UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
LICENCIATURA EM ENGENHARIA INFORMÁTICA
REDES DE COMPUTADORES I

TEMA: Introdução a Segurança de Informação

Grupo Docente:

- Engaº. Ivone Cipriano
- Engº. Délcio Chadreca

Tópicos da Aula

- Conceitos
- Vulnerabilidade, Ameaças e Risco
- Métodos de Ataques
- Medidas de Segurança
- Normas e regulamenta
- A importância da conscientização dos usuários
- Gestão de incidentes de segurança

Introdução

A história da segurança da informação está directamente ligada à evolução da tecnologia da informação e da computação. As primeiras preocupações com a segurança da informação surgiram no contexto militar, durante a Segunda Guerra Mundial, quando os alemães criaram a máquina de criptografia **Enigma** para enviar mensagens secretas.

Os Aliados, por sua vez, desenvolveram a máquina Colossus para decifrar essas mensagens.

Cont.

Na década de 1990, com a popularização da Internet, a segurança da informação se tornou um desafio ainda maior, já que a rede mundial de computadores trouxe novas ameaças, como malware, phishing e ataques de negação de serviço.

A partir daí, as empresas e governos passaram a investir mais em medidas de segurança, como firewalls, antivírus, criptografia e autenticação de usuários.

Teoria Actor Rede

A Teoria Actor-Rede foi desenvolvida entre as décadas de 1980 e 1990, a partir de estudos na área de ciência e tecnologia. Bruno Latour, Michel Callon e John Law foram alguns dos principais nomes que se dedicaram aos primeiros trabalhos na elaboração dessa teoria (Coutinho & Viana, 2019).

Underwood (1998), diz que actor-rede é um sistema de relações, trocas, alianças e negociações entre os actuantes. Actualmente, a ANT caracteriza- se como um tratamento analítico que visa compreender as relações ou associações que formam a sociedade, a partir do modelo de rede. A Teoria da Rede de Atores (ANT) enfatiza a análise da acção e dos atores que compõem as associações e agrupamentos sociais, incluindo tanto elementos humanos como não humanos.

Segurança da informação

“É a protecção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios” (ISO 27002)

Segundo Leite (2016), a segurança da informação é uma ferramenta fundamental para viabilização, manutenção e homologação da cadeia de serviços das organizações que trabalham directamente com informações sigilosas e requisitos como confidencialidade e integridade são indispensáveis para as organizações que lidam directa ou indirectamente com informações como um bem intangível.

Cont.

A norma NBR ISSO/IEC 17799 (ABNT, 2005), sublinha ainda que a abrangência da segurança da informação não se restringe apenas ao ambiente computacional, mas a todo meio envolvido na disseminação da informação

Para Lyra (2015), de uma forma simples e directa, a Informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto

Propriedades Básicas da Segurança de Informação

Pilares da Segurança de Informação	Definição
1. Confidencialidade	Garantia de que o acesso à informação é restrito aos seus usuários legítimos (Beal, 2008).
1. 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).
1. Disponibilidade	Garantia de que a informação e os activos associados estejam disponíveis para os usuários legítimos de forma oportuna (Beal, 2008).
1. Autenticidade	Garantir que um usuário é de fato quem alega ser (Lyra, 2015).
1. Não-Repúdio	Capacidade do sistema de provar que um usuário executou uma determinada ação (Lyra, 2015).
1. Legalidade	Garantir que o sistema esteja aderente à legislação (Lyra, 2015).
1. Privacidade	Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (Lyra, 2015).
1. Auditoria	Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque (Lyra, 2015).

Introdução a Segurança de Sistemas de Computadores

No âmbito da segurança de sistemas de computadores são geralmente considerados três grandes áreas de actividade:

Defesa contra catástrofe físicas:

- Catástrofes ambientais;
- Catástrofes politicas; e
- Catástrofes materiais.

Defesa para falhas/previsíveis

- Falhas no fornecimento de energia eléctrica;
- Bloqueio de execução de aplicações ou sistemas aplicativos; e
- Falhas temporárias de conectividade em troços da rede.

Cont.

