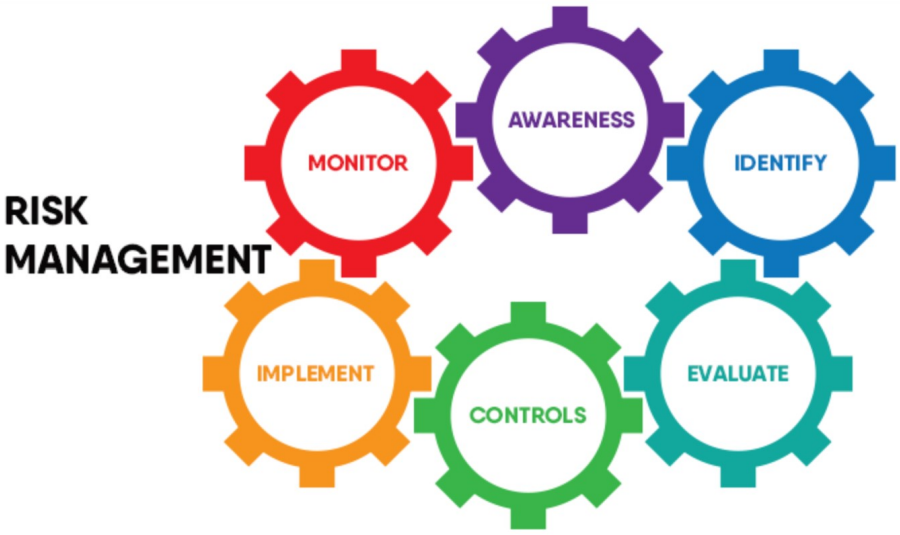
Gestão da Segurança de Informação - ISO 27001

Pedro Antunes

November 4, 2022



U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

up201507254
Instructor: Paulo de Carvalho Martins

Índice

Resumo

A ISO 27001 é uma norma internacional, que específica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar qualquer sistema de gestão de segurança da informação. Consequentemente, específica os requisitos para os controlos de segurança que devem ser implementados de acordo com as necessidades do sistema e da organização em questão, com o objetivo de mitigarem e gerirem o risco da organização, originando assim um elevado grau de confiança.

A implementação das especificações mencionadas na norma ISO 27001, demonstra que, a organização teve considerações e que tomou medidas para proteger a informação, tentando garantir a confidencialidade, integridade e disponibilidade da informação. Posto isto, a implementação desta norma também permite uma gestão eficaz e uma fácil integração com outros sistemas por seguir uma abordagem à segurança independente de marcas/fabricantes.

Este trabalho foi uma oportunidade para realizar uma investigação das várias áreas de trabalho nas quais a norma se foca e também adquirir conceitos novos de gestão de segurança de informação.

Neste relatório são abordados várias situações de risco que as organizações deveriam ter consentimento. Também são abordadas frameworks/standards e ferramentas de gestão de risco para que as organizações possam garantir uma segurança maior da sua informação.

1 Gestão de Risco

Quando abordamos a gestão de segurança da informação necessariamente precisamos de refletir e analisar o risco associado a todas as propriedades envolventes no contexto analisado. Uma gestão de risco faz com que estejamos sensibilizados para as ameaças que podem desencadear uma insegurança da nossa informação. E com isto, possamos prevenir situações de risco que coloquem em perigo informação primária.

1.1 Descrição de risco

Existem matrizes de risco, como o CVSS(Common Vulnerability Scoring System) que se tentam focar em propriedades práticas de vulnerabilidades tais como, o vetor de ataque, a necessidade ou não de elevados privilégios, a complexidade do ataque, etc. Podemos descrever um risco de um modo mais teórico por:

- Natureza de um potencial evento encadeador;
- Causas
- Probabilidade de ocorrer
- Impacto das consequências
- Indicadores

1.2 Exemplos de riscos em áreas da ISO 27001

Na tabela seguinte são apresentados riscos práticos, frameworks e ferramentas para cada área do anexo A da norma ISO 27001.

Áreas ISO	Risco Associado	Framework	Ferramenta IT
Politicas de segurança de Informação	Passwords fracas	ISO 31K	SpiraPlan
Organização interna de segurança de informação	Falta de confidencialidade, integridade e disponibilidade de informações	ISO 27K	Risk Management Studio
Segurança de recursos humanos	Emails de Phishing	COSO Framework	CheckIt
Gestão de Ativos	Servidor corrompido	CSA - Cloud Controls Matrix (CSM)	Isometrix
Controlo de acessos	Partilha de informações TOP SECRET	Control Objectives for Information Technology (COBIT)	Isolocity
Criptografia	Cifras fracas	ISA/IEC 62443	GRC Cloud
Segurança Física e Ambiental	Catástrofes naturais	ITU Critical Information Infrastructure Protection (CIIP)	iTrak
Segurança de Operações	Falta de backups	NIST Risk Management Framework	Enablon
Segurança de Comunicações	Informação exposta por técnicas MITM	CISA - Transporation Systems Sector (TSS)	Active Risk Manager
Aquisição, desenvolvimento e manutenção de sistemas	Utilização de recursos obsoletos	HITRUST Cybersecurity Framework	A1 Tracker

Áreas ISO	Risco Associado	Framework	Ferramenta IT
Relações com Fornecedores	Serviços externos maliciosos	Payment Card Industry Data Security Standard (PCI DSS)	Analytica
Gestão de incidentes e de segurança da informação	Incidentes que danifiquem a informação, como Ransomwares	MITRE ATT&CK	nTask
Aspectos de segurança da informação na gestão da continuidade do negócio	Falta de planeamento de falhas em um ou vários sistemas	Factor Analysis of Information Risk (FAIR)	Chaos Monkey
Conformidade	Falta de auditorias	NIST Special Publication 800-82	MasterControl Risk Analysis

Tabela 1. Riscos, Frameworks e ferramentas IT de acordo com as respetivas áreas do Anexo A da norma ISO 27001