

# Segurança e controlo nos SI

***Tema 7***



**BULLGUARD**



# Temas de destaque

- A vulnerabilidade dos SI
- Desafios das organizações no âmbito de Segurança dos SI
- Tipos de Ameaças
- Acções dos “hackers”
- Ciber-terroristas
- Tipo de Virus
- Medidas de prevenção
  - Backups; Autenticação do acesso; Anti-vírus; Firewalls
  - Encriptação e Disaster Recovery
- Princípios da Política de Segurança da Informação
- Soluções para evitar ameaças exteriores na Segurança de SI/TIC

# Considerações Iniciais

- Na actual Sociedade de Informação (SI) os Sistemas de Informação assumem o papel de relevo, tanto nos processos como nos objectivos do negócio nas Organizações, tornando se imperativo a sua segurança.
- A Segurança dos SI aumentou consideravelmente, exigindo a participação de todos os intervenientes nas Organizações, nos processos decisórios, estratégicos e técnicos
- Acontecimentos tais como o 11 de Setembro de 2001 nos EUA trouxeram para a ribalta a importância da segurança de de dados e Informação em situações de desastres.
- O ano de 2017 foi marcado por diversos acontecimentos no mundo da Segurança da Informação. Tivemos o enfático 12 de maio e os ataques de **Ransomware** com **WannaCrypt**, onde milhares de empresas e organizações de todo o mundo foram afetadas, além de vários outros ataques a nível mundial.

# ...Considerações Iniciais

- À medida que os serviços de Tecnologia da Informação surgem nas diversas áreas e ficam disponíveis para melhorar a vida das pessoas e das Organizações, mas também ficam vulneráveis a ataques cibernéticos das mais diferentes formas.

# ...Considerações Iniciais

## **Qual será o objectivo dos ataques cibernéticos?**

Estes ataques visam:

- causar a indisponibilidade de sistemas e serviços,
- obter acesso não autorizado,
- roubo de dados,
- propagação de códigos maliciosos em rede de computadores,

# ...Considerações Iniciais

- desconfiguração (*defacement*) - *modificação da página* de um site e podem causar prejuízo para:
  - pessoas, empresas, entidades governamentais e
  - demais usuários que utilizam serviços de tecnologia da informação.

# ...Considerações Iniciais

- **Antivírus, firewall ou anti-spam** são expressões comuns num meio dominado pelas tecnologias da informação e onde proteger os sistemas é uma necessidade que não pode ser descuidada pelos riscos que traz.
- As ameaças informáticas e os ataques às redes podem ter consequências altamente prejudiciais ao funcionamento e credibilidade das empresas, além dos elevados custos que acarretam.

# ...Considerações Iniciais

- Nn *Sniffers*, *crackers*, *spoofing*, *syn\_flooder*, *dnsskiller*, *ping o'death*, *winnuke*... nomes assustadores que parecem ter saído de filmes de horror.
- Mas na verdade são nomes de vírus indesejável que atacam os SI: os *hackers* (ou, segundo alguns preferem, *crackers*, ou ainda invasores).



# A vulnerabilidade dos SI

**Os perigos que afectam os SI podem ser descritos aos seguintes níveis:**

## ■Integridade:

- Ameaças de Ambiente (fogo, inundações, tempestades, sismos ...)
- Erros humanos
- Fraudes
- Erro de processamento



# ...A vulnerabilidade dos SI

- **Indisponibilidade:** Falhas em sistemas ou nos diversos ambientes computacionais
- **Divulgação da Informação:**
  - Divulgação de informações premeditada
  - Divulgação de informações acidental
- **Alterações não Autorizadas:**
  - Alteração premeditada
  - Alteração acidental

# ...A vulnerabilidade dos SI

- O processo de globalização, comércio eletrônico e a Internet que resulta em:
  - Fusões,
  - Disponibilidades de serviços na rede para um número diversificado de usuários,
  - Revisão e flexibilização dos processos de negócios,
  - Estreitamento dos relacionamentos com os clientes, distribuidores, fornecedores, parceiros comerciais, associados e funcionários, entre outros,
  - Internet das Coisas adiciona mais perigos nas organizações, onde a maioria desses dispositivos não está seguro desde sua concepção.
- Todos estes processos exigem maior segurança dos SI nas organizações.

# Desafios das organizações no âmbito de Segurança dos SI

Este novo cenário exige das empresas:

- Uma administração ou gestão que leve em conta os aspectos de Segurança e Negócios,
- Preservação dos maiores patrimônios (informações e negócios),
- Privacidade das informações de cada usuário, dando, ao mesmo tempo amplo, acesso aos serviços e informações disponíveis aos clientes.