Defesa contra actividades não autorizadas: As actividades ilícitas ou não autorizadas podem ser de cinco tipos:

- Acesso a informação;
- Alteração da informação;
- Utilização abusiva ou exagerada dos recursos computacionais;
- Impedimento de prestação de serviço (Denial of Service, DoS); e
- Vandalismo

Alguns Conceitos Gerais da Segurança de Informação

Vulnerabilidade: É uma característica de uma sistema que o torna sensível a certos ataques

Ataque: é um conjunto de passos executados no âmbito da exploração das vulnerabilidades de um sistema e que permitem concretizar uma acção ilícita no sistema alvo.

Risco (ou ameaça): é o potencial que uma dada ameaça ira explorar vulnerabilidade para causar perda ou danos de um activo ou grupo de activos.

Defesa: Consiste no conjunto de politicas e mecanismos desenhados, concretizados e implementados para:

- Diminuir as vulnerabilidades de um sistema;
- Detectar e contrariar/anular ataques passados ou actuais; e
- Minimizar os riscos decorrentes de ataques bem sucedidos.

Uma defesa correcta devera contemplar todas as três vertentes enunciadas e não apenas algumas.

Vulnerabilidades

Vulnerabilidades são pontos fracos, na segurança de um sistema de computador ou processo, através das quais podem surgir certos tipos de **ameaças** que podem colocar em **risco** a confidencialidade, integridade e autenticação da informação (Milagres & Steven, 2017).

- Vulnerabilidades de *Design;*
- Vulnerabilidades de configuração;
- Vulnerabilidades de implantação;
- Vulnerabilidades organizacionais;
- Vulnerabilidades tecnológicas;
- Vulnerabilidades de controlo.

Ameaça

Segundo Beal (2008), **ameaça** é definido como sendo a espectativa de acontecimento acidental ou propositado, causado por um agente, que pode afectar um ambiente, um sistema ou um activo de informação. As ameaças podem ser:

- Naturais
- Intencionais e
- Involuntárias

Métodos de Ataque a Sistemas de Computadores

Um ataque pode ser entendido como a concretização de uma ameaça, isto é, a exploração de uma vulnerabilidade

- Malware
- Ataques baseados na Web
- Phishing
- Ataques a aplicativos da Web
- SPAM
- Negação de serviço distribuída (DDoS)
- Roubo de identidade
- Violação de dados
- Ameaça interna
- Botnets
- Manipulação física, danos , Roubo e perda
- Vazamento de informações
- Ransomware
- Espionagem cibernética
- Criptojacking

Cont.

A **probabilidade** é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos activos que sustentam o negocio e o grau das **ameaças** que possam explorar estas vulnerabilidades.ao negocio da organização

O **impacto** de um incidente são as potenciais consequências que este incidente possa causar ao negocio da organização

O **risco** é a relação entre a probabilidade e o impacto organização

É a base para a identificação dos pontos que demandam por investimentos em segurança da informação.

Riscos dos Sistemas de Computadores

Riscos dos sistemas de computadores relativos aos computadores e redes que constituem o sistema.

Em relação aos computadores temos os seguintes riscos:

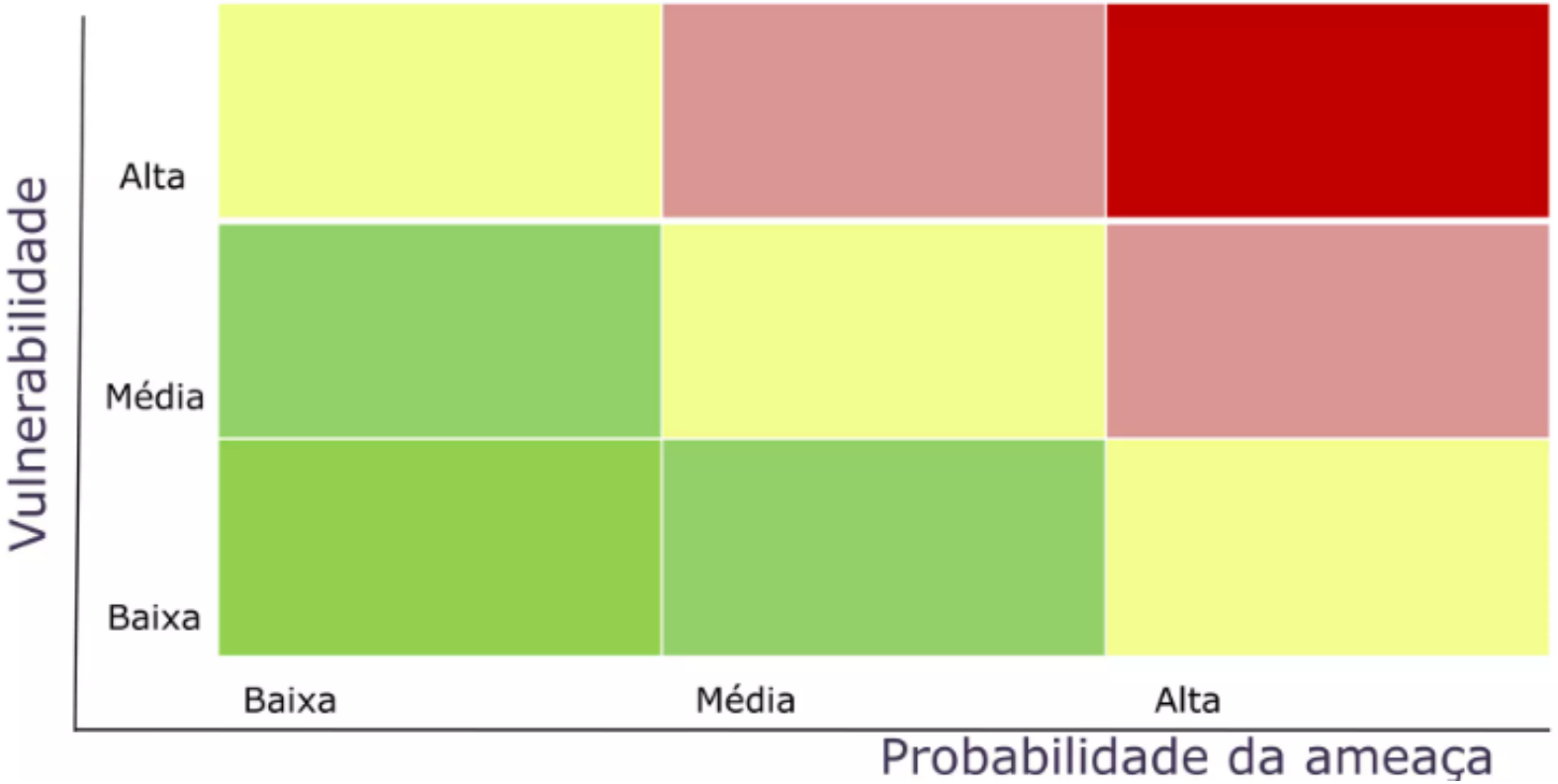
1. Intrusão;
2. Acesso a informação reservada ou confidencial;
3. Perda ou roubo de informação;
4. Personificação; e
5. Incapacidade de prestação de serviços.

Em relação as redes, temos os seguintes riscos:

1. Acesso a informação reservada ou confidencial;
2. Personificação;
3. Intercepção de fluxos de dados (ataque de interposição, *Man-in-the-middle attack*);
4. Modificação de fluxos de dados; e
5. Reprodução de fluxos de dados.

Gestão de Risco

Processo no qual os riscos são identificados, analisados e reduzidos a um nível aceitável.



Etpas da Gestão de Risco

Segundo ISSO 27005 Existem sete potencias fases:

1. Caracterização do Ambiente de TI
2. Identificação dos Riscos
3. Analise dos Controles
4. Determinação da Probabilidade do Risco
5. Analise do Impacto
6. Determinação do Risco
7. Recomendações

Complexidade do Problema da Segurança de Sistemas de Computadores

Os sistemas de computadores unidos por redes, em particular a Internet, são cada vez mais usados para guardar e manipular informação usada no dia-a-dia das pessoas e das organizações

A segurança dos sistemas de computadores é cada vez mais um problema simultaneamente **técnico e social (sócio-técnico)**.

