

Projecto Moçambique Ciber Seguro



"Moçambique Digital, Moçambique Seguro!"

Abstrato

Nos últimos anos, Moçambique tem-se destacado nos *rankings* da Cibersegurança devido as grandes taxas de infeções de *malware*, software desatualizado e vulnerabilidades expostas na internet.

Muitos dos riscos de Cibersegurança identificados em Moçambique, podem ser evitados com higiene básica de Cibersegurança.

O Projecto Moçambique Ciber Seguro (PMCS) é um Projecto criado para ajudar as instituições do país e as pequenas e médias empresas (PME) de Moçambique a melhorar a sua postura de Cibersegurança, mediante a adoção de um conjunto de diretrizes fundamentais relacionadas com a gestão de tecnologia em 10 domínios distintos:

1. Políticas corporativas
2. Gestão de Inventário
3. Gestão de contas e controlos de acesso
4. Proteção de E-mail e Web
5. Defesas anti-malware
6. Recuperação de dados
7. Consciencialização e treino de competências
8. Gestão de vulnerabilidades
9. Proteção de dados
10. Resposta a incidentes

Colaboradores

As seguintes individualidades e/ou instituições colaboraram na elaboração deste documento:

Nome	Tipo de Contribuição	Instituição
André Tenreiro	Autor principal	Individual

Histórico do documento

Nome	Data	Versão	Comentários
André Tenreiro	10/12/2023	1.0	Versão inicial

1. Introdução

O PMCS é um conjunto diretrizes de Cibersegurança não prescritivas que recomenda um conjunto de **ações básicas** de Cibersegurança de forma a reduzir rapidamente o risco e a superfície de ataque de grande parte das instituições e empresas em Moçambique.

1.1 Estrutura do documento

O PMCS recomenda um conjunto de ações nos seguintes domínios:

1. Políticas de segurança
2. Controlo de Inventário (software/hardware)
3. Gestão de contas e controlos de acesso
4. Proteção de E-mail e Web
5. Defesas anti-malware
6. Recuperação de dados
7. Consciencialização e treino de competências
8. Gestão de atualizações
9. Proteção de dados
10. Resposta a incidentes

Em cada um destes domínios, há um conjunto de subactividades denominados de **controlos** (de segurança).

Cada controlo de segurança incluirá o seguinte:

- Identificador único do controlo de segurança (exemplo "5.1")
- Nome do controlo de segurança
- Descrição da medida de segurança que inclui alguns objectivos principais
- Função de segurança (ver alínea seguinte)

1.2 Funções de Segurança

Tal como descrito da diretriz de segurança do NIST¹, um controlo de segurança poderá ter as seguintes funções:

Função de Segurança	Descrição
Identificar	Esta categoria envolve o desenvolvimento de uma compreensão organizacional para gerir o risco de segurança cibernética para sistemas, ativos, dados e capacidades. Isso inclui a identificação de ativos críticos, a avaliação de riscos e a definição de um plano de gestão de riscos.
Proteger	Esta função foca-se na implementação de salvaguardas apropriadas para garantir a entrega de serviços críticos. Inclui aspectos como controlo de acesso, proteção de dados, manutenção de sistemas e procedimentos de segurança para proteger contra ameaças e vulnerabilidades.
Detectar	Esta categoria está centrada na implementação de atividades necessárias para identificar a ocorrência de um evento de segurança cibernética. Isso pode envolver o monitoramento contínuo de sistemas e redes, a deteção de anomalias e a realização de avaliações de segurança.
Responder	Após a deteção de um evento de segurança cibernética, esta função trata da resposta a esse evento. Isso inclui ações como comunicação do incidente, análise do impacto, contenção do incidente e coordenação com partes interessadas externas, se necessário.
Recuperar	Esta última categoria aborda as atividades necessárias para restaurar quaisquer serviços que foram prejudicados devido a um incidente de segurança cibernética. Isso pode incluir a restauração de sistemas e dados, melhorias nos controlos de segurança e a comunicação com partes externas para restabelecer a confiança e a reputação.

