, there is a need to improve IT security policy in an attempt to reduce the chances of fraud. Therefore, it is important to identify the success factors for improving a security policy, as well as to assess the level of relevance of any of them. The improvement of good practices within the institution comes from greater reliability in the use of data and, naturally, the increase in the credibility of the institution itself. The study aimed to know the impact of the incorporation of technologies related to computer security in the protection process, and the implementation policies on the progress of the Higher Institute of Police and Criminal Sciences in Angola. The data collected showed that educational institutions are facing technological means and training their staff in the use of new technologies. It was decided to carry out a case study in this institution. To collect data, a questionnaire was used, so that employees had the chance to evaluate the benefits of computer security policies. The result achieved was to analyze the risks existing in the institution, which was in accordance with the purpose for which it was possible to gain knowledge about such risks. The objective was to develop IT security policies to prevent violations that were circulating within the institution.
**Keywords**: Improvement; Policies; IT Security; Networks.

**RESUMEN**

La información se ha convertido en el activo más valioso de las organizaciones, siendo un blanco potencial para amenazas que pretenden explotar sus vulnerabilidades y causar daños considerables. Por lo tanto, es necesario mejorar la política de seguridad informática en un intento de reducir las posibilidades de fraude. Por tanto, es importante identificar los factores de éxito para mejorar una política de seguridad, así como evaluar el nivel de relevancia de cualquiera de ellos. La mejora de las buenas prácticas dentro de la institución pasa por una mayor confiabilidad en el uso de los datos y, naturalmente, por el aumento de la credibilidad de la propia institución. El estudio tuvo como objetivo conocer el impacto de la incorporación de tecnologías relacionadas con la seguridad informática en el proceso de protección, y las políticas de implementación en el progreso del Instituto Superior de Ciencias Policiales y Penales de Angola. Los datos recabados evidenciaron que las instituciones educativas se encuentran a la vanguardia de los medios tecnológicos y capacitando a su personal en el uso de las nuevas tecnologías. Se decidió realizar un estudio de caso en esta institución. Para recolectar datos se utilizó un cuestionario, para que los empleados tuvieran la oportunidad de evaluar los beneficios de las políticas de seguridad informática. El resultado obtenido fue analizar los riesgos existentes en la institución, lo cual estuvo acorde con el propósito por el cual fue posible obtener conocimiento sobre dichos riesgos. El objetivo fue desarrollar políticas de seguridad informática para prevenir las violaciones que circulaban al interior de la institución.
**Palabras clave**: Mejora; Políticas; Seguridad informática; Redes.

## INTRODUÇÃO

Há toda necessidade em melhorar as políticas de segurança informática no Instituto Superior de Ciências Policiais e Criminais (ISCPC). Existe uma grande fragilidade no que concerne à segurança informática, no âmbito tecnológico, dentro do aparato informático da referida instituição.

Sequesseque (2017) afirma que "a comunicação deve ser conservada em segurança, assim como o envolvente e os equipamentos usados para o seu processamento. As instituições sabem da necessidade de se executar Segurança Informática com urgência" (p.22).

Como problema científico: que tipo de política de segurança informática a ser melhorada na rede do ISCPC? E a situação problemática que leva a aplicar as medidas e melhoria de políticas de segurança no ISCPC está ligada ao levantamento feito no campo de investigação daquela Unidade Policial, depois de serem identificadas as seguintes irregularidades: falta de senhas seguras para todos os usuários e equipamentos; falta de controlo e protecção no acesso à *Internet*; falta de antivírus em alguns computadores de serviço; falta de cópia de *backup* dos dados importantes nos demais terminais de trabalho; não há permissões de acesso nos arquivos partilhados; não há defesa sobre a engenharia social; vazamento de informações sigilosas; não existe gerenciamento das credencias de acesso; não há controlo de acesso às redes sociais e *sites*, etc.

Este artigo tem como objectivo geral, melhorar a política de segurança informática no ISCPC, e, para o cumprimento deste objectivo, pretendemos, determinar as possíveis fragilidades sobre a protecção da informação dentro do ISCPC; identificar as principais vulnerabilidades no que toca ao perigo que a instituição atravessa e os métodos utilizados na redução de invasões constantes nos dados para a protecção da informação; explicar outras medidas preventivas e necessárias para a segurança informática no ISCPC; estabelecer uma melhoria de políticas de segurança informática no ISCPC para garantia de um bom desempenho e a eficácia no tratamento da informação digital, sobre tudo no que tange a confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade da informação.

As políticas de segurança auxiliam a organização a alcançar seus objectivos estratégicos através da implementação de controlo de segurança informática, baseando-se em seu contexto, estimulando uma diminuição dos riscos provenientes de ameaças e vulnerabilidades através de uma segurança informática eficiente e eficaz (Vasconcelos, 2017).

De acordo com a norma (ISO/IEC 27002, 2022) "a segurança informática é conseguida pela implementação de um conjunto apropriado de verificação, cercando políticas, processos, procedimentos, construção organizacional e serviços de *software* e *hardware*".

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

Para o Miano (2016), a segurança informática, pode ser gerido por processo:

> A inexistência de um processo de formação e manutenção de cultura em segurança informática enfraquece a cadeia de valores para a obtenção do nível adequado de protecção. Agindo deste modo, não há proatividade para que se estabeleça a segurança. Os gestores que não implementarem esse processo serão relapsos em suas obrigações profissionais (p.112).