- **Técnico** porque a multiplicidade de arquitectura de hardware, sistemas operativos e suas versões, protocolos aplicacionais e requisitos aplicacionais fazem com que a definição e implantação de politicas de segurança em sistemas distribuídos ligados a Internet seja difícil, quer de por em pratica quer de manter.
- **Social** porque a grande maioria dos utentes dos sistemas de computadores domésticos e de pequenas empresas não estão normalmente cientes dos problemas de segurança a que estão sujeitos nem qual a melhor forma de com eles lidar.

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.

Politicas *vs.* Mecanismos de Segurança

A **Politica de Segurança** define o foco de segurança e o que esta deve garantir.

Os **Mecanismos de Segurança** são tecnologias que permitem por em pratica as politicas de segurança.

Um **Domínio de Segurança** consiste num universo de recursos tecnológicos (maquinas, redes, etc.) e humanos sujeitos a mesma politica de segurança.

A definição correcta e tão complexa quanto possível da politica de segurança para sistemas de computadores é critica para a sua protecção usando os mecanismos de segurança.

Se não se souber o que interessa proteger e qual o modelo base em que se deve assentar essa protecção, não é possível conceber e implementar uma segurança adequada.

Definição de Politicas de Segurança de Sistemas de Computadores

As politicas de segurança definem fundamentalmente os requisitos de segurança que devem ser respeitados para garantir um determinado resultado. Esse resultado pode ser variado, por exemplo:

- Garantir a confiabilidade de informação reservada ou confidencial;
- Protecção de informação crítica;
- Continuidade de operações ou de prestação de serviços;
- Confiança na correcção da operação do sistema;
- Prova de correcção ou de autoria na troca de informação; e
- Capacidade de auditoria das acções passadas.

Os requisitos podem também ser vários, por exemplo:

- Autenticação de sujeitos ou serviços;
- Autorização de sujeitos ou serviços;
- Privilégios de sujeitos ou serviços;
- Monitorização e registo de actividades; e
- Auditoria de registos de actividades.

Normas de Segurança de Informação

- 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 controles, para garantir a segurança de informação, nas camadas física, lógica e humana ou cognitiva.
- 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).

PDCA

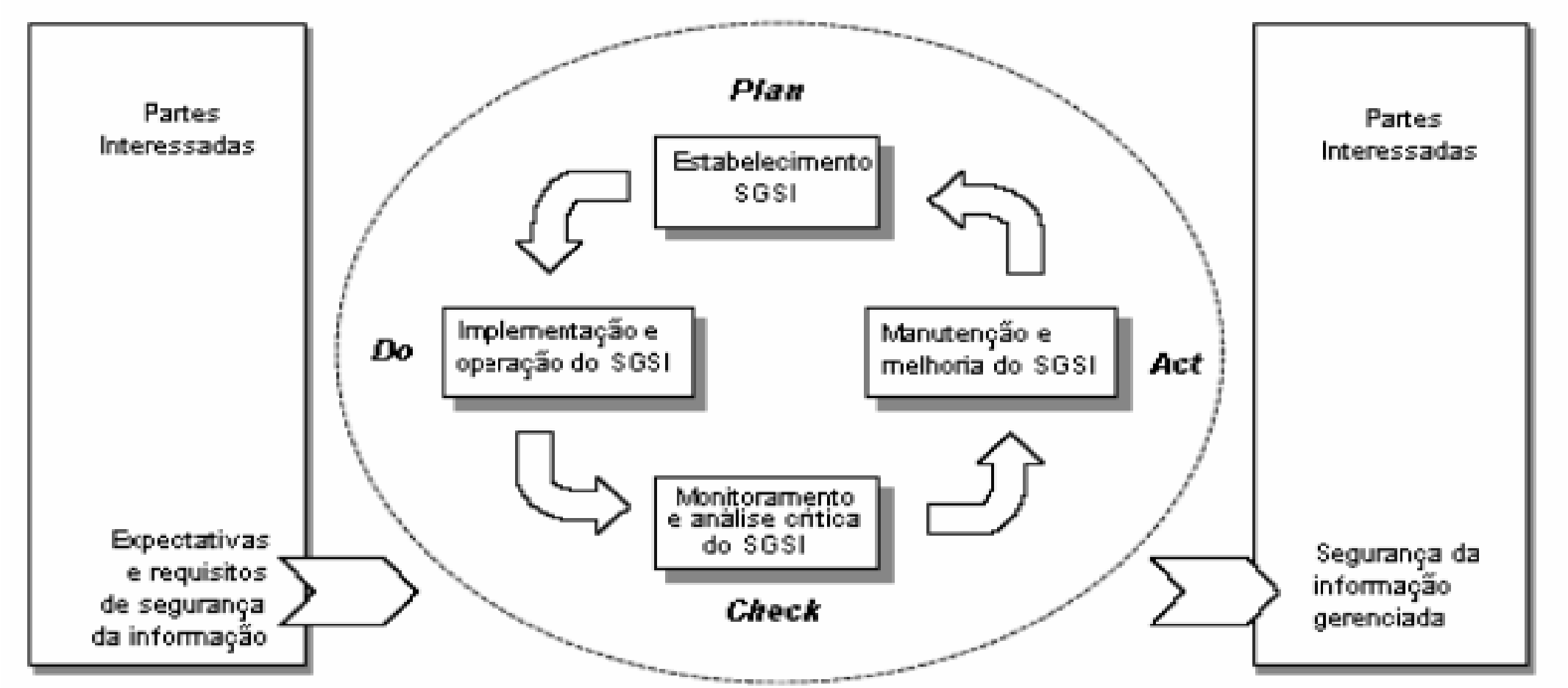
P – Planear: estabelecer os objectivos e processos necessários para fornecer resultados de acordo com os requisitos e políticas pré-determinados.

