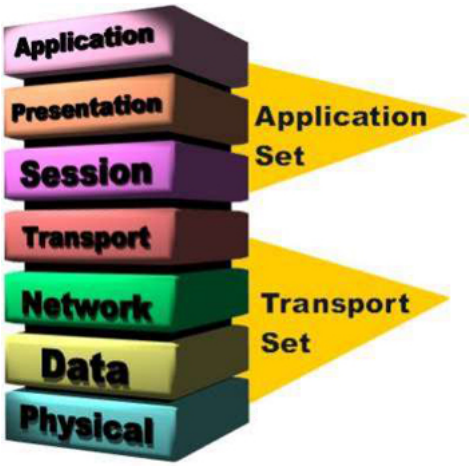
Gestão da Segurança de Informação - ISO 27001

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, 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 falamos sobre o modelo OSI de redes de comunicações e associamos alguns controlos de segurança de acordo com cada camada do modelo e das áreas ISO 27001. Falamos também de algumas ferramentas que possam implementar os controlos de segurança descritos no documento.

1 Controlos de defesa por camadas OSI

Para termos a nossa informação segura, precisamos de procurar defesas para todos os pontos da superfície de ataque. Se dividirmos a superfície de ataque por conjuntos, conseguimos criar controlos de defesa específicos para cada conjunto.
O modelo OSI é um modelo de redes de comunicação que divide a comunicação entre dois pontos por camadas. No total, contém sete camadas. Na tabela seguinte, tentamos intersetar a normas ISO 27001 com o modelo OSI. Deste modo, apresentamos alguns controlos de defesa que podemos praticar de acordo com as áreas da ISO 27001 e das camadas do modelo OSI.

Áreas ISO	**L1 Físico**	**L2 Lógico**	**L3 Rede**	**L4 Transporte**	**L5 Sessão**	**L6 Apresentação**	**L7 Aplicação**
Politicas de segurança de Informação	Escolher uma placa de rede de confiança	Não partilhar endereços MAC	Não partilhar endereços IP	Proibição de abrir sockets de comunicação desnecessários	Não utilizar sessões de outras pessoas	Apresentar os dados em codificação ASCII	Não utilizar protocolos HTTP
Organização interna de segurança de informação	Fornecer computadores controlados aos colaboradores	Fornecer computadores controlados aos colaboradores	Assegurar a privacidade da rede interna	Assegurar a privacidade da rede interna	Assegurar a privacidade da rede interna	Não utilizar protocolos HTTP	Não utilizar protocolos HTTP
Segurança de recursos humanos	Sensibilizar para os RH não instalarem PENs drives	Verificar possíveis antecedentes criminais	assinar um termo onde diz concordar com a política de segurança da informação	sigilo de informações sensíveis	sigilo de informações sensíveis	treinos adequados	treinos adequados
Gestão de ativos	Devolução de ativos após despedimentos	Randomizar os endereços MAC	Dinamizar os endereços IP	Estabelecer comunicações seguras e fidedignas	Terminar sessões nos serviços ativos após 1h	Codificar algumas informações secretas	Aceder aos servidores remotamente por SSH
	Freshservice	Total Network Inventory	JIRA Service Management	NinjaOne	N-central	EZOffice-Inventory	SysAid

Áreas ISO	**L1 Físico**	**L2 Lógico**	**L3 Rede**	**L4 Transporte**	**L5 Sessão**	**L6 Apresentação**	**L7 Aplicação**
Controlo de acessos	Ativos desbloqueados com cartões magnéticos	Restringir utilizadores por endereço MAC	Restringir utilizadores por endereços IP		Public Key Infrastructure for OTP strong authentication		Bloquear portas de serviços de informação para fora da rede interna
	Leitor de cartões magnéticos	Twingate-NAC	Blacklists-Firewall		SSL Certificate Verifier		BitDefender-Firewall
Criptografia	Hardware Security Model		IPSec	Utilizar túneis criptográficos invioláveis	Public Key Infrastructure for OTP strong authentication		SSH
	IBM Cloud Hardware Security Module		Strongswan (Linux)	SSL Server Test	SSL Certificate Verifier		OpenSSH
Segurança de operações							Intrusion Detection/Prevention System
							Snort

Tabela 1. Controlos de segurança por camadas do modelo OSI de acordo com as respetivas áreas do Anexo A da norma ISO27001