Actualmente, o mundo permanece cada vez mais aflito com a protecção dos dados pela via das plataformas digitais ou novas tecnologias, com ajuda da dependência da *Internet*, por esta razão, há vulnerabilidades nos sistemas computacionais contidos de forma permanente nas instituições no geral. Os efectivos, no verdadeiro sentido, precisam de aplicabilidade e usabilidade das normas internacionais no que concerne à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio (CIDAN) dos dados da instituição.

### 1.1. Política de segurança informática

Hoje em dia, é compreensível que a Segurança da Informação das instituições seja emblema estratégica primordial na grande maioria dos casos, suportados pela informática. E sempre teve um impacto no acompanhamento das informações no nosso quotidiano. De acordo com o Monteiro (2017) "a política de segurança é observada por muitos criadores como sendo um documento dirigido e normativo de atitude sob ponto de vista do socorro da informação de possíveis invasores" (p.8).

Corroboram (Rios, Filho & Rios, 2017), "a política e uma regra universal, dentro de uma organização, que define as acções e limites para obter os objectivos e metas institucionais" (p.51).

A política de segurança da informação é um conjunto de regulamentos que definem como os activos de tecnologia da instituição devem ser protegidos, fazendo com que os utilizadores tenham acesso apenas ao que for essencial, explicitando o que é permitido fazer ou não (Oliveira et al., 2019).

Para o Quissanga e Fernandes (2020), neste âmbito, refere:

> A segurança da informação tem estado um cuidado em todo mundo, a informação tornou-se muito essencial, e o seu manejo pede muitos cuidados, sendo necessário criar condições para proteger. Desta configuração, é impossível dizer que estamos completamente seguros, mesmo quando se trata da segurança de países do primeiro mundo. (p.88).

Para concretizar os princípios primários da segurança da informação, de concordância com a (ISO/IEC 27002, 2022), é necessário que haja:

**Confidencialidade**: propriedade que delimita o acesso à informação tão unicamente às entidades legais, ou seja, àquelas permitidas pelo dono da informação. De acordo Manoel (2014), ratifica essa mesma ideia, quando escreve: "toda informação deve ser guardada de acordo com a categoria de sigilo" (p. 3).

**Integridade**: característica que garante que a informação pervertida mantenha todos os distintivos originais estabelecidos pelo dono da informação, incluindo verificação de mudanças e fiança do seu ciclo de vida (presente, intermediária e estável). Segundo o Manoel (2014) "Integridade: atributo da informação de manter-se na mesma situação em que ficou disponibilizada pelo seu dono" (p.3).

**Disponibilidade**: qualidade que garante que a informação permaneça sempre disponível para o uso legal, ou seja, por aqueles utilizadores autorizados pelo dono da informação. Como afirma o Manoel (2014), "disponibilidade é a qualidade de tornar livre para utilizadores, sempre que indispensável e para qualquer aplicação, a informação gerada ou alienada por um indivíduo ou estrutura" (p.3). A disponibilidade é a garantia para que os utilizadores autorizados consigam acesso à informação e aos activos similares sempre que necessário.

**Autenticidade**: qualidade que garante que a comunicação é originária da fonte comunicada e que não ficou alvo de transtornos ao longo de um procedimento.

**Não-repúdio/Irretratabilidade ou ainda Irrefutabilidade**: qualidade que garante a impossibilidade de contraditar a autoria em conexão a uma transacção previamente feita.

**Conformidade ou Legalidade**: propriedade que garante que o sistema deve perseguir as leis vigentes e normas associadas a este tipo de método.

## 1.2. Modos de ataque

### 1.2.1. Phishing

Como afirma o Tavares (2017), "*Phishing* é oriundo da palavra pesca em inglês, e é propositadamente mal escrito para mostrar a facilidade de confundirmos palavras similares, fazendo uma comparação com a facilidade de confundir um domínio ligeiramente errado" (p.38). Neste caso, a vítima é o peixe que morde a isca.

### 1.2.2. Engenharia Social

O maior problema na segurança são as pessoas, que, pelas suas características psico-emocionais, podem facilmente serem manipuladas, induzidas, coagidas, ou

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

forçadas a violar aspecto de segurança para conceder acesso ou privilégios a alguém, dai que, a maior protecção contra a Engenharia Social, continua a ser a educação e consciencialização (Tavares, 2017, p.22).

De acordo com Winnefeld (2015):

> Há maiores chances de sucesso em ataques de Engenharia Social, quando as pessoas são ignorantes relativamente às práticas de segurança. Por esta razão, a característica mais comum nos ataques modernos é concentrarem-se no elo mais fraco na cadeia de segurança, ou seja, no ser humano.

Por outra, o atacante pode também criar uma situação que influencia a vítima a iniciar o contacto, pedindo uma solução para uma questão técnica. Como afirma o Tavares (2017), "o principal benefício desta técnica é que os usuários nunca questionam da autenticidade da informação que eles iniciaram, devido à ilusão de controlo da situação, por terem sido eles que iniciaram a conexão, técnica chamada de Engenharia Social Inversa" (p.31).

### 1.2.3. Byod

Na fase de consumerização de TI, as organizações permitem que seus funcionários tragam seus dispositivos pessoais para o ambiente de trabalho. Isso é obtido por meio da aplicação de uma política intitulada Bring Your Own Device (Traga seu Próprio Dispositivo). As políticas BYOD adoptadas em várias organizações, são vagas e geralmente imaturas ( Costa & Sebastião, 2021).