D – Fazer: implementar as acções necessárias.

C – Verificar: consiste em monitorar e avaliar continuamente os processos e produtos de acordo com as políticas, objectivos e requisitos predefinidos, e apresentar relatórios sobre os resultados obtidos.

A – Agir: executar acções para promover continuamente a melhoria dos processos.

Modelo PDCA aplicado aos processos do SGSI



Agrupamento de Controles da norma ISO 27001

A.5 Política de segurança da informação;

A.6 Organização de segurança informação;

A.7 Segurança em recursos humanos;

A.8 Gestão de Activos;

A.9 Controles de acesso;

A.10 Criptografia;

A.11 Segurança física e ambiental;

A.12 Segurança das Operações;

A.13 Segurança nas comunicações;

A.14 Aquisição, desenvolvimento e damanutenção do sistema;

A.15 Relações com fornecedores;

A.16 Gestão de incidentes de segurança da informação;

A.17 Aspectos de segurança da informação para gestão de continuidade de negócios;

A.18 Conformidade.

NIST

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).

Framework versão 1.1

Cont.

Ao fornecer uma liderança técnica, para a infra-estrutura nacional de medição e padrões, o NIST desenvolve técnicas de teste, dados de referência, implementações de teste de análise conceitual e técnica para avançar no desenvolvimento e uso produtivo da tecnologia das informações. O NIST contém o desenvolvimento de técnicas e procedimentos administrativos e de gestão para a segurança adequada e privacidade de informações sensíveis não classificados, em sistemas de computador.

Center For Internet Security Controls - CIS

O Center for Internet Security Critical Security Controls (CIS Controls) nasceu em 2018 e foi criado em cooperação com representantes do governo dos Estados Unidos da América e organizações de pesquisa de segurança do sector privado.

Os controlos CIS são um conjunto de defesas e práticas de natureza técnica destinadas a impedir os ataques cibernéticos mais comuns que podem comprometer os sistemas de informação (Cert-py, 2017).

Segundo CIS (2018), os controlos propostos pela CIS são projectados para priorizar, focar e para aproveitar o poder de uma grande comunidade de especialistas, para identificar e apoiar práticas e etapas de alto valor fundamental e para auxiliar na cibersegurança de empresas ou instituições

Controls CIS

Controlos Basicos do CIS

CSC1 - Inventário de dispositivos autorizados e não autorizados;

CSC2 - Inventário de *software* autorizado e não autorizado;

CSC3 - Configurações seguras de *hardware* e software em dispositivos móveis, laptops, estações de trabalho e servidores;

CSC4 - Avaliação e Correcção Contínua de Vulnerabilidades;

CSC5 - Uso Controlado de Privilégios Administrativos.

