UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
LICENCIATURA EM ENGENHARIA INFORMÁTICA
Administração e Segurança de Sistemas de Informação

TEMA: Introdução a Segurança de Informação

Grupo Docente:

- Engº. Ivone Cipriano
- Engº. Délcio Chadreca

Tópicos da Aula

- Introdução
- Segurança de Informação e Ciberespaço
- Activos
- Vulnerabilidades
- Ameaças
- Ataques
- Gestão de Risco
- Padrões de Segurança de Informação

Introdução

Nas organizações contemporâneas, testemunhamos uma mudança de paradigma significativa. Os tradicionais "colaboradores", que antes recebiam informações passivamente, deram lugar aos "usuários", elementos activos que participam activamente dos processos e sistemas de informação. Isso ocorre à medida que os sistemas de informação se tornam mais flexíveis e se adaptam às inovações tecnológicas.

Nesse cenário dinâmico, as organizações precisam adoptar uma postura proactiva em relação à segurança de informação.

Comportamentos inactivos **não são mais aceitáveis**, visto que vivemos uma era de transição, marcada pela interacção contínua e pela conectividade, impondo desafios à área de segurança da informação.

Cont.

A gestão da segurança da informação se tornou uma actividade essencial para proteger a **integridade, disponibilidade e confidencialidade (CIA)** dos dados, desempenhando um papel estratégico na tomada de decisões.

A informação é **fundamental** para a competitividade e sobrevivência das organizações, sendo a **gestão da segurança da informação crucial** para garantir a protecção dos activos informacionais e/ou tecnológicos no ambiente empresarial contemporâneo.

Dilema

Como controlar, proibir e gerir essa infinidade de recursos dentro da organização sem limitar, endurecer e gerar conflitos?

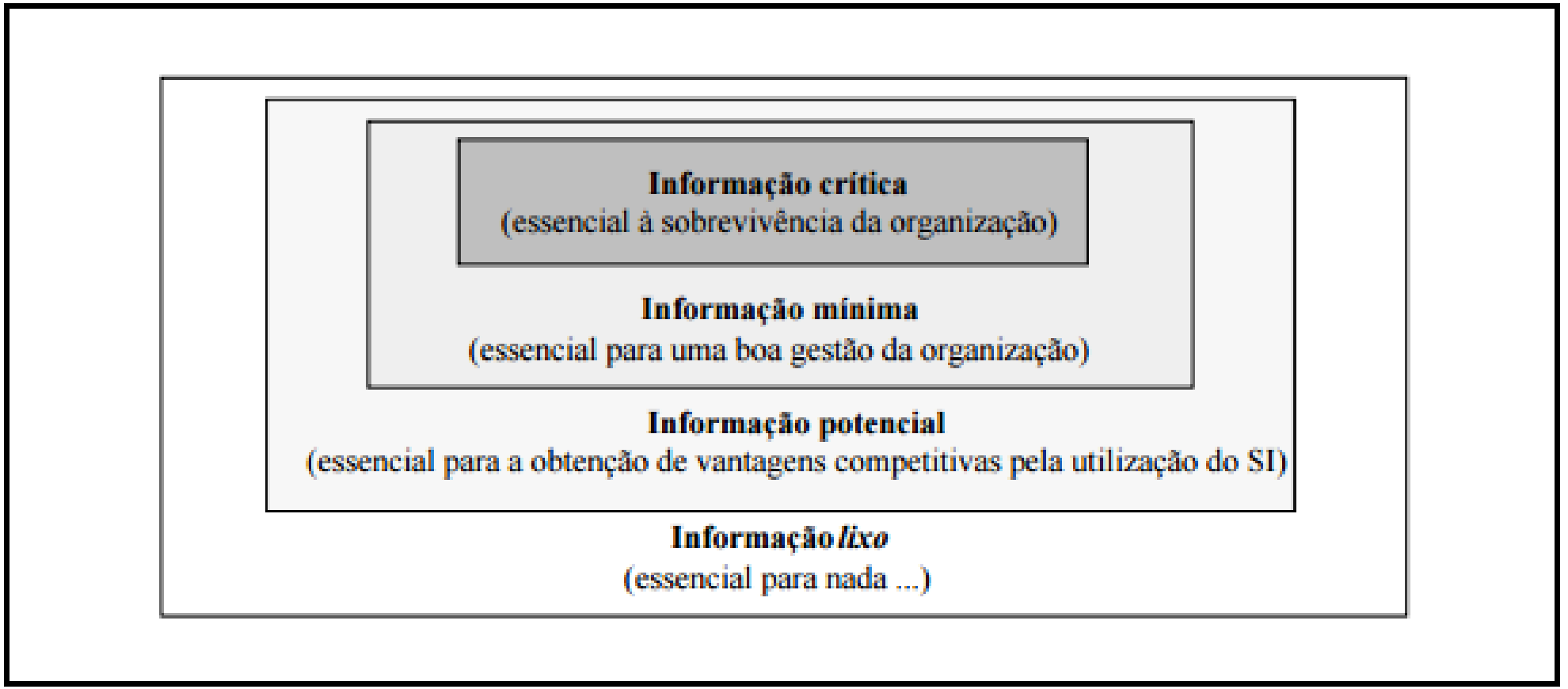
Como garantir um ambiente informacional seguro, considerando a evolução tecnológica e da sociedade?