Com afirmação do Cometti e Aguado (2016), "agora que você já domina os melhores exercícios de segurança da informação, deve conhecer mais sobre essa nova inclinação na zona de *IT* chamada de *BYOD*. Finalmente, ela pode fazer elevar-se novas ameaças no quadro tecnológico" (p. 34).

### 1.2.4. Modelo – Plan, Do,Check, Act (PDCA)

Nesta senda, a gestão responde ao que será feito para acreditar a segurança informática, e a tecnologia assume o papel de responder "como" será acreditada a segurança informática.

A norma ABNT NBR ISO/IEC 27002 tem por objectivo normal um modelo para instituir, implementar, realizar, monitorar, analisar criticamente, sustentar e aprimorar um Sistema de Gestão de Segurança da Informação (ABNT NBR ISO/IEC 27002, 2022).

Para cumprir com seu objectivo a ABNT NBR ISO/IEC 27002 usa o modelo PDCA (Plan-Do-Check-Act), essa norma tende a garantir melhoramento contínua do Sistema de Gestão de Segurança da Informação

(SGSI), para melhor entendimento dessa norma a imagem abaixo enobrece o ciclo PDCA.

Conforme Menezes (2016), "o sistema de administração de segurança informática sabe fazer a gerência da informação através de um sistema que proporciona uma garantia pela sua abordagem que possibilita atingir uma melhoria continua deste sistema" (p.45). Assim, a *figura 1* mostra todos os passos do ciclo PDCA com uma breve explicação.


Figura 1: Ciclo de vida PDCA aplicado aos processos de um SGSI.
Fonte: Adaptado de Oliveira (2017).

❶ **Plan** (planear): Definição de procedimentos, políticas, processos e objectivos necessários para a administração dos riscos, de modo a aumentar a segurança informática;

❷ **Do** (fazer; implementar e operar): Implementar e operar as políticas, processos e procedimentos que foram definidos na fase de planeamento;

❸ **Check** (verificar; monitorizar e rever): Monitorização da performance dos processos implementados com as políticas e objectivos definidos; e

❹ **Act** (agir; manter e optimizar): Realizar medidas correctivas e preventivas, baseadas na monitorização realizada na fase *check*.

Segundo a norma (ABNT NBR ISO/IEC 27002, 2022) "tem por objectivo insinuar bons exercícios de gerência de segurança informática para as organizações, através da selecção, implementação e gerenciamento de controlos apoiados nos ambientes institucionais".

## 2. METODOLOGIA DE INVESTIGAÇÃO

Esta fase, apresenta a necessidade de narrar e justificar os comportamentos metodológicos usados na realização de investigação sobre a melhoria de políticas de segurança informática no ISCPC.

Para o Pardal e Lopes (2012) dizem nos que:

> "O procedimento metodológico acomoda a um corpo orientador da investigação que, obedece a um sistema de regras, torna possível a escolha e a articulação tecnológica, com o intuito de se poder fortalecer o processo de pesquisa, conferindo ordem, coerência ao longo da pesquisa" (p.12).

Para a efectivação da investigação, recorreu-se a análise de caso como existindo uma das escolhas metodológicas, que de forma limpa e acessíveis, nos conduz ao alcance dos objectivos preconizados para o artigo.

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

## 2.1. Caracterização do instituto superior de ciências policiais e criminais.

### 2.1.1. Definição

Instituto Superior de Ciências Policiais e Criminais, adiante designado por ISCPC, estabelecimento de ensino superior politécnico, público e policial que integra o sistema de formação, ensino e preparação das forças e serviços da Polícia Nacional, com vista a desenvolver actividades de ensino, de investigação e de apoio à comunidade, com a finalidade essencial de formar oficiais destinados aos quadros da Polícia Nacional.

### 2.1.2. Natureza

O Instituto Superior de Ciências Policiais e Criminais é, nos termos da lei, uma pessoa colectiva pública, dotada de personalidade jurídica, e goza de autonomia estatutária, científica, pedagógica, cultural, financeira, disciplinar e administrativa.

### 2.1.3. Missão

O ISCPC tem por missão formar oficiais de Polícia, habilitando-os ao exercício das funções que estatutariamente lhes são cometidas, bem como promover o desenvolvimento individual para o exercício de funções técnicas, no âmbito dos cursos de especialização e de progressão na carreira.

### 2.1.4. Estudo de caso

É nessa perspectiva que a investigação pretende fazer referência ao nível de perfilhamento de políticas de segurança do sistema de informação no ISCPC, onde, para o efeito, se recorreu a esta metodologia de investigação.

### 2.1.5. Inquérito por questionário

Tratando-se do grupo da amostra em termos quantitativos mais significativos, o inquérito por questionário foi escolhido, pelas vantagens que brindava, como sendo a prática mais adaptada à intenção.

### 2.1.6. Aplicação de Inquérito aos efectivos do ISCPC

Foi elaborado um questionário com perguntas fechadas, mas sempre respeitando a confidencialidade dos participantes. Foi concedido aos inquiridos, o tempo necessário para a leitura e compreensão das questões de modo a responderem adequadamente às mesmas. O questionário foi respondido exclusivamente por via presencial, com recurso ao documento impresso em folha de papel A4, entre os dias 19 à 24 de Maio de 2024, tendo sido recolhidos 31 inquéritos.