# Tipos de Ameaças

- ☐ Ciber-terroristas

- ☐ Hackers

- ☐ Virus



# ...Tipos de Ameaças

## Ciber-terroristas

São aquelas que procuram causar danos às pessoas para destruir sistemas críticos ou informação. Eles servem-se da Internet como armas de destruição maciça.

## Virus

são softwares desenhados ou que se desenvolvem nos computadores, geralmente com intenção maliciosa, causar incômodo, estragos ou não. Um vírus pode ser benigno ou maligno.



# ...Tipos de Ameaças (cont.)

## Hackers

As pessoas que interferem nos computadores alheios são chamadas de “hackers”. Estes normalmente têm bom domínio da utilização de computadores e:

1. Alguns usam a sua competência para invadir computadores e prejudicar pessoas e organizações, mas
2. Outros usam a mesmas competências em benefício de SI, de suas companhias ou de terceiras pessoas para as ajudar a ultrapassar tais situações.

# Acções dos “hackers”:



- Interferem em sistemas de computadores alheios e procuram oportunidade para destruir informação ou todo o SI;
- Disconfiguram a Web site, redes internas;
- Adulteram os bancos de dados das Organizações;
- Identificam códigos (password) na Internet que possam clicar para causar danos nos sistemas ou espalhar virus;
- Fazem a espionagem nas corporações disfarçadamente;



## ...Ações dos “hackers”

- O FBI revelou que, embora considerasse o custo do crime cibernético em cerca de US \$ 3.5 bilhões para os EUA em 2019, o número real poderia ser muito maior, porque muitas explorações e ataques passam despercebidos.
- A McAfee acredita que o custo do crime cibernético em todo o mundo é de cerca de US \$ 1 trilhão por ano, representando cerca de 1% do PIB mundial.

## ...Acções dos “hackers”

- De acordo com a IBM, o custo médio de uma violação de dados era de cerca de US \$ 3.68 milhões em 2020. Em 2021, esse custo acelerou para US \$ 3.61 milhões so em ambientes de nuvem híbrida.
- O que torna os custos das violações de dados ainda maiores é que o tempo médio para identificar uma violação costuma ser em torno de 287 dias ou mais.

# Tipo de Virus



## Benignos

Ostentam uma mensagem no ecrã ou que regularmente passa no computador, para alertar, sem contudo causar estragos.

## Malígnos

Destroem ou corrompem os directórios, documentos, bases de dados e podem danificar o próprio hardware entre outros.

# ... Tipo de Virus

## **Worm**

É um tipo de vírus que se espalha de um documento para outro e de computador para computador através dos e-mails e outros traficos na Internet.

## **DoS attacks**

Infestam o Web site de muitas perguntas de modo que acaba se tornando lento ou até pode avariar.

O objectivo de **DoS attacks** é evitar que um legítimo usuário dum determinado SI possa continuar a aceder ao destino final.

# Medidas de prevenção

De entre várias formas podemos destacar:

## Backups

Um Backup é a realização de cópias da informação armazenada no computador. Nenhuma acção pode ser tão simples e básica como elaborar a(s) cópia(s) de uma determinada informação importante metódicamente e de forma regular (pelo menos uma vez por semana).

## Software de Anti-vírus

Detectam e removem ou colocam em quarentena os vírus que infectam os computadores ou SI.

Novos vírus são criados diariamente e cada nova geração mais resistente que a anterior. Logo o anti-virus precisa periodicamente ser actualizado para estar a altura dos novos vírus.

# ...Medidas de prevenção (cont.)

## Firewalls

É um hardware e/ou software que protege o computador ou rede de intrusos. O Firewall examina cada mensagem que pretende entrar na rede, como uma espécie de guarda fronteira examinando a entrada de estrangeiros. A não ser que a mensagem tenha um dispositivo que bloqueia a detensão de elemento estranho.

Um bom Administrador de redes irá sempre ter um firewall na sua rede para evitar “intrusos”

## Autenticação do acesso

Permite o acesso de usuários autorizados ao sistema ou à determinados compartimentos através de um sistema de autenticação que verifica se o usuário está autorizando antes de aceder ao sistema.

**Existem três formas de fazer isso:**

- (1) O password;
- (2) O cartão ATM;
- (3) Através de características registadas (uma impressão, ou outras características físicas da pessoa).