Juntas, estas categorias formam um ciclo contínuo de melhoria e fortalecimento da segurança cibernética de uma organização, permitindo uma melhor preparação, resposta e recuperação de incidentes de segurança.

¹ <https://csrc.nist.gov/>

2. Domínios de Segurança

01 Políticas de Segurança

Objectivo: Esta categoria de controlos visa estabelecer um regulamento interno para o uso responsável das tecnologias. As empresas, deverão ter a flexibilidade de definir o que deve constar neste regulamento e o mesmo dever ser informado de forma clara e objetiva.

Controlos

Ref.	Nome	Função de Segurança
1.1	Política de uso informático A empresa deverá definir uma política de uso responsável dos meios informáticos disponibilizados. A política deve constar, informações tais como os seguintes <u>exemplos</u> : <ul style="list-style-type: none">• Definir que os meios informáticos disponibilizados pela empresa aos seus funcionários devem ser utilizados apenas para fins profissionais.• Definir exceções para uso pessoal (se aplicável) desde que as mesmas sejam autorizadas pela empresa (exemplos: sites de notícias).• Proibição de instalação ou uso de qualquer aplicação local ou na Cloud que não seja previamente autorizada.• Proibição que o equipamento seja manuseado por pessoas externas a empresa e/ou pessoal não autorizado.• Proibição de partilha de informação da empresa para meios privados, como o envio de informações para contas de E-mail pessoal ou cópia de dados para o computador pessoal.• Proibição do uso de dispositivos de armazenamento externo (tais como USB drives) que costuma ser um meio de transmissão de <i>malware</i>.• proibição do acesso a sites tais como: conteúdo adulto, download/visualização de vídeos não autorizados (“piratas”). As políticas devem ser revistas de forma anual, e atualizadas se necessárias.	Identificar

02 Gestão de Inventários

Objectivo: No mundo da Cibersegurança é difícil defender algo que não é conhecido. Este domínio pretende criar mecanismos para que haja uma gestão de todo o inventário de *hardware/software* na empresa para que os mesmos sejam identificados, controlados e atualizados de forma rigorosa. Os adversários, estão continuamente a “varrer” o Ciberespaço à procura de dispositivos vulneráveis.

Controlos

Ref.	Nome	Função de Segurança
2.1	Estabelecer um inventário detalhado de hardware	Identificar

Estabelecer um inventário detalhado de todos os dispositivos de *hardware* tais como: *laptops*, servidores, *routers/switches*, sistemas de armazenamento, etc.

Deverá haver um repositório centralizado de informação, que inclua informações tais como:

- Marca e modelo do dispositivo
- Tipo de dispositivo (*laptop*, servidor, redes, storage, etc.)
- Data de compra
- Número da ordem de compra
- Informação relativa ao suporte (se aplicável)
- Endereço IP do equipamento
- Versão de *firmware* (se possível)
- Criticidade do Dispositivo/Activo (se possível)

Sempre que possível, a catalogação deste inventário deverá ser o mais automatizada possível. Mecanismos para o descobrimento de equipamento ligado, incluem *logs* de DHCP bem como o varrimento da rede (usando o Nmap por exemplo).

2.2	Estabelecer um inventário detalhado de software	Identificar
	Estabelecer um inventário detalhado de todo o <i>software</i> disponível na empresa, seja <i>on-prem</i> ou <i>Cloud</i> , bem como as suas versões.	