O questionário que funde o presente estudo foi composto por 19 perguntas e estruturado em um único grupo de questões. Com característica ao nível do conhecimento sobre a política de segurança informática na

instituição em estudo (ISCPC), opinião e atitude dos efectivos face à segurança informática e Engenharia Social.

### 2.1.7. Etapas para melhoramento e desenvolvimento da política de segurança informática no ISCPC.

De acordo com a busca bibliográfica, deve-se organizar o trabalho de melhoramento e elaboração da política de segurança informática, baseado em vários trabalhos referenciados; assim foi possível a elaboração feita pelo autor, em esquema de três etapas que se relacionam na próxima *tabela nº 1*:

Tabela 1. Etapas para melhoramento e desenvolvimento da política de segurança informática na rede do ISCPC.

| | MÉTODO/TECNOLOGIA | SOLUÇÃO |
|---|---|---|
| 1ª ETAPA: LEVANTAMENTO DA INFORMAÇÃO | Ambiente Tecnológico ou parque tecnológico | Pretende-se ter o controlo da métrica de segurança informática na instituição para se verificar se os mecanismos de protecção estão a ser realizados de forma adequada, avaliar constantemente a evolução do nível de segurança do seu meio de TIC e esperar um retorno dentro do parque informático, com auxílio do instrumento Wireshark. |
| | Workflow entre ambientes | Pretende-se saber do fluxo de trabalho entre workstations para melhor equilibrar aquilo que é o objectivo esperado com o suporte da ferramenta keylogger ou screenlogger. |
| | Contrato com as plataformas de computação em nuvem para reforçar o backup | Apetece-se com isso dizer que a computação em nuvem, ou cloud computing, será sobreposta como tecnologia para proporcionar armazenar e acessar arquivos 24h ao dia na Internet. Ou seja, não será sempre a necessidade de socorrer-se a um espaço físico ou mecanismos de hardware com memória limitada para salvar dados e informações. Em teoria, tudo é executado por meio de um software individualizado e cabe ao fornecedor desse tipo de serviço acreditar a segurança de tudo que está sendo reservado. |
| 2ª ETAPA: DESENVOLVIMENTO E ELABORAÇÃO DOS PROCEDIMENTOS DE POLÍTICAS E NORMAS DE SEGURANÇA | Regras de criptografia | São fornecidas senhas interinas aos usuários de forma segura. O uso de notícias nos correios electrónicos desprotegidas (não criptografadas) poderá ser evitado. A possibilidade de usar recursos de criptografia e legalização digital na protecção dos repositórios a serem produzidos por efectivos do ISCPC. |
| | Criar hotline | Instala-se um canal de denúncia das actividades desenvolvidas pelos efectivos do ISCPC para o controlo milimétrico da produção diária, com ajuda de um sistema utilitário hotline com keylogger ou screenlogger. |
| | Comité de segurança informática | Intende-se montar uma equipa responsável por criar procedimentos e realizar a divulgação para os membros da instituição. É recomendável que líderes/chefe de outras áreas façam parte desta equipa, pois os valores das informações mudam de área para área. |
| | Proprietário da informação | Caberá ao proprietário da informação realizar a deliberação do tipo de acesso que poderá ter, sendo necessária uma autorização directa ou designada com uma responsabilidade acrescida. |
| | Usuário do sistema computacional | Nesta etapa, os utilizadores dos sistemas computacionais são reconhecidos e autenticados durante um procedimento chamado Login. Os métodos de login são utilizados para atribuir a passagem aos dados e aplicativos em um sistema computacional e direccionam os utilizadores durante seu reconhecimento e autenticação. Geralmente, esse processo circunda a entrada de ID e uma senha. A identificação esclarece para o computador quem é o utente e a senha é um autenticador, isto é, ela assegura ao |

