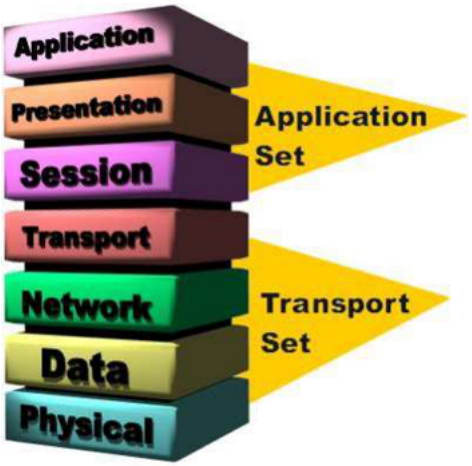
Gestão da Segurança de Informação - ISO 27001

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	BD	AD	Router	FW Proxy	WAF	IDS IPS	Linux	Windows	AWS
Politicas de segurança de Informação	Existe redundância da BD?	As passwords estão configuradas para expirarem?	As credenciais por defeito foram alteradas ?	A firewall está configurada em modo whitelist, permitindo acessos apenas a hosts autorizados ?	A WAF previne contra o top 10 de ataques web OWASP?	Os registos de eventos são documentados?	O inventário de software de Linux é documentado ?	O Windows Defender está ativo e configurado corretamente?	
	Sanitizar inputs	Passwords fortes	Alterar as credenciais por defeito	registar hosts fidedignos e autorizados	Sanitizar inputs	Atualizar assinaturas de malware	Documentar inventário de software	Documentar inventário de software	
Organização interna de segurança de informação	Quem tem acesso à BD	Quem tem acesso ao servidor AD?	Quem tem acesso admin ao router?	Quem pode configurar a FW?	Quem pode configurar a WAF?	Quem monitoriza o IDS?	Quem tem contas de utilizador no linux?	Quem tem contas de utilizador no Windows?	Quem pode aceder ao AWS?
	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.	Atribuir acesso a pessoas competentes.

Áreas ISO	BD	AD	Router	FW Proxy	WAF	IDS IPS	Linux	Windows	AWS
Segurança de recursos humanos e ambientais	Os colaboradores competentes à BD têm certificações na área?	Os colaboradores competentes à AD têm certificações na área?	Os colaboradores competentes ao router têm certificações na área?	Os colaboradores competentes à FW têm certificações na área?	Os colaboradores competentes à WAF têm certificações na área?	Os colaboradores competentes à IDS têm certificações na área?	Os colaboradores competentes têm certificações na área?	Os colaboradores competentes têm certificações na área?	Os colaboradores competentes à AWS têm certificações na área?
	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos	Conscencializar os colaboradores com treinos educativos
Gestão de ativos	Quem é responsável pela BD?	Quem é responsável pela AD?	Quem é responsável pelo router?	Quem é responsável pela FW?	Quem é responsável pela WAF?	Quem é responsável pelo IDS?	O inventário de software de Linux é documentado ?	O inventário de software de Windows é documentado ?	Quem é responsável pela AWS?
	Prevenir a divulgação de informação não-autorizada da BD.	Prevenir a divulgação de informação não-autorizada do AD.	Prevenir a divulgação de informação não-autorizada do router.	Prevenir a divulgação de