Deverá haver um repositório centralizado de informação, que inclua informações tais como:

- Fabricante, nome e versão do *software*

	<ul style="list-style-type: none"> • Tipo de <i>software</i> (aplicações de produtividade, <i>backups</i>, gestão financeira, E-mail, Web Browser, etc.) • Data de compra • Número da ordem de compra • Informação relativa ao suporte (se aplicável) • Licenças do <i>software</i> <p>Sempre que possível, a catalogação deste inventário deverá ser o mais automatizada possível. Mecanismos para o descobrimento de aplicações incluem o varrimento de redes em portos específicos (exemplo 80, 443, 8080, etc.) bem como a instalação de aplicações nos <i>laptops</i>/servidores que comuniquem todo o <i>software</i> que se encontra instalado.</p>
--	---

2.3	Estabelecer um procedimento para gerir inventário não autorizado	Identificar
	<p>Estabelecer um procedimento para gerir todo inventário de hardware/software que tenha sido encontrado na empresa.</p> <p>Todo o inventário não autorizado, deverá ser analisado e removido da empresa caso não haja uma forte razão para o manter.</p> <p>Caso haja exceções, estas deverão ser documentadas e autorizadas por escrito para efeitos de práticas de “boa governação”.</p>	

03 Gestão de contas e acessos

Objectivo: Esta categoria de controlos visa estabelecer um procedimento seguro para o uso responsável de contas e acessos. O comprometimento de acessos por falta de higiene básica, é um problema predominante e explorado frequentemente por adversários.

Controlos

Ref.	Nome	Função de Segurança
3.1	Gestão de Senhas	Proteger
	Estabelecer uma política e procedimento de gestão de senhas, tais como: <ul style="list-style-type: none">• Rotatividade periódica (exemplo: a cada 90 dias)• Proibição de reutilização de senhas antigas (exemplo: últimos 12 meses)• Número mínimo de caracteres (exemplo: 8-12 caracteres)• Utilização de símbolos e dígitos	
3.2	Restrição de privilégios	Proteger
	O acesso de administrador deverá estar limitado exclusivamente a contas de administrador. Contas de utilizador, não deverão ter privilégios elevados. É aconselhado que os administradores tenham duas contas distintas, uma para uso não elevado (exemplo: autenticação no computador, email, etc.) e outra para operações que requerem acesso elevado na organização tais como administração de sistemas e da rede.	
3.3	Desativar acessos inativos	Proteger
	Todos os acessos que estejam inativos, deverão ser desativados. Deve haver um processo e mecanismo na organização que identifique contas que não tenham sido utilizadas acima de um período definido (exemplo: 60 dias)	
3.4	Gestão de concessão de revogação de acesos	Proteger

	<p>Todos a concessão e revogação de acessos deverá estar sujeita a aprovação de modo que haja um histórico de todos os acessos.</p> <p>Sempre que houver uma mudança, tais como a saída de um funcionário da empresa, os acessos deverão ser revogados imediatamente.</p> <p>Idealmente, deverá haver um sistema automatizado de aprovações, mas na falta deste, poderá ser utilizado o e-mail para aprovações e o devido registo do e-mail para consulta futura.</p>
--	---

3.5	Utilização de MFA	Proteger
	<p>Sempre que possível, deverá ser utilizada autenticação multifatorial (MFA) principalmente para acessos a aplicações expostas à internet tais como: E-mail / Webmail, VPN, etc.</p> <p>Sempre que possível, também deve ser exigido o MFA para acessos administrativos.</p>	

04 Proteção de E-mail e Navegação Web

Objectivo: Um dos pontos comuns para a entrada de *malware* para uma intrusão é via E-mail e Web, por estes serem meios frequentes de intrusão em empresas. Deverá haver mecanismos para evitar que os utilizadores sejam ludibriados a abrir conteúdo malicioso nos respetivos clientes de e-mail e navegadores web.