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

| | | |
|---|---|---|
| | | computador que o utilizador é efectivamente quem ele diz ser. Devem colar-se às determinações explicadas pelos profissionais de segurança informática. |
| | Auditoria Interna | Fiscalizar as actividades internas dos efectivos, sobre a política de auditoria nos diferentes sistemas de tecnologia da informação relativos à protecção e precaução no tratamento dos dados da instituição, com suporte de um espião screenlogger ou kali linux. Também são responsáveis pelo fornecimento de relatórios para gerência superior sobre a eficácia dos controlos de segurança, consolidados através de auditorias independentes e frequentes. Como também examinam se as políticas, padrões, orientações e procedimentos são infalíveis e estão em semelhança com os objectivos de segurança definidos para a instituição ou equipa. |
| | Classificação da informação de acordo o nível | Classificar-se-ão as informações para que se tenha uma visão ampla do que carece ser protegido, pois cada informação tem um valor desigual. É necessário analisar e identificar as informações para que se possa classificá-las em níveis. Tais níveis também podem ser usados por toda a instituição, a fim de padronizá-las. |
| | Resposta de gerenciamento a incidentes e recuperação de desastre | Pretende-se criar uma dinâmica na instituição, caso haja um quebramento de segurança informática. Por isso, pode-se manter uma equipa de IT sempre pronta para gerenciamento e recuperação de desastre. Elas efectuam treinamentos constantes para replicar aos mais diversos tipos de incidentes. Esses exercícios incluem simulações juntas, actividade de agilidade técnica e compartilhamento de inteligência com instituições parceiras. |
| | Processo disciplinar | Aplica-se uma chamada de atenção ou mesmo uma sanção na violação da política de segurança informática. Trata-se de uma declaração poderosa, pois garante que acções disciplinares possam ser tomadas contra um utilizador se a directiva não for aderida. É muito importante que esta declaração esteja directamente relacionada com a política disciplinar geral vigente no ISCPC. |
| | Acesso à Internet | Poder-se-á controlar o acesso à Internet, porque a maior porta de entrada de arquivos maliciosos tem como origem o acesso irrestrito à internet. Deverá ter limite ou bloqueio ao acesso à internet para pessoas autorizadas, sendo monitorado o login do usuário, sites acessados e suas respectivas horas, a partir do firewall e iptables. |
| | Acesso à segurança física | O acesso à segurança física deve ser bem controlado com algumas medidas de precaução conhecidas como: portas brindadas, fechaduras com sistema de alarme, guardas de segurança etc. O acesso para esse espaço deve ser sempre monitorado e permitido somente para pessoas autorizadas, pois há um grande risco na instituição se houver algum problema nos equipamentos existentes. |
| | Acesso à segurança lógico | Poderá ser usada tecnologia avançada no controlo de acesso lógico, com objectivo de proteger, aplicativos e repositórios de dados contra escassez, modificação ou difusão não autorizada. Os sistemas computacionais, bem desiguais de outros tipos de protecções, não podem ser facilmente fiscalizados apenas com mecanismos físicos, como cadeados, alarmes ou protecções de segurança. Há necessidade de implementação de firewall e iptables. |
| | Protecção contra softwares maliciosos | Os softwares maliciosos podem entrar no computador de vários formatos. Seguem-se alguns itens de clarificação dos casos recorrentes de software maliciosos: - Transferência de software grátis da Internet que sigilosamente contém programas maldosos; |

| | | |
|---|---|---|
| | | - Transferência de software leal que ocultamente contém programas maldosos; - Visita a um Website contagiado com programas maliciosos; - Clique numa mensagem de engano ou janela de pop-up inexacta que começa uma transferência de programas maldosos; - Abertura de um agregado de e-mail que contém softwares maliciosos. Como prevenir: Firewall, antivírus, iptables, programas anti-spywares. |
| | Mantenhas os softwares e drives actualizados | Como é recomendado que os programas estejam sempre actualizados para evitar a penetração dos hackers aos sistemas, é por meio de fracassos encontrados em programas que são aproveitadas. Por isso, vai-se acompanhar o lançamento de novas actualizações dos fornecedores, para corrigir os fracassos que possibilitam esse tipo de acção e tornar os sistemas mais honestos. Caso não se actualize, as brechas demoram e os cibercriminosos procedem ter seus mecanismos de acção facilitados. |
| | Estabelecer controlo de acesso para os efectivos e colaboradores | Sabe-se que uma maneira comum de ajudar os problemas de segurança informática é por canal de acções inadequadas dos utilizadores. Por isso, mantem-se o controlo ao acesso eficaz do pessoal, para evitar perca de dados, com ajuda de login ou por sensor de presença para captação da imagem. |
| | Estabeleça bloqueio de sistemas de saída | Deve-se estabelecer uma verificação de cerco de sistema de saída: controlar os aplicativos em computadores do ISCPC; cercar virtualmente todo qualquer Cavalo de Troia, spyware ou malware que tente ser executado ou carregado em um aplicativo presente; bloquear ou permitir diferentes modelos de dispositivos que se encaixam a computadores do ISCPC, como dispositivos USB, bluetooth, etc. Cercar ou permitir vias seriais e portas paralelas; impedir que malware assuma a verificação de aplicativos; restringir os aplicativos que devem ser executados; barrar utilizadores de alterar repositórios de configuração; proteger chaves do registo próprio; proteger pastas próprias como WINDOWS\system; pode-se bloquear o uso de e-mails individuais dentro do ambiente institucional, bem como sites de redes sociais. |
| | Monitoramento do uso e acesso ao sistema académico | Um pessoal técnico poderá, de forma permanente, fazer o monitoramento das actividades em algumas áreas, dentro do ISCPC e no sistema académico, para evitar o uso inadequado, e, é preciso conhecer o que está ocorrer no sistema académico e em toda extensão da rede. Qualquer tipo de procedimento errado, vulnerabilidade, mudança nos modelos de acesso deve ser percebido prontamente, de forma a ser contida e acautelar um ataque digital gerado por pessoas mal intencionadas. Como suporte de apoio técnico Wireshark e screenlogger. |
| | Contracto de ajuda ou resgate de empresas especializadas em SI | Poderão ser contratadas instituições especializadas na zona de segurança informática para esforçar a privacidade e integridade dos dados do ISCPC. Elas estão sempre atentas para as novidades, trazer e desenvolver decisões importantes e inteligentes que auxiliarão a potencializar os mecanismos de protecção da instituição. Por exemplo, pode-se computar com essas instituições/organizações para o armazenamento de backups nas nuvens como reforço. |
| | Leitura biométrica | Notou-se que, nos últimos anos, a senha vem sendo deixada cada vez mais de lateral, para dar espaço a modos mais eficazes de autentificar o acesso a dados, como a autenticação ou leitura biométrica. Podem-se usar características biológicas físicas para identificação e autenticação dos utilizadores dos sistemas, já que características pessoais como impressão digital, geometria da mão e padrão ocular, não podem ser roubadas, apesar de que esta |