Informação

Segundo Nakamura e Geus (2002), “a informação é um activo que, como qualquer outro activo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida”.

Pode existir em diversos meios, ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio por meios electrónicos e apresentada em filmes ou dita em conversas (ABNT NBR ISO/IEC 27002, 2013).

Classes de informação nas organizações



Fonte: Amaral (1994)

Cont.

Actualmente é visível uma enorme quantidade de recursos tecnológicos sendo introduzidos no ambiente de trabalho, como redes sociais, aplicativos móveis, plataformas de colaboração e ferramentas de mensagens instantâneas.

Isso ocorre devido aos vários benefícios que essas tecnologias trazem, como maior agilidade, produtividade e capacidade de solucionar problemas no ambiente corporativo.

No entanto, em alguns casos **se não a maioria**, observa-se uma falta de atenção às diversas ameaças e vulnerabilidades que essas ferramentas podem trazer consigo.

Segurança de Informação

A segurança de informação é caracterizada pela aplicação adequada de dispositivos de protecção sobre um activo ou um conjunto de activos, visando preservar o valor que este possui, para as organizações.

A implementação de medidas de protecção objectiva preserva as propriedades de confidencialidade, integridade e disponibilidade (CIA) dos dados, os quais não se limitam exclusivamente a sistemas e aplicações, mas também abrangem informações armazenadas ou transmitidas por meio físico ou electrónico. (Bastos & Caubit, 2009).

Cont.

A segurança da informação é um dos pilares fundamentais na era digital em que vivemos. Ela envolve a proteção de dados, sistemas e redes contra ameaças, sejam elas acidentais ou intencionais. Em um mundo cada vez mais interconectado e dependente da tecnologia, a segurança da informação desempenha um papel crucial na preservação da integridade, confidencialidade e disponibilidade dos ativos de informação Trade CIA.

Tipton e Micki Krause, define a segurança da informação como "a proteção da informação contra riscos para garantir a continuidade do negócio, minimizar danos económicos e maximizar o retorno dos investimentos e as oportunidades de negócio.“

Cont.

Bruce Schneier, destaca a crescente complexidade das ameaças à segurança da informação na era digital e a necessidade de se adoptar uma abordagem proactiva para enfrentar esses desafios. Schneier ressalta a importância de considerar a segurança da informação como um **processo contínuo e não apenas um produto ou uma solução pontual.**

Pilares de Segurança de Informação

Pilares da Segurança de Informação	Definição
Confidencialidade	Garantia de que o acesso à informação é restrito aos seus usuários legítimos (Beal, 2008).
Integridade	Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais (Sêmola, 2003).
Disponibilidade	Garantia de que a informação e os activos associados estejam disponíveis para os usuários legítimos de forma oportuna (Beal, 2008).
Autenticidade	Garantir que um usuário é de fato quem alega ser (Lyra, 2015).
Não-Repúdio	Capacidade do sistema de provar que um usuário executou uma determinada ação (Lyra, 2015).
Legalidade	Garantir que o sistema esteja aderente à legislação (Lyra, 2015).
Privacidade	Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (Lyra, 2015).
Auditoria	Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque (Lyra, 2015).

Espaço Cibernético

De acordo com a definição do Departamento de Defesa norte-americano (*DoD*), o ciberespaço é um domínio global que faz parte do ambiente de informação e que é composto por uma infra-estrutura de tecnologia da informação. Essa infra-estrutura inclui a Internet, redes de telecomunicações, sistemas de informação e sistemas computacionais com processadores e controladores.

O governo de Moçambique considera o ciberespaço como um ambiente complexo, que envolve valores e interesses, caracterizado como uma área de responsabilidade colectiva, resultante da interacção entre pessoas, redes e sistemas de informação (BR n°253, 2021). De forma mais ampla, o ciberespaço é entendido como um novo espaço estratégico compartilhado por países, organizações e pessoas.

Activo

È qualquer elemento de valor para uma organização, seja humano, tecnológico ou software, como, por exemplo, banco de dados, softwares, equipamentos (computadores e notebooks), servidores, elementos de rede (roteadores, switches, entre outros), pessoas, processos e serviços.

O autor Sêmola (2012) o define como “todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada e os equipamentos em que é manuseada, transportada e descartada”

Tipos de Activos

A norma ABNT NBR ISO/IEC 27005: 2011 sugere a distinção entre activos primários e activos de suporte e infraestrutura.

Os primários são as informações, os processos e as actividades de negócio.

Suporte compreendem os meios em que os primários se apoiam e podem ser agrupados em: hardware, software, rede, recursos humanos, instalações físicas e estrutura da organização

Cont.

É de extrema importância que a organização conheça seus activos tangíveis e intangíveis, classifique-os e lhes atribua responsabilidades pelos activos.

Isso poderá diminuir as chances de que a segurança desses activos seja comprometida.

Para isso, é necessário que seja realizado um inventário dos activos e, para cada activo identificado, seja definido seu proprietário, que ficará encarregado de manter os controles de segurança.

Vulnerabilidade

Segundo Sêmola (2012 Vulnerabilidade é a fragilidade de um activo ou grupo de activos, que pode ser explorada por uma ou mais ameaças.

As vulnerabilidades são falhas que, por si sós, não provocam incidentes, pois são elementos passivos que dependem de um agente causador ou favorável que a explorem tornando-as ameaças para a segurança da organização

As organizações devem conhecer e controlar as meaças a seus activos informacionais, pois, quando as vulnerabilidades são exploradas elas, podem gerar impactos de proporções imensuráveis.

Tipos de Vulnerabilidades

Físicas - Falta de medidas anti-incêndio e acesso não autorizado a locais sensíveis.

Naturais - Riscos ambientais próximos a equipamentos electrónicos.

Hardware - Componentes defeituosos ou inadequadamente protegidos.

Software - Erros na codificação e configuração que podem levar a problemas de segurança.

Mídias - Perda ou danos a meios de armazenamento de dados.

Comunicação - Vulnerabilidades na infraestrutura de comunicação.

Humanas - Falta de treinamento, má-fé ou descontentamento de funcionários.

Ameaças

Uma ameaça é qualquer evento que explore as vulnerabilidades e lhes atribui a causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização.

Para Dias (2000), “é um evento ou atitude indesejável (roubo, incêndio, vírus etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso”.

Segundo Sêmola (2012), “são agentes ou condições que causam incidentes que comprometem as informações e seus activos, por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização”

Grupos de Ameaças

As ameaças podem ser classificadas em três grupos:

- **Naturais** – que são as decorrentes de fenómenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.
- **Involuntárias** – são as ameaças inconscientes, quase sempre causadas pelo desconhecimento, como acidentes, erros, falta de energia, entre outros.
- **Voluntárias** – são as ameaças propositais, causadas por agentes humanos, como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador e incendiários.

Ataques

Os ataques relacionados à segurança da informação podem ser destinados a qualquer uma de suas dimensões e são uma ameaça que, quando bem-sucedida, causa uma acção danosa à organização.

Segundo Coelho et al (2014) “o ataque é um acto deliberado de tentar se desviar dos controles de segurança, com o objetivo de explorar as vulnerabilidades”

Formas de Ataques

Passivos – baseados em escutas e monitoramento de transmissões, com o intuito de obter informações que estão sendo transmitidas.. Ataques dessa categoria são difíceis de detectar porque não envolvem alterações de dados, todavia podem ser prevenidos com a utilização de criptografia.

Activos – envolvem modificação de dados, criação de objectos falsificados ou negação de serviço e têm propriedades opostas às dos ataques passivos. São difíceis de ser prevenidos, devido a necessidade de proteger completamente todas as facilidades de comunicação e processamento, durante o tempo todo. Assim, é possível detectá-los e aplicar uma medida para recuperar prejuízos causados.

Tipos de Atques

Engenharia Social: Visa enganar pessoas para obter informações confidenciais.

Negação de Serviço (DoS e DDoS): Busca interromper serviços ou computadores através de sobrecarga na rede.

Phishing: Captura informações sensíveis por meio de fraudes electrónicas, geralmente via e-mail ou sites falsos.

IP Spoofing: Assume a identidade de outro computador usando IPs falsos.

Cont

Malware: Engloba vírus, cavalos de Tróia, adware, spyware, e outros programas maliciosos.

Ataques de Força Bruta: Tenta descobrir senhas exaustivamente por meio de criptoanálise.

Ransomware: Esse tipo de malware criptografa os arquivos do usuário e exige um resgate para descriptografá-los. Se o resgate não for pago, os dados permanecem inacessíveis.

Ataque de Injeção de SQL: Os invasores inserem comandos SQL maliciosos em campos de entrada de dados para explorar vulnerabilidades de segurança em bancos de dados e obter acesso não autorizado.

Cont.

Ataque de dia zero: Esse tipo de ataque explora vulnerabilidades de segurança desconhecidas, antes que os desenvolvedores tenham uma solução ou actualização para corrigi-las.

Ataque de Man-in-the-Middle (MitM): Os invasores se posicionam entre a comunicação de duas partes e interceptam ou alteram os dados transmitidos.

Ataques de Buffer Overflow: Os invasores inserem mais dados do que o buffer pode manipular, levando a falhas no sistema ou possíveis execuções de código malicioso.

Engenharia Reversa: Os atacantes descompilam ou desmontam aplicativos para entender seu funcionamento interno, frequentemente visando encontrar vulnerabilidades ocultas.

Cont.

Pharming : Os atacantes redirecionam o tráfego da web para sites falsos com o objetivo de coletar informações confidenciais.

Ataque por Força Bruta: Tentativas repetidas são feitas para adivinhar senhas ou chaves criptográficas usando um método de tentativa e erro.

Ataque de Insider: Um ataque conduzido por alguém com acesso legítimo a uma organização, como funcionários, para causar danos internos.

Gestão de riscos

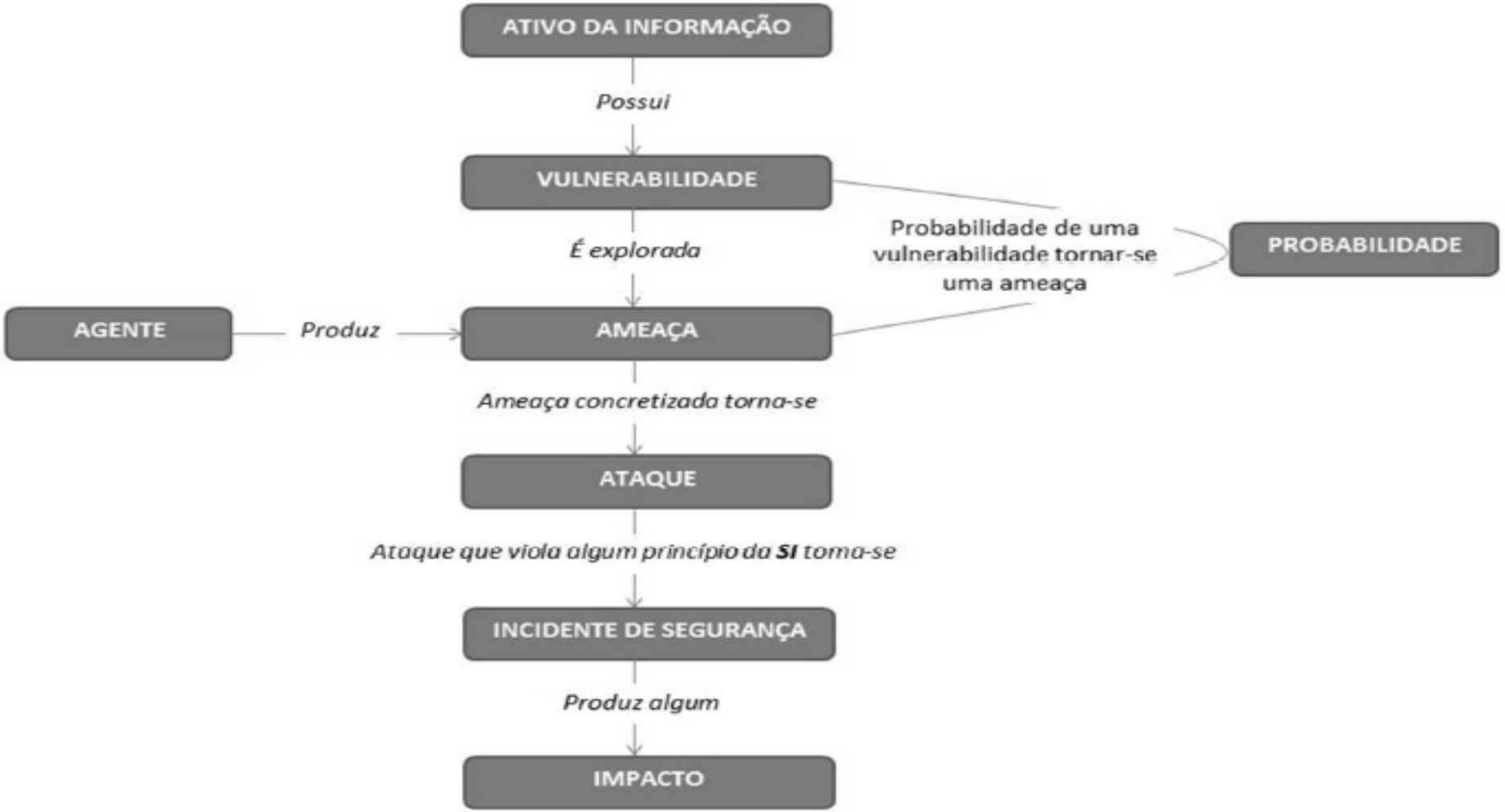
Riscos de segurança da informação "é a possibilidade de determinada ameaça explorar vulnerabilidades de um activo ou conjunto de activos, causando impactos negativos a organização".

Elementos cruciais para entender e executar a gestão de riscos: activos, ameaças, vulnerabilidades e **impacto.**

Lyra (2015) define **probabilidade** como sendo a possibilidade de uma falha de segurança acontecer, observado-se o grau de vulnerabilidade encontrada nos activos e as ameaças que porventura venham a influenciá-lo

Impacto é uma mudança adversa no nível obtido dos objectivos de negócios, que pode se manifestar em diversos âmbitos, tais como prejuízo financeiro, de reputação, de produto etc.

Risco de Segurança de Informação



Padrões ou Framework de Segurança Cibernética

Actualmente, a indústria da segurança cibernética tem, ao seu dispor, diversos modelos, padrões e/ou *framework*, desde genéricos aos específicos, isto é, ajustados a cada indústria. Um dos padrões bem conhecido é o IEC/ISO 27001, composto por mais de 100 controlos, para garantir a segurança de informação, nas componentes físicas, lógica e humana ou cognitiva.

Entretanto, embora o padrão ISO/27001 seja altamente robusto, o governo dos Estados Unidos da América, no ano de 2014, desenvolveu um modelo denominado NIST-800, que tem como função nuclear proteger todo o tipo de organizações, de ataques cibernéticos.

ISO 27001

É a norma para segurança de computadores da Organização Internacional de Padronização, que descreve como gerir a segurança da informação, em uma empresa. É baseado no ciclo de melhoria contínua, proposto por Deming (Plan, Do, Check, Act - PDCA), que implica que um sistema de gestão da informação baseado nessa norma é dinâmico, pois está sendo verificando continuamente. (Calder & Watkins, 2008).

De acordo com a ISO/IEC 27001 (2018), os controlos da norma ISO 27001 são agrupados da seguinte maneira:

- Política de segurança da informação
- Organização de segurança da informação
- Segurança em recursos humanos
- Gestão de Activos
- Controles de acesso
- Criptografia
- Segurança física e ambiental
- Segurança das Operações
- Segurança nas comunicações
- Conformidade
- Aquisição, desenvolvimento e manutenção do sistema
- Relações com fornecedores
- Gestão de incidentes de segurança da informação
- Aspectos de segurança da informação, para gestão de continuidade de negócios

NIST: Padrões e Directrizes para a Segurança Cibernética

É uma metodologia de gestão de riscos, fornecida como um guia, desenvolvida pelo Departamento de Comércio do Governo dos Estados Unidos. O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) implementou o guia de Segurança da informação para pequenas empresas, que visa fornecer recomendações de segurança cibernética básica para empresas, através de um processo de avaliação de risco (NIST, 2012).

“Principais” Controles

- Políticas de segurança da informação
- Mecanismo de Segurança em recursos humanos
- Mecanismo de Criptografia
- Mecanismos de segurança física e do ambiente
- Mecanismos de segurança, nas operações
- Mecanismos de segurança, nas comunicações
- Mecanismos de aquisição, desenvolvimento e manutenção de sistemas
- Aspectos da segurança da informação, na gestão da continuidade do negócio
- Mecanismos de conformidade Legal

Defesa de Perímetro $vs.$ Defesa em Profundidade

A segurança pressupõe uma atitude defensiva, que pode ser aplicada segundo duas politicas:

- **Defesa de Perímetro**: consiste em definir uma linha que delimita um espaço englobando um conjunto de computadores e redes e evitar interacções indesejáveis entre os dois lados (espaços) dessa linha de delimitação.

  Mas a defesa em perímetro pode ir mais longe, considerando a defesa contra abusos de utilizadores que estão dentro do espaço delimitado pelo perímetro.

  Assim, defesa de perímetro serve fundamentalmente para restringir as interacções entre domínios de segurança.
- **Defesa em Profundidade**: esta politica segue a estratégia mais complexa que se preocupa com todos os níveis de segurança, e não com domínios. A defesa em profundidade é particularmente útil para detectar problemas internos a domínios de segurança e que foram originados internamente, ou que por alguma razão foram originados externamente ao perímetro de segurança.

Defesa em Perímetro:

- Foca em proteger um perímetro ou fronteira específica, como uma cerca, parede ou firewall, contra ameaças externas.
- A ideia central é impedir que ameaças cruzem essa fronteira e acessem o interior do sistema ou rede.
- É mais tradicional e foi amplamente usada em estratégias de segurança física e na segurança de redes **no passado**.
- Pode ser eficaz para evitar ataques iniciais, mas não lida tão bem com ameaças que já estão dentro do perímetro.

Defesa em Profundidade:

- Baseia-se na ideia de que não se deve confiar apenas em uma única barreira de segurança. Em vez disso, várias camadas de segurança são implementadas em diferentes níveis do sistema ou rede.
- Cada camada é projetada para detectar e responder a ameaças de maneira independente.
- Caso uma camada seja comprometida, outras camadas de segurança podem continuar a proteger o sistema.
- É uma estratégia mais moderna e é amplamente usada em segurança de TI, segurança cibernética e também em estratégias de defesa militar.
- Proporciona uma abordagem mais resiliente e adaptável contra ameaças, especialmente aquelas que já estão dentro do perímetro inicial.

Engenharia Social e a Humanização dos Firewalls

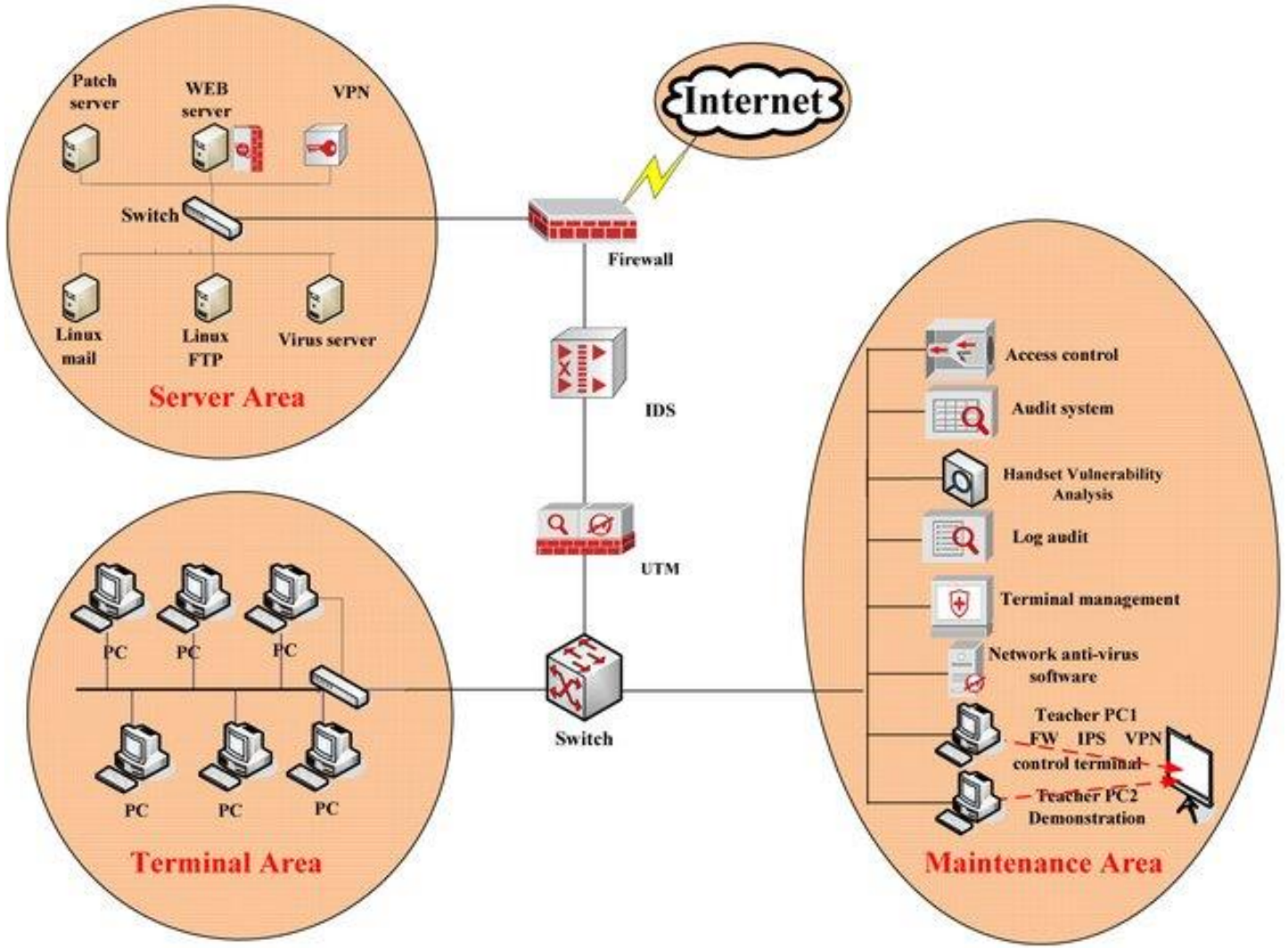
A *firewall* humana surge como resposta aos ataques de engenharia social. Com efeito, para proteger a privacidade contra os ataques dos "engenheiros sociais", a melhor abordagem para as organizações é capacitar as suas equipas no uso adequado das políticas de segurança.

Segundo Pereira (2022), uma *firewall* humana é a linha de defesa que as pessoas constituem, para combater as ameaças à segurança de uma organização. Enquanto uma firewall tecnológica regula o tráfego digital, em uma rede, uma firewall humana actua como uma camada de protecção humana

Principais Ataques Cibernéticos no Ciberespaço Moçambicana

Tipo de Ataque	Potencial Vítima	Descrição
Web Defacement	Instituições	Troca de conteúdo de páginas web
Ramsonware	Instituições	Sequestro de informações
Negação de Serviço	Geral	Indisponibilidade de serviços
Phising	Cidadãos	Roubo de senhas de utilizadores
Simbox	Cidadãos	Chamadas Internacionais mascaradas em chamadas internas
Simswaps	Cidadãos	Troca de cartões sim
Fake News	Cidadãos	Desinformação ou disponibilidade de informação falsa
Cryptojacking	Cidadãos	Uso abusivo de poder de processamento do computador, a partir de um malware em um navegador

Ecosistema corporativo contemporâneas



OBRIGADO !!!