Resumo de Segurança e Gestão de Risco

Segurança

- **Segurança da informação**: Proteção dos dados e informações contra acesso não autorizado, alteração, destruição ou divulgação.
- **Segurança dos Sistemas de Informação**: Inclui a segurança da informação, mas também envolve a proteção dos sistemas de hardware e software que processam e armazenam essas informações.

CIA

As três características essenciais da segurança da informação:

- **Confidencialidade**: A informação apenas deve ser acessível a quem tem permissão para tal;
- **Integridade**: A informação deve ser precisa e completa;
- **Disponibilidade**: A informação deve estar disponível quando necessária.

Conceitos base

- **Ativo**: Qualquer coisa que tenha valor para a organização (ex: informação, hardware, software, etc.);
- **Ameaça**: É qualquer ato (humano intencional ou não, ou causado por fenómenos naturais) que possa causar danos a um sistema ou organização (ex: *phishing*, *social engineering*, etc.);
- **Vulnerabilidade**: É uma fraqueza ou falha num sistema que pode ser explorada por uma ameaça;
- **Impacto**: É a consequência de uma ameaça sobre um sistema ou organização;
- **Risco**: É a combinação de ameaça com probabilidade de ocorrência e impacto, expresso em níveis acordados.

ISO 27001

Esta norma define um conjunto de controlos de segurança que devem ser implementados numa organização:

- Requisitos de um Sistema de Gestão;
- Controlos de Segurança;
- Modelo PDCA (Plan, Do, Check, Act).

Modelo PDCA

Feito por Walter Shewhart e popularizado por W. Edwards Deming, este modelo é amplamente utilizado para garantir a melhoria **contínua** em diversos tipos de **sistemas de gestão**.

É composto por quatro etapas:

- **Plan**: Definir objetivos e processos necessários para atingir resultados de acordo com as políticas da organização;
- **Do**: Implementar os processos;
- **Check**: Monitorizar e avaliar os processos;
- **Act**: Tomar ações para melhorar continuamente os processos.

Gestão de Continuidade de Negócio (BCM)

O processo de Gestão Continuidade de Negócio conduz à produção de planos e procedimentos que permitem responder a incidentes

> O standard a seguir nesta área é a ISO 22301 (normas de Sistemas de Gestão de Continuidade de Negócio).

Gestão de Risco

Avaliação de Risco

- **Identificação de Ativos**: Os ativos que precisam de ser protegidos;
- **Identificação de Ameaças**: As ameaças que podem afetar os ativos;
- **Identificação de Vulnerabilidades**: As vulnerabilidades dos ativos;
- **Análise de Risco**: Avaliar o risco associado a cada ameaça;

Existem várias formas de calcular o risco, exemplo:

- Risco = Probabilidade x Consequência x Severidade, util
- Risco = Valor_Ativo x Probabilidade x Impacto.
- Risco = Probabilidade x Impacto.

Normalmente são utilizados valores **quantitativos** (1,2,3,...) em vez de **qualitativos**, pois é mais fácil de definir prioridades.

Tratamento de Risco

Para tratar o risco, existem formas de tratar o risco:

- **Assumir o risco**: Aceitar o risco;
- **Evitar o risco**: Eliminando a causa do risco ou as consequências (desativar certas funcionalidades ou, mesmo, desligar o sistema);
- **Transferir o risco**: Transferir o risco para outra entidade (ex: seguros);
- **Planeamento de risco**: Gerir o risco, desenvolvendo um plano de mitigação que prioriza, implementa e mantem os controlos.
- **Limitar o risco**: Implementar controlos para diminuir a probabilidade de ocorrência.
- **Reconhecimento e Desenvolvimento de controlos**: À medida que as vulnerabilidades são reconhecidas, é implementado um plano de desenvolvimento e implementação de controlos que permitam corrigir ou minimizar a vulnerabilidade

> A **limitação do risco** e o **reconhecimento e desenvolvimento de controlos** são formas de tratamento de risco predominantemente **técnicas**.

Risk Mitigation Checklist

Definido por **NIST** (*National Institute of Standards and Technology*), é uma lista de controlos que podem ser implementados para mitigar o risco.

Controlos de segurança

Estes podem ser:

- **Técnicos**: *firewalls*, *antivírus*, etc.;
  - **Suporte**: *patches*, *updates*, etc.;
  - **Prevenção**: *firewalls*, *antivírus*, etc.;
  - **Deteção**: *IDS*, *IPS*, etc.;
- **Não técnicos**: Políticas, procedimentos, etc.
  - **Controlos Operacionais**: normas definidas na gestão;
  - **Controlos de Gestão e Organização**: definem como os elementos da organização devem agir.

Business Impact Analysis (BIA)

Um processo de *Business Impact Analysis* pretende **determinar os impactos que um incidente disruptivo tem** na operação e na viabilidade dos processos core de negócio.

Antes:

- Determinar os processos *core* (mais importantes);
- Determinar quais são os recursos necessários para manter esses processos.

Depois:

- Classificar esses recursos por ordem de importância;
- Caracterizar os requisitos de tempo de recuperação para cada recurso.

Requisitos de Recuperação

- **R.P.O. (Recovery Point Objective)** - O ponto até ao qual os dados podem ser perdidos;
- **R.T.O. (Recovery Time Objective)** - O tempo máximo que um sistema ~~pode estar inativo após um incidente;~~
- **W.R.T. (Work Recovery Time)** - O tempo necessário para ~~recuperar o trabalho perdido;~~
- **M.T.D. (Maximum Tolerable Downtime)** - O tempo máximo que um sistema pode estar inativo antes de causar danos irreparáveis.