## ...Medidas de prevenção (cont.)

### Encriptação

Consiste em proteger uma mensagem ou documento escondendo-a espiões visuais através da codificação. Sinais visuais ou ortográficos que só podem ser decifrados por quem os conhece.



# Disaster Recovery/ Recuperação em caso de Desastres

- Antes de avançar vejamos o que se entende por Disponibilidade quando falamos em servidores, é portanto, o tempo que o servidor fica no ar durante o ano.
- Neste contexto, existem dois aspectos principais a considerar quando se ter a disponibilidade desejável: **Prevenção e Disaster Recovery.**



# ...Disaster Recovery

- Refere-se a habilidade de uma infra-estrutura recuperar todos os arquivos, programas e sistemas operacionais instalados, depois que acontece um desastre.
- É também a capacidade de responder a uma interrupção dos serviços ao implementar um plano de "Disaster Recovery", a fim de restaurar as funções fundamentais de negócio e de uma companhia.

# ...Disaster Recovery

Algumas acções de **Disaster Recovery** podem ser:

## Implementação de sistemas redundantes -

Onde um ou mais servidores possam assumir as responsabilidades do Primary Server, para que caso algum problema grave aconteça, possa-se dispor de, pelo menos, 1 ou 2 cópias exatas do banco de dados de produção colocadas em outro(s) data centers diferentes (redundância);

# ...Disaster Recovery

## Redução de pontos de falhas –

Os data centers (centro de dados) devem ser colocados em lugares estratégicos longe de terremotos, enchentes e outras fenômenos físicos e geográficos capazes de atingí-los acidentalmente.

## Planeamento e administração dos servidores -

Não basta ter redundância dos servidores é preciso testar os backups, verificar os discos e a memória, medir o desempenho e analisar a segurança.

# Plano de Disaster Recovery

- É conhecido como DRP - *disaster recovery plan*, os planos normalmente são desenvolvidos pelos gestores de ativos, muitas vezes por exigências de regulamentações internacionais como a lei Sarbanes-Oxley, Bacen 3380, ISO 27000, ou devido a exigências de acionistas ou do próprio negócio.

## ...Plano de Disaster Recovery

- O **plano de recuperação** de desastres é composto, por cenários e procedimentos, que deverão ser aplicados sempre que ocorrer uma falha devido a alguma inconsistência provocada em virtude de: ameaças como incêndios, inundações, vandalismo, sabotagem, guerra ou falhas de tecnologia.

# ...Plano de Disaster Recovery

- O DRP - *disaster recovery plan* Geralmente é composto de três fases:
  1. Programa de Administração de Crise. Plano desenvolvido em conjunto, com definição de actividade, pessoas, dados lógicos e físicos
  2. Plano de Continuidade Operacional. Possui directivas do que fazer em cada operação em caso de desastres.
  3. Plano de Recuperação de Desastres. É a aplicação na prática do plano de continuidade operacional.



# Política de Segurança da Informação

## Objectivo de uma Política de Segurança da Informação

Actualmente, a informação é o ACTIVO valioso das Empresas. Contudo, apesar da maioria do corpo executivo das Empresas estarem conscientes da necessidade da criação e cumprimento de uma Política de Segurança da Informação, torna-se necessário um grande esforço para que as Unidades de Segurança possam lançar mão dos recursos necessários para este fim e manutenção.

# Princípios da Política de Segurança da Informação

A Política de Segurança da Informação deve seguir quatro paradigmas básicas em sua composição:

- a. **Integridade:** a condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.
- b. **Legalidade:** Estado legal da informação, em conformidade com os preceitos da legislação em vigor.






# ...Princípios da Política de Segurança da Informação (cont.)

- **Confidencialidade:** propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono.
- **Disponibilidade:** Característica da informação que se relaciona directamente à possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas actividades.

# SISTEMA DE SEGURANÇA NA INTERNET



# Requisitos mínimos da Política de Segurança em Moçambique:

Requisitos	Elementos a ter em conta
Agentes envolvidos na Segurança da Informação	<ul style="list-style-type: none"><li> <b>Gestor da Informação:</b> O indivíduo responsável para tomar decisões em nome da organização no que diz respeito ao uso, à identificação, à classificação, e à proteção de um recurso específico da informação</li><li> <b>Custodiante:</b> Agente responsável pelo processamento, organização e guarda da informação.</li><li> <b>Usuário:</b> Alguma pessoa que interage diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.</li></ul>