Controlos

Ref.	Nome	Função de Segurança
4.1	Garantir que apenas que clientes de e-mail e navegadores web autorizados sejam utilizados	Proteger
	<p>Garantir que apenas clientes de E-mail e Navegadores Web fidedignos sejam utilizados. Outros clientes de E-mail/Navegação podem não conter todos os padrões de segurança e facilitar intrusões em empresas.</p> <p><u>Exemplos</u> de software considerado fidedigno incluem:</p> <p>Email</p> <ul style="list-style-type: none">• Microsoft Outlook• Microsoft Office 365 (Outlook web)• Google Workspace (GMail for Business)• Mozilla Thunderbird <p>Navegadores Web</p> <ul style="list-style-type: none">• Microsoft Edge• Google Chrome• Mozilla Firefox <p>De forma a assegurar uma proteção mais elevada, os mesmos devem ser atualizados com frequência para as últimas versões disponíveis.</p>	

4.2	Proteção contra emails forjados	Proteger
	<p>A utilização de SPF, DMARC e DKIM é crucial para as empresas na proteção contra fraudes de e-mail e <i>phishing</i>.</p> <p>O SPF (<i>Sender Policy Framework</i>) ajuda a validar os servidores autorizados a enviar emails em nome do domínio da empresa, prevenindo a falsificação de endereços.</p> <p>O DKIM (<i>DomainKeys Identified Mail</i>) adiciona uma assinatura digital aos emails, garantindo sua integridade e autenticidade.</p> <p>Por fim, o DMARC (<i>Domain-based Message Authentication, Reporting, and Conformance</i>) combina o SPF e o DKIM, fornecendo políticas e relatórios sobre a autenticação de emails, aumentando a segurança e a confiabilidade da comunicação empresarial.</p>	
4.3	Utilização de filtragem de DNS	Proteger
	<p>A filtragem de DNS é vital para empresas e indivíduos, pois bloqueia o acesso a sites maliciosos.</p> <p>Ao filtrar solicitações de DNS, impede-se o acesso a páginas que podem conter <i>malware</i>, <i>phishing</i> ou conteúdo inapropriado. Isso protege as redes e dispositivos de ameaças <i>online</i>, reduzindo o risco de ataques cibernéticos e comprometimento de dados. Além disso, a filtragem de DNS pode melhorar a produtividade ao limitar o acesso a sites não relacionados ao trabalho.</p> <p>Existem serviços gratuitos de filtragem de DNS, tais como:</p> <ul style="list-style-type: none"> • Quad9 • Cloudflare • OpenDNS <p>É importante salientar que o serviço de DNS do Google, conhecido como "8.8.8.8" não faz bloqueio de <i>malware</i> ou de conteúdo malicioso.</p> <p>Ao utilizar serviços gratuitos de filtragem de DNS, as empresas devem estar cientes de que estes provedores têm visibilidade sobre os domínios que são acedidos a partir da sua rede. Embora não tenham acesso ao conteúdo da navegação ou das comunicações, estas consultas podem revelar padrões de actividade.</p> <p>É fundamental avaliar as políticas de privacidade dos serviços escolhidos, uma vez que muitos recolhem e armazenam registos das consultas DNS para fins estatísticos ou de segurança.</p>	

É recomendável optar por provedores reputados e transparentes quanto ao tratamento destes dados, assegurando a privacidade e a integridade das informações corporativas.

05 Defesas Anti-malware

Objectivo: Empresas devem ter defesas *anti-malware* para proteger contra software malicioso que pode roubar dados, danificar sistemas e interromper operações. Essas ferramentas detetam e neutralizam ameaças, minimizando riscos de ataques cibernéticos e garantindo a segurança de informações confidenciais. Além disso, fortalecem a confiança dos clientes e cumprem regulamentações de proteção de dados, essenciais para a integridade e continuidade dos negócios.

Controlos

Ref.	Nome	Função de Segurança
5.1	Instalação de software de anti-malware	Proteger
	<p>As empresas deverão ter meios de proteção de <i>anti-malware</i> e execução de código malicioso, nomeadamente Antivírus.</p> <p>A instalação de <i>anti-malware</i> é recomendada em sistemas Windows e MacOSx, sejam workstations ou servidores.</p> <p>Em sistemas Linux (normalmente servidores) também é recomendado, contudo é necessário ter uma especial atenção porque nem todos fabricantes suportam devidamente esta arquitetura.</p>	
5.2	Atualizações automáticas de assinaturas de anti-malware	Proteger
	<p>De forma a garantir que a empresa está protegida contra novas variantes de <i>malware</i>, os softwares de <i>anti-malware</i> deverão dispor de atualizações automáticas de assinaturas.</p>	
5.3	Desativar a execução automática de armazenamento externo	Proteger

De forma a proteger contra a propagação e instalação de *malware* que possa estar contido em armazenamento externo (como drives USB's).