GAP Analysis

GAP Analysis consiste na **comparação entre o estado presente e o estado desejado** (futuro).

Para tal é preciso resposta para:

- Qual o estado pretendido:
  - Ou estado *compliant* (em conformidade);
- Quando numa auditoria/certificação:
  - Qual o estado actual;
  - O que é preciso ser feito;

Políticas de Segurança

As políticas de segurança são um conjunto de regras que definem o que é permitido e o que não é permitido no que toca à segurança da informação, no que diz respeito à preservação da confidencialidade, integridade e disponibilidade da informação.

Políticas específicas:

- Classificação da informação;
- Uso aceitável;
- Controlo de acesso;
- Backup;
- Teletrabalho e Acesso remoto;
- Controlo criptográfico;
- Fornecedores;

Criptografia

Permite:

- Salvaguardar informação (confidencialidade);
- Proteger a confidencialidade (e.g. hackers, espiões);

Temos dois tipos de criptografia:

- **Simétrica**: A mesma chave é usada para cifrar e decifrar a informação;
- **Assimétrica**: Duas chaves são usadas, uma para cifrar e outra para decifrar;

A simétrica é mais rápida, porém envolve a partilha da chave, o que pode ser um problema. Enquanto que a assimétrica é mais lenta, mas mais segura na partilha da chave.

Hashing

É um algoritmo que transforma uma string de caracteres em uma sequência de caracteres de tamanho fixo (e.g. SHA-256).

PKI (*Public Key Infrastructure*)

Infraestrutura de gestão do "ciclo de vida" das chaves criptográficas assimétricas:

- Geração;
- Distribuição;
- Revogação;
- Renovação;
- etc.;

Isto é feito através de **certificados digitais**.

Certificados Digitais

É um documento eletrónico que contém a chave pública de um utilizador, que é usada para cifrar informação, e a identificação do utilizador.

Dentro dos sistemas criptográficos assimétricos, temos:

- **Listas de Revogação de Certificados** (CRL): Lista de certificados revogados;
- **Lista de Confiança de Certificados** (CTL): Lista de certificados confiáveis;

SSL/TLS

Protocolo de segurança que permite a comunicação segura entre um cliente e um servidor (e.g. HTTPS). A comunicação é cifrada e autenticada.

Gestão de Chaves

É o processo de geração, distribuição, armazenamento, recuperação e destruição de chaves criptográficas.

No PKI, a gestão de chaves é feita através de:

- **Autoridade de certificação** (CA): Entidade que emite os certificados digitais;
- **Autoridade de registo** (RA): Entidade que valida a identidade do requerente;
- **Autoridade de validação** (VA): Entidade que valida a validade do certificado;

TSA (*Time Stamping Authority*)

Autoridade que garante a data e hora de um documento.

Processo de análise de Risco FRAAP

A metodologia de análise e avaliação de risco FRAAP (Facilitated Risk Analysis and Assessment Process), é uma abordagem sistemática para identificar, analisar e avaliar os riscos de segurança da informação numa organização.

Envolve a **análise de um** sistema processo, plataforma, processo de negócio definido de cada vez, sendo divido em **três fases**:

- **Pré-FRAAP**: Tem como propósito definir as bases de trabalho para as fases seguintes.
- **FRAAP**: Incluí uma equipa mais abrangente, como responsáveis de negócio e da infraestrutura, e tem como propósito a identificação de ameaças, vulnerabilidades, impactos e controlos.
- **Pós-FRAAP**: É composto por a análise dos resultados e realização do relatório final.

Baseia-se nas normas existentes (ISO 17799/27002), que fornecem as boas práticas e não a metodologia.

Esta metodologia é vantajosa, pois:

- Resulta da experiência da equipa em projetos;
- Tem sido usada e melhoradas nos últimos 15 anos;
- É dirigido pelo responsável de negócio;
- Leva dias, em vez de semanas;
- Boa relação custo-benefício;
- Utilizar especialistas/experiência interna.

Gestão de Vulnerabilidades

Processo contínuo e abrangente que envolve não apenas a identificação de vulnerabilidades, mas também a priorização, remediação, monitorização e revisão das mesmas.

É um ciclo completo que garante a mitigação eficaz dos riscos associados às vulnerabilidades identificadas.

Funcionalidades a implementar para a gestão de vulnerabilidades

Existem várias funcionalidades que podem ser implementadas para garantir uma gestão eficaz de vulnerabilidades:

- **Descoberta e Inventário de Ativos**
- **Estabelecimento de método de classificação e Priorização de Vulnerabilidades**
- **Estabelecimento de planeamento e remediação de Vulnerabilidades**
- **Gestão de Conformidade**
- **Educação e Sensibilização**
- **Integração com sistemas de gestão de incidentes (e.g. SIEM)**

Análise de Vulnerabilidades

É um processo que identifica, avalia e reporta vulnerabilidades em sistemas, aplicações e redes.

Ferramentas de análise de vulnerabilidades

Consistem em **software** que identifica, avalia e reporta vulnerabilidades em sistemas, aplicações e redes.

Contribuem para a **identificação de riscos** ao:

- **Identificar Vulnerabilidades**: Deteta fraquezas conhecidas nos sistemas.
- **Priorizar Riscos**: Classifica vulnerabilidades por severidade, permitindo foco nas mais críticas.
- **Automatizar Processos**: Torna a análise mais rápida e eficiente.
- **Gerar Relatórios**: Fornece documentação detalhada para ações corretivas.
- **Monitorar Continuamente**: Deteta novas vulnerabilidades em tempo real.
- **Apoiar Conformidade**: Ajuda a cumprir regulamentações de segurança.

Risco inerente → Risco antes implementação de controlo
" residual → " após " " "