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

| | | |
|---|---|---|
| | | solução requer um alto investimento na aquisição de equipamentos de autenticação telebiométricos, como leitores e câmaras, que produzam a leitura das características físicas das pessoas. |
| | Plano de contingência | Não basta pensar em medidas precaucionais. Sabe-se que os cibercriminosos são talentosos e criam constantemente novas configurações de actuação para conseguirem seus objectivos. Para não surpreenderem, os péritos em segurança informática devem estar preparados de forma a reverter a situação, para evitar perdas inestimáveis. Além disso, as questões não se delimitam apenas aos casos de ataques produzidos por hackers: desastres tecnológicos, fracassos humanos, entre outros, são continuamente. É preciso ter conhecimento como agir nessas posições. Assim, é essencial instituir actividades uniformizadas, já que a mitigação dos danos pode ser executada por qualquer um dos membros conscientes pela zona de segurança informática. As acções podem transformar de profissional para profissional, o que pode provocar problemas posteriores. Portanto, pode ser fundamental a criação de parâmetros de padronização como um documento no qual estarão definidas as responsabilidades estabelecidas no ISCPC, para reflectir a uma emergência e também deve englobar informações aprofundadas sobre as características da área ou sistemas enrolados. |
| | Capacitação dos efectivos e técnicos do ISCPC | Capacitação dos efectivos e técnicos, com o intuito de acreditar o comportamento seguro no ingresso de dispositivos da instituição e pessoais à rede do ISCPC. Se, por um lado, os utilizadores precisam estar conscientes dos riscos e punições ao expor as informações da instituição, da mesma forma, o ISCPC deve investir na implementação e actualização constante dos técnicos que poderão dar resoluções de segurança informática nos equipamentos da instituição ou pessoais, que acessam a rede do ISCPC. |
| 3ª ETAPA: APROVAÇÃO E IMPLEMENTAÇÃO DE POLÍTICAS, NORMAS E PROCEDIMENTOS DE SI | O papel da alta administração | Sabe-se que o sucesso da PSI está directamente relacionado ao envolvimento e à actuação da alta regência. Quanto superior for o comprometimento da administração superior com os processos de composição e implementação da PSI, superior a possibilidade de ela ser efectiva e eficiente. Esse comprometimento reconhece ser expresso oficialmente, por escrito, pela equipa multidisciplinar da segurança informática. |
| | Responsabilidade na implementação | A responsabilidade sobre a segurança informática no seu melhoramento de políticas na incumbência da equipa de IT do ISCPC. |
| | Processo de Implementação e Manutenção da política | O sistema de implementação de política de segurança informática reconhece ser formal. No decorrer dessa implementação do processo, a PSI deverá permanecer susceptíveis acertos para melhor adaptar-se às reais precisões. O tempo, desde o começo até a completa implementação, tende a ser prolongado. Em resumo, as essenciais etapas que dirigem à implementação bem-sucedida da PSI são: elaboração, aprovação, implementação, divulgação e manutenção. Muito cuidado deve ser dado às duas últimas etapas. Geralmente, após o alcançamento das três primeiras fases, as gerências de segurança recomendam terem cumprido o dever e esquecem-se da importância da propagação e actualização da PSI. |

Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

## 3. RESULTADOS

Tratando-se do grupo da amostra em termos quantitativos mais significativos, o inquérito por questionário foi escolhido pelas vantagens que brindava, como sendo a técnica mais adaptada à intenção.

O questionário com perguntas fechadas, mas sempre respeitando a confidencialidade dos participantes. Foi concedido aos inquiridos, o tempo necessário para a leitura e compreensão das questões de modo a responderem adequadamente às mesmas. O questionário foi respondido exclusivamente por via presencial, com recurso ao documento impresso em folha de papel A4, entre os dias 19 a 24 de Maio de 2024, tendo sido recolhidos 31 inquéritos do público alvo (efectivos do ISCPC).

Tabela 2. Já teve acesso as políticas de segurança informática digitais?

| SINALIZAÇÃO | Frequência | % |
|---|---|---|
| Sim, quando assinei o contracto de trabalho | 8 | 26% |
| Tenho acesso periodicamente | 5 | 16% |
| Está sempre disponível | 3 | 10% |
| Nunca tive acesso | 15 | 48% |
| Total | 31 | 100% |

Fonte: Elaboração dos autores (2024)

Tabela 3. Há objectivos de segurança a serem atingidos para poder melhorar a qualidade da informação digital?

| SINALIZAÇÃO | Frequência | % |
|---|---|---|
| Sim | 12 | 39% |
| Não | 1 | 3% |
| Não sei | 18 | 58% |
| Total | 31 | 100% |

Fonte: Elaborado pelos autores (2024)

Tabela 4. É importante a organização apresentar, por escrito, as políticas de segurança que tenho de respeitar?

| SINALIZAÇÃO | Frequência | % |
|---|---|---|
| Discordo totalmente | 2 | 6% |
| Discordo em parte | 1 | 3% |
| Nem concordo nem discordo | 5 | 16% |
| Concordo em parte | 16 | 52% |
| Concordo totalmente | 7 | 23% |
| Total | 34 | 100% |

Fonte: Elaborado pelos autores (2024)

## 4. DISCUSSÃO DOS RESULTADOS

Foram analisadas e expostas as respostas obtidas em cada questão do inquérito. A discussão dos resultados tem como objectivo apresentar a visão dos efectivos do Instituto Superior de Ciências Policiais e Criminais (ISCPC), relativamente à melhoria de políticas de segurança informática na rede. Através de questionário contendo questões fechadas foram colectados dados para a pesquisa, tratados de forma estatística e representados através de e gráficos, onde o tratamento dos mesmos foi feito por meio do programa Microsoft Excel 2019.

