Gestão da Segurança de Informação - ISO 27001

Pedro Antunes

November 4, 2022

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, esta implementação também permite uma gestão eficaz e uma fácil integração com outros sistemas por seguir uma abordagem à segurança independente de marcas/fabricantes. Envolve várias áreas de trabalho, no entanto e independentemente da área relacionada, o foco da norma é voltada totalmente para assegurar a segurança da informação. As organizações procuram bastantes certificações para que os seus parceiros obtenham certificações ISO 27001 e que, assim, possam demonstrar a adoção e a certificação na norma. Neste relatório é abordado temas como empregos, certificações e incidentes que as organizações devem adotar relacionados com o conjunto de controlos da segunda componente da norma (Anexo A).

1 Áreas ISO 27001

Esta norma padrão é composta por duas componentes. Na primeira componente são definidas as regras e os requisitos de cumprimento da norma, tais como:

- ***Contexto da organização***;
- ***Liderança***. *Contextualizam-se políticas de segurança e distribuem-se funções e responsbilidades*;
- ***Planeamento***. *Ações para caracterizar riscos e vulnerabilidades e identificação do que é necessário para alcançar os objetivos de segurança*;
- ***Suporte*** *Enumerar ou apoiar recursos, competências, consciencialização, comunicar e documentar informações para todos os envolventes da organização*;
- ***Operação***. *Efetivar e controlar o planeamento proposto. A avaliação e o tratamento do risco da segurança de informação é contínuo de acordo com a dinâmica do sistema*;
- ***Avaliação de desempenho***. *Monitorizações, auditorias e revisões*;
- ***Melhoria***.

A segunda componente é mais virada para a realidade do mundo de trabalho e é composta por um conjunto de controlos que as organizações devem adotar. Para cada controlo que a organização deve tomar é apresentada uma tabela com alguns trabalhos, certificações e vídeos de incidentes relacionados com cada objetivo de controlos.

Áreas ISO	Empregos	Certificações	Vídeo incidente BT/RT
Politicas de segurança de Informação	Information Security Specialist, Euronext	Certified Ethical Hacker (CEH), 1200$, EC-Council	What's It Like As A Red Team Operator?
Organização interna de segurança de informação	Senior Security Architect , stefanini	GIAC Defensible Security Architecture (GDSA), 2500$,GIAC	Security Architect to CISO - advice on cybersecurity roles
	Scrum Master IT, NBCC Consulting	Certified ScrumMaster, 400$,ScrumAlliance	
Segurança de recursos humanos	Portuguese Team Manager, LG	IASSC Certified Lean Six Sigma Green Belt (ICGB), 300$,IASSC	SOC Team Roles and Responsabilities
Gestão de Ativos	Senior IT Project Manager, Amaris Consulting	Associate in Project Management, 300$, GAQM	AWS Systems Manager Incident Manager
Controlo de acessos	Windows System Administrator - Active Directory	CompTIA Server+, 340$,Comptia	Red Teaming: ADventures in Active Directory
Segurança de Operações	Incident Response Officer - SOC Leader	Certififed SOC Analyst (CSA), 1200$,EC-Council	Introduction to Incident Response — What is Incident Response in Cyber Security

Áreas ISO	Empregos	Certificações	Vídeo incidente BT/RT
Segurança física	Team Lead of Infrastructure and Cloud Services, Euronext	CompTIA CertMaster Practice for Cloud+, 550$, Comptia	Red Team vs. Blue Team on AWS
Segurança nas comunicações	Network and Security Operations Team Leader	Certified information security manager (CISM),550$, ISACA	Network Analysis - Blue Team Junior Analyst
Conformidade	Information Security Auditor	Certified Information Systems Auditor (CISA), 600-800$,ISACA	Security Auditing and Compliance

Tabela 1. Carreiras e certificações de acordo com as respetivas áreas do Anexo A da norma ISO27001

Os principais benefícios da implementação da norma e posterior certificação são:

- Identificação proativa da superfície de ataque a que a organização está exposta, caracterizando as ameaças e as vulnerabilidades a que estão sujeitas;
- Garantia da continuidade do negócio, salvaguardando a informação relevante;
- Definição de um plano de recuperação de incidentes e de procedimentos de reativação de serviços;
- Proteção dos sistemas em todas as fases de desenvolvimento;
- Confidencialidade e integridade da informação;
- Criação de uma cultura de segurança de informação através da divulgação de políticas e orientações para os envolventes;
- Monitorização contínua das infraestruturas relacionadas com os sistemas organizacionais.