# ...Requisitos mínimos da Política de Segurança em Moçambique:

Requisitos	Elementos a ter em conta
Classificação de Informações	<p>Classificar todas as informações críticas segundo o seu grau de criticidade e teor:</p> <ul style="list-style-type: none"><li>🖥️ Informações Confidenciais: Devem ser disseminadas somente para empregados nomeados</li><li>🖥️ Informações Corporativas: Devem ser disseminadas somente dentro da Empresa</li><li>🖥️ Informações Públicas: Podem ser disseminadas dentro e fora da Empresa</li></ul>
Política de Acesso físico	<ul style="list-style-type: none"><li>🖥️ Controle de acesso físico</li><li>🖥️ Monitoração de ambientes</li></ul>

# ...Requisitos mínimos da Política de Segurança em Moçambique:

Requisitos	Elementos a ter em conta
Política de uso da Internet	<ul style="list-style-type: none"><li>🖥️ Acesso de Empregados ao Provedor Corporativo</li><li>🖥️ Padronização da Home-Page Institucional</li><li>🖥️ Padronização da Home-Page Comercial</li><li>🖥️ Certificação</li><li>🖥️ Configuração do Firewall</li><li>🖥️ Política de Backup</li></ul>
Política de uso de software	<ul style="list-style-type: none"><li>🖥️ Controle anti-pirataria</li><li>🖥️ Definição da linha mestra dos softwares utilizados por ambiente computacional.</li></ul>

# ...Requisitos mínimos da Política de Segurança em Moçambique:

Requisitos	Elementos a ter em conta
Política de Acesso Lógico	<ul style="list-style-type: none"><li> Política de Senhas e Userid</li><li> Log de Eventos Mínimos nas transações (Dia e hora do acesso; Endereço eletrónico de quem acessou; Ações executadas)</li><li> Definição de perfis de acesso aos ambientes e aplicativos.</li></ul>

# Soluções para evitar ameaças exteriores na Segurança de SI

- O sucesso de uma empresa está em muito associada à capacidade de preservar a confidencialidade das suas informações e de proteger a sua rede de ataques exteriores; este é um dos desafios das organizações que dependem de sistemas informáticos e de telecomunicações.
- A introdução de um Sistema de Gestão de Segurança da Informação (Information Security Management System - ISMS) tem como objectivo estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação, numa perspectiva organizacional e de protecção global.



# Malha de Segurança

Actualmente, uma arquitetura de malha de segurança cibernética (CSMA) ajuda a fornecer uma estrutura e postura de segurança comum e integrada para proteger todos os ativos, sejam eles locais, em Data Centers ou na Nuvem.



# Conclusão

Já falamos muito da prevenção de perda de informação. Todavia importa recordar que:

- Com as inúmeras vulnerabilidades a que o ambiente de TI/SI está sujeito, torna-se difícil prever quando algum sistema entrará em colapso.
- Os calpsos afectam não só a produtividade por ter máquinas paradas, mas também as empresas correm o risco de perder dados importantes em discos corrompidos.

*Mesmo tomando todas as precauções até aqui referidas e outras, desastres acontecem e um plano de emergência deve ser criado antes que isso ocorra.*

# ...Conclusão

- Recordando a história do Titanic? Ele tinha 16 compartimentos à prova d'água e teoricamente, mesmo que 4 compartimentos inundassem ele não afundaria e mesmo assim afundou.
- Se tivesse botes salva-vidas para todos, ninguém teria morrido e esse é o objetivo de quem trabalha com servidores, mesmo que uma catástrofe aconteça, é necessário ter recursos para recuperar os servidores e disponibilizar os dados.

## ...Conclusão



- As soluções de segurança devem possibilitar a gestão constante de riscos e a redução dos impactos de falhas no sistema, garantir que são cumpridos os requisitos regulatórios em conformidade com a legislação vigente no País, manter a credibilidade das organizações junto dos clientes, entre outros.
- O cumprimento destes requisitos obriga à adopção de políticas de segurança que promovam a **confidencialidade** - a informação é acessível apenas a quem tem autorização para o fazer - a **veracidade** e encadeamento dos dados e a acessibilidade, por forma a que as informações estejam acessíveis de forma rápida e completa a todos aqueles que delas precisem.

## ...Conclusão

A melhor solução para segurança dos SI/TIC é a **Prevenção**, consubstanciada nas medidas que nós adoptamos para reduzir o risco de uma catástrofe incluindo pessoas, processos e tecnologias.

Mas devemos estar cientes de que não existe 100% de segurança em nenhuma actividade humana.



**MUITO OBRIGADO**