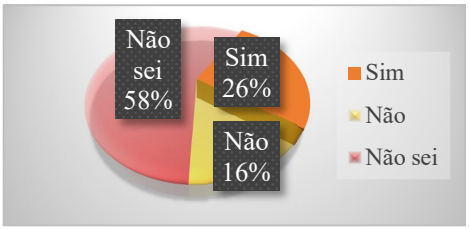


Gráfico 1: Existe uma área que analisa as possíveis fragilidades sobre a protecção da informação no ISCPC?

Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

Relativamente as fragilidades 26% afirmavam que sabiam da existência da área de análise e 16% juravam que não existe nenhuma área que analisa esses dados e informações. Durante a pesquisa, percebeu-se que era desconhecida a possível fragilidade sobre a protecção das informações digitais dentro do ISCPC, com mais de 55% dos efectivos que não sabiam do assunto.

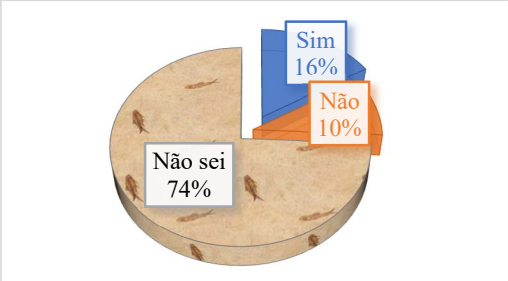


Gráfico 2: As ameaças estão identificadas no processo de informação dentro do ISCPC?
Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

De acordo com os dados estatísticos apresentados na figura acima, pode-se compreender que 74% dos efectivos do ISCPC não têm capacidade de identificar as ameaças no processo da informação digital. Outros 16% dos efectivos têm a noção das ameaças que são sujeitas, e 10% não sabem da existência das ameaças no meio do parque informático.

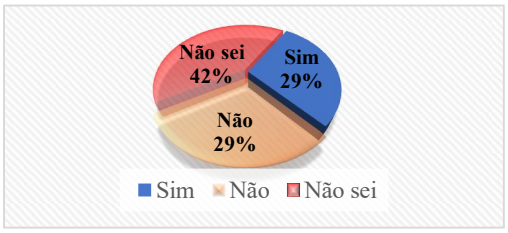


Gráfico 3: A instituição utiliza boas práticas em segurança da informação digital?

Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

Quanto às boas práticas em segurança da informação digital, 42% não sabem se existe ou não dentro do parque informático do ISCPC, já com a percentagem igual a 29% responderam sim, e igual percentagem que optaram em não respectivamente.

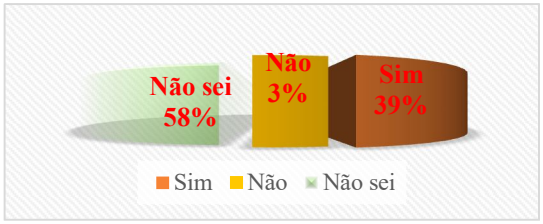


Gráfico 4: Há objectivos de segurança a serem atingidos para poder melhorar a qualidade da informação digital?
Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

No gráfico acima, verificou-se que 58% dos efectivos do ISCPC não sabiam o objectivo da segurança digital para melhoria da qualidade da informação, mas apurou-se que 39% dos efectivos têm intenção de que sejam aplicados objectivos da segurança da informação digital, e apenas 3% não apoiam essa iniciativa.

Pode-se afirmar que, aproximadamente, 61% dos efectivos não têm conhecimento de como melhorar a qualidade de serviço na instituição.

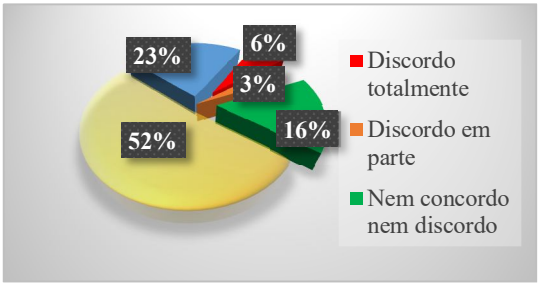


Gráfico 5: É importante a organização apresentar, por escrito, as políticas de segurança que tenho de respeitar?

Fonte: Elaboração própria dos autores a partir de dados da pesquisa (2024).

De acordo com os inquiridos, 52% concordam, em parte, que a instituição apresente, por escrito, um documento que dirige as regras da política de segurança. 23% dos efectivos concordam totalmente com esta iniciativa de que o órgão deve, necessariamente, apresentar por escrito, pelo facto de ter uma grande importância no campo tecnológico e não só. Também se apurou que 16% nem concordam e nem discordam com esta iniciativa de se ter um documento por escrito sobre a importância das políticas de segurança no ISCPC. 6% que discordam totalmente com a bela iniciativa que pode facilitar a protecção dos dados dentro desta unidade policial e 3% discordam em parte sobre esta iniciativa de aplicar esse dossiê no órgão. Os resultados no gráfico 05 indicam que 77% dos funcionários concordam, em parte, em ter uma política de segurança da informação, que permite planear a questão do aumento do conhecimento sobre a actividade e colocar em discussão e generalizar a política de segurança da informação que se propõe para que todos os funcionários do ISCPC assimilem a sua importância e a necessidade de ser melhorada, de modo a salvaguardar a integridade da sua informação.