A importância da conscientização dos usuários

De acordo com Castells (2003), o ciberespaço é um novo espaço estratégico e comum a todos os países, organizações e pessoas. Em sua forma mais simples, o ciberespaço contempla os seguintes elementos, dentro das três dimensões do ambiente de informação global:- cognitivo, de informações e físico.

Najah (2020) ,define o ciberespaço como a interacção dinâmica de três camadas. A primeira delas refere-se à camada física, abrangendo elementos materiais, como satélites, cabos submarinos, data *centres*, telefonia fixa/móvel, dentre outros

Cont.

A segunda camada é a das aplicações, a qual inclui os sistemas operacionais, protocolos, códigos, aplicações, bases de dados etc. Por último, a camada virtual permite a utilização da infra-estrutura física, mas também a produção e circulação de conteúdos produzidos.

A terceira camada é chamada de cognitiva. Seguindo a lógica do autor, a camada individual e colectiva é o ponto de convergência das duas camadas anteriores, permitindo a produção de informações, a criação de redes sociais e a realização de discussões e intercâmbio de dados em tempo real.

Engenharia Social e Firewall Humano

Actualmente, as organizações enfrentam uma crescente quantidade de ameaças de segurança, que podem comprometer seus activos e causar prejuízos financeiros e de reputação.

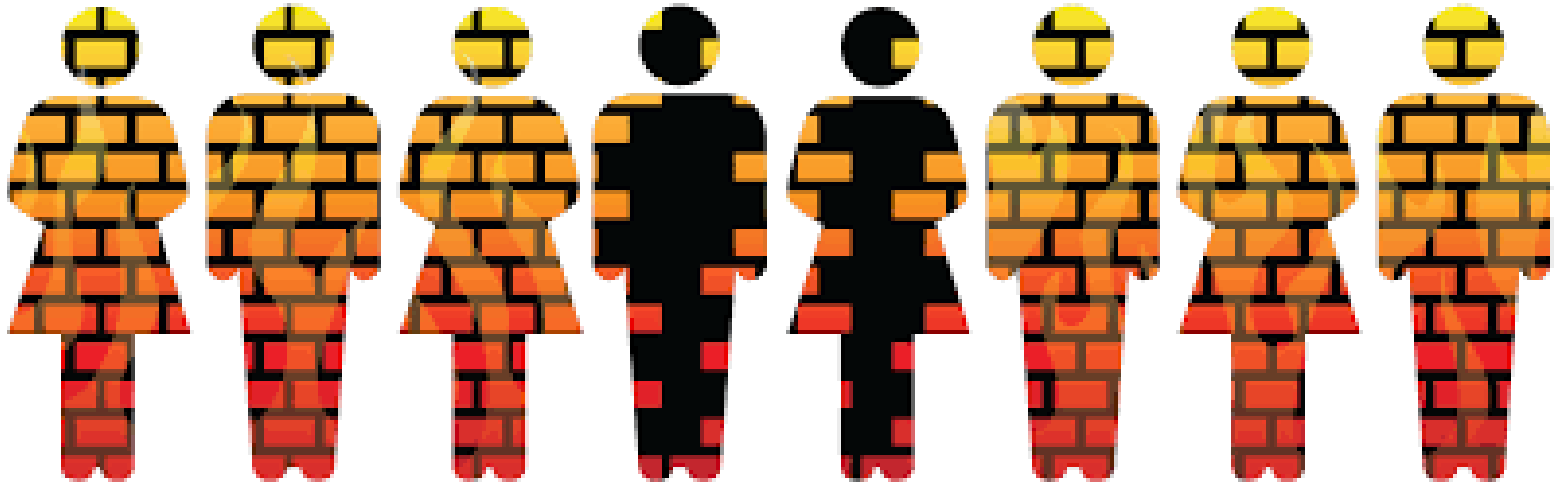
É fundamental que essas organizações adoptem medidas proactivas para mitigar os riscos de segurança e garantir a protecção de seus dados e sistemas, além de estarem preparadas para responder rapidamente a incidentes de segurança quando estes ocorrerem. Isso faz com que elas se dediquem cada vez mais à segurança de seus sistemas, investindo em mecanismos de defesa mais eficazes e avançados.

Cont.