06 Recuperação de dados

Objectivo: Empresas devem ter meios de recuperação de dados para garantir a continuidade dos negócios após incidentes como falhas de sistema, ataques cibernéticos ou desastres naturais. Essas soluções permitem a rápida restauração de informações vitais, minimizando o tempo de inatividade e a perda financeira. Além disso, ajudam a manter a confiança dos clientes e a conformidade com regulamentações de proteção de dados.

Controlos

Ref.	Nome	Função de Segurança
6.1	Implementar e sustentar um procedimento para a restauração de dados.	Recuperar
O processo de recuperação de dados para uma empresa deve incluir: identificação de dados críticos, implementação de <i>backups</i> , escolha de soluções de armazenamento confiáveis (como nuvem e servidores físicos), desenvolvimento de um plano de recuperação de desastres claro, treinamento de equipa para responder a emergências, realização de testes periódicos para garantir a eficácia da recuperação.		
6.2	Execução automática de <i>backups</i>	Recuperar
	De forma a minimizar qualquer erro humano, todos os dados sensíveis da empresa deverão ser automaticamente salvaguardados de acordo com a política de <i>backups</i> definida pela empresa.	

07 Consciencialização e treino de competências

Objectivo: Na Cibersegurança, a consciencialização e o treino dos funcionários são essenciais pois o fator humano é frequentemente o elo mais fraco. Treinar a equipa aumenta a vigilância contra-ataques como *phishing* e *malware*, promove práticas seguras de uso da internet e dispositivos, e ensina a identificar e reportar ameaças. Isso fortalece a defesa geral da empresa contra incidentes cibernéticos, minimizando riscos e protegendo dados sensíveis.

Controlos

Ref.	Nome	Função de Segurança
7.1	Estabelecer um programa de Consciencialização e treino de competências	Proteger
	<p>Um programa de consciencialização e treino em Cibersegurança é crucial para educar funcionários sobre ameaças digitais e boas práticas.</p> <p>Deve ser implementado através de sessões regulares de formação, materiais de aprendizagem atualizados, simulações de ataques, e avaliações contínuas para reforçar a importância da segurança de dados e responsabilizar todos na prevenção de incidentes de segurança.</p> <p>Os temas abordados devem incluir:</p> <ul style="list-style-type: none">• Como tratar informações sensíveis (exemplo, dados de clientes)• Qualquer lei ou regulamento nacional aplicável• Como reconhecer padrões de engenharia social (exemplo, <i>phishing</i>)• Boas práticas a nível de higiene básica de informática	

08 Gestão de vulnerabilidades

Objectivo: Na gestão de vulnerabilidades, as empresas identificam, avaliam, tratam e reportam falhas de segurança em seus sistemas e software. Isso é crucial para antecipar e prevenir ataques cibernéticos, protegendo dados e infraestruturas críticas. Através deste processo, as empresas mantêm-se atualizadas contra ameaças emergentes, minimizando o risco de brechas de segurança e assegurando a continuidade das operações comerciais, além de atenderem a requisitos regulatórios e de conformidade.

Controlos

Ref.	Nome	Função de Segurança
8.1	Estabelecer um processo continuo de gestão de vulnerabilidades	Proteger
	De forma a manter os seus sistemas e ativos protegidos contra vulnerabilidades conhecidas, as empresas deverão estabelecer um processo continuo de gestão de vulnerabilidades, através da instalação de novos patches de seguranças de forma recorrente.	
8.2	Gestão de patches de sistemas operativos	Proteger
	Os sistemas operativos das empresas (tais como os de workstations, servidores, redes e VPN) deverão de forma periódica e consistente receber atualizações de segurança do fabricante. Recomenda-se que este processo seja automatizado para torná-lo mais fácil e eficiente.	
8.3	Gestão de patches de aplicações	Proteger
	As aplicações das empresas, principalmente o navegador web e ferramentas de produtividade tais como Microsoft Office, Acrobat ou outras aplicações web expostas, deverão também receber atualizações de segurança do fabricante de forma periódica e consistente. Recomenda-se que este processo seja automatizado para torná-lo mais fácil e eficiente.	