## 5. CONCLUSÕES

Na investigação realizada no ISCPC conclui-se que não ter um marco de políticas bem definidas, embora a área de tecnologia tenha alguns controlos internos, é fundamental que se sigam esboços para a segurança informática e não estar expostos a ataques de roubo de informação. Nos resultados do diagnóstico realizado à segurança informática, pode-se constatar que os pontos mais vulneráveis são: área dos departamentos no seu compito geral, área de base de dados para o controlo dos docentes e cadetes, área do corpo de alunos, área dos computadores servidores e a falta de políticas de segurança informática nos portões da referida instituição, o que suporta a uma falta de revisão e verificação do cumprimento destas, falta de documentação técnica e de treinamento e a elaboração de planos de contingência adequados para garantir a recuperação dos serviços que se brindam a toda a comunidade universitária ante desastres e interrupções do serviço. Com a

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN PRINT: 3006-2489; ISSN ONLINE: 3006-2470
1ª Ed, Vol. 1, No. 9, Novembro, 2025
https://alba.ac.mz/index.php/alba/issue/view/12
albaisfic@gmail.com; alba@isfic.ac.mz

identificação da importância que têm os domínios de segurança informática, por meio da análise da informação proporcionada pelos funcionários, pode-se qualificar que controlos se consideram como os mais urgentes para melhorar as percentagens de cumprimento actual, também se pode evidenciar que existe uma grande preocupação pela ausência de algumas políticas de segurança informática na instituição. Por isso, uma adequada etapa de políticas de segurança informática e as revisões periódicas de seu cumprimento ajudam a manter sob controlo os riscos de segurança informática que tanto os usuários, pessoal técnico, coordenadores e autoridades estão expostos diariamente. As políticas que se desenharam são consideradas como as mais adequadas para aumentar as percentagens de cumprimento, já que, ao estabelecer políticas de segurança informática, se vai conseguir uma melhor segurança, organização, conscientização, desempenho trabalhista e o resultado foi a obtenção de uma melhoria na segurança informática. Os funcionários, como os usuários finais, terão constantemente o conhecimento de suas obrigações, responsabilidades, proibições, consequências e tarefas que têm que desempenhar diariamente em seus postos de trabalho.

## 6. REFERÊNCIAS BIBLIOGRÁFICAS

Cometti, M. B., Aguado, A. G. (2016). Políticas de segurança da informação para byod. *R.tec.fatecam*, 4(1), 151-173.

ISO/IEC 27002 (2022). *Information security, cybersecurity and privacy protection — Information security controls*. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Manoel, S. S. (2014). *Governança de Segurança da Informação: como criar oportunidades para o seu negócio*. Rio de Janeiro: Brasport.

Menezes, U. T. J. (2016). *O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola*. (Dissertação de Mestrado), Faculdade de Direito da Universidade de Lisboa, Lisboa, Portugal.

Miano, M. V. (2016). Elementos necessários para o desenvolvimento de uma política de segurança da informação para uma instituição de ensino superior pública. *Revista Tecnológica da Fatec Americana*, 04(02), 112-125.

Monteiro, J. F. (2017). *Adopção de Políticas de Segurança de Sistemas de Informação nas Universidades Moçambicanas*. Dissertação do Mestrado, Escola Superior de Tecnologia e de Gestão Instituto Politécnico de Bragança, Portugal.

Oliveira, G. L. (2017). *O Impacto da Engenharia Social em Uma Cooperação*. Disponível em: https://www.riuni.unisul.br/bitstream/handle.pdf

Oliveira, I. B. P., Figueiredo, W. C. A., Faria, A. C. C. (2019). Política de Segurança da Informação: Um Modelo Voltado para uma Instituição de Ensino Superior.

*Revista Electrónica Cosmopolita em Acção, 6(1), 21-30.*

Pardal, L., e Lopes, E. (2012). *Métodos e técnicas de investigação social*. Porto: Areal editores.

Costa, N., Sebastião, M. (2021). *Bring Your Own Device (Byod): políticas de segurança na implantação em ambientes corporativos.* Disponível em: *https://repositorio.ifap.edu.br/jspui/handle/prefix/383*

Quissanga, F. C., Fernandes, R. F. (2020). Importância da segurança da informação nas empresas corporativas do ramo da tecnologia de informação. *Project, Design and Management, 2*(1), 87-102.

Rios, O. K. L., Filho, J. G. A. T., Rios, V. P. S (2017). Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. *Revista de Gestão e Tecnologia Navus*, 7(2), 49-65.

Sequesseque, M. T. M. (2017*). O impacto da implementação de segurança da informação na usabilidade dos sistemas de informação.* Dissertação de Mestrado, Instituto Politécnico de Setúbal, Portugal.

Tavares, T. (2017*). O Factor Humano na Segurança de Informação nas Organizações.* Dissertação de mestrado, Faculdade de Direito, Lisboa.

Vasconcelos, E. O. (2017). *Gestão da segurança da informação no serviço público estadual de minas gerais.* Dissertação de mestrado, Escola de Governo Professor Paulo Neves de Carvalho da Fundação João Pinheiro, Brasil.