A *firewall* humana surge como resposta aos ataques de engenharia social. 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. O objectivo principal desta formação é capacitar os usuários a se tornarem uma "firewall humana", ou seja, desenvolver habilidades e conhecimentos para aumentar a segurança digital e proteger as informações em diferentes contextos.

Cont.

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

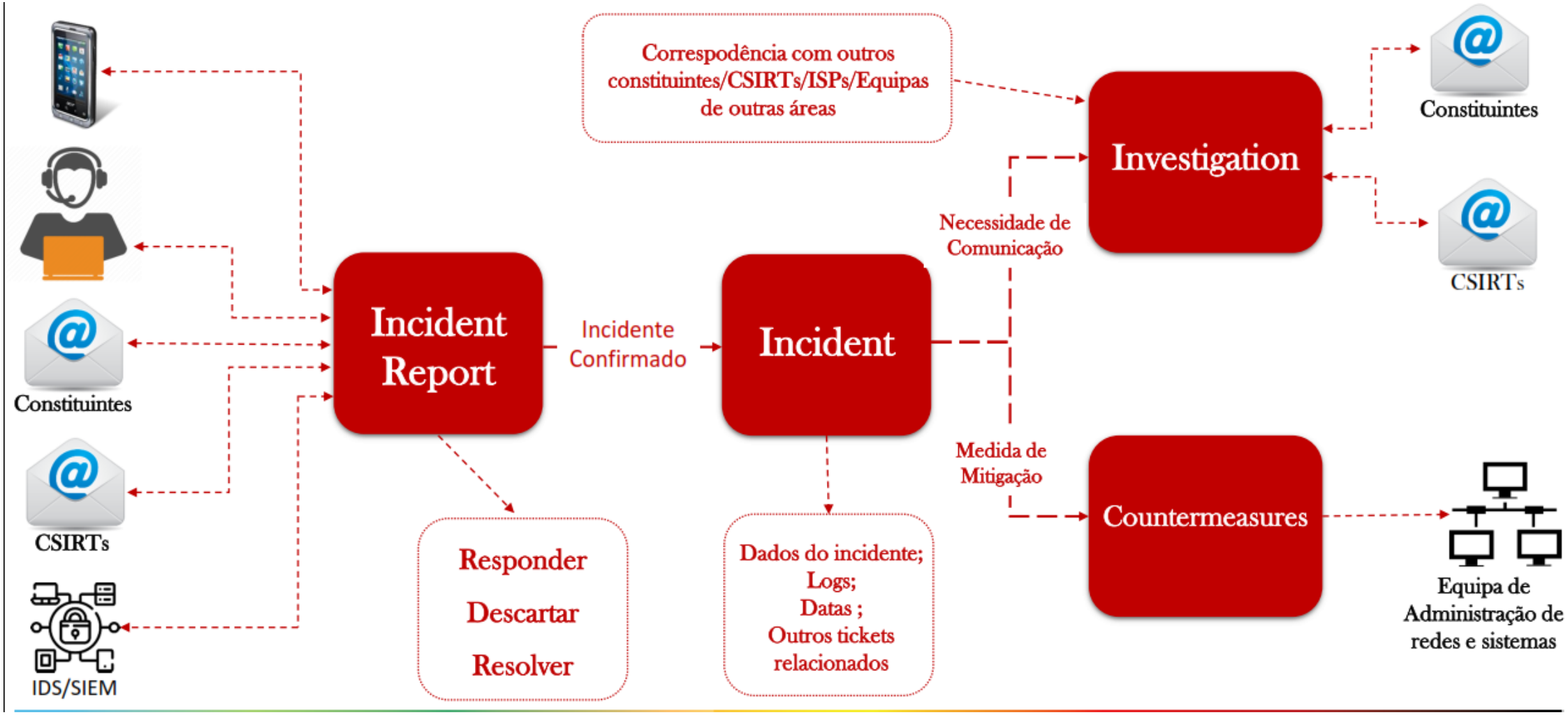


Gestão de Incidentes de SI

Consiste em gerir qualquer evento adverso indesejados ou inesperados, confirmado ou sob suspeita, que tenham a probabilidade de comprometer e ameaçar a informação.

Fonte: https://datasus.saude.gov.br/gestao-de-incidentes-de-sic/

Moçambique



Fonte: INAGE 2023

OBRIGADO !!!