09 Proteção de dados

Objectivo: Os dados são o mais importante ativo de uma empresa. A implementação de mecanismos de proteção de dados é vital para salvaguardar informações confidenciais de clientes e da empresa contra acessos não autorizados, perda ou roubo. Isso previne danos financeiros e reputacionais, assegura a conformidade com leis de privacidade, e fortalece a confiança dos clientes. Tais medidas incluem criptografia, controle de acesso, e políticas de segurança robustas, essenciais para combater ameaças cibernéticas e manter a integridade e a disponibilidade dos dados.

Controlos

Ref.	Nome	Função de Segurança
9.1	Estabelecer um processo de gestão de dados	Identificar
	<p>A empresa deverá ter um processo de gestão de dados que esteja enquadrado com as leis nacionais de proteção de dados.</p> <p>O processo deverá estabelecer o seguinte:</p> <ul style="list-style-type: none">• Criação de um inventário de dados mais sensíveis da empresa, como informação de clientes externos.• Classificação dos diferentes níveis de confidencialidade dos dados da empresa.• Política de retenção de dados (de acordo com as leis aplicáveis)• Como descartar dados de forma segura	
9.2	Encriptação de dados em dispositivos de utilizadores	Proteger
	No caso de o dispositivo do utilizador ter sido extraviado, deverá haver mecanismos de proteção para que os dados dos dispositivos continuem seguros. Em sistemas Windows, o uso de BitLocker é fortemente encorajado.	

10 Resposta a incidentes

Objectivo: É essencial nas empresas para gerir eficazmente as consequências de um ataque cibernético ou violação de segurança. Este processo permite identificar rapidamente o incidente, limitar o dano, e restaurar os serviços normais o mais breve possível, minimizando o impacto nas operações e na reputação da empresa. Além disso, uma resposta eficaz a incidentes ajuda a analisar o ocorrido para aprender e melhorar as estratégias de segurança, evitando futuras violações e cumprindo as regulamentações legais.

Controlos

Ref.	Nome	Função de Segurança
10.1	Estabelecer um processo de gestão de resposta a incidentes	Responder
	<p>Na empresa deverá haver um processo de gestão de resposta a incidentes de Cibersegurança.</p> <p>O processo de gestão de incidentes, deverá incluir informações tais como:</p> <ul style="list-style-type: none">• Contacto(s) para reportar incidentes de segurança• Quem deverá estar envolvido em incidentes de segurança e quem será o responsável pela coordenação dos incidentes• Contactos de outros CERTs/CSIRTs que possam ser relevantes• Tipos e classificação de incidentes de segurança	
10.2	Mecanismo para reportar incidentes	Responder
	Deverá haver um mecanismo, seja telefone, distribuição de e-mail ou portal web para submissão de incidentes de segurança.	

3. Matriz de Controlos

No total, o Projecto empresa segura consiste num total de 26 controlos de segurança que as empresas deverão implementar.

Domínio	Funções de Segurança					
	Identificar	Proteger	Detectar	Responder	Recuperar	
01 Políticas corporativas	1					1
02 Gestão de Inventário	3					3
03 Gestão de contas e controlos de acesso		5				5
04 Proteção de E-mail e Web		4				4
05 Defesas anti-malware		3				3
06 Recuperação de dados					2	2
07 Consciencialização e treino de competências		1				1
08 Gestão de vulnerabilidades		3				3
09 Proteção de dados	1	1				2
10 Resposta a Incidentes				2		2
	5	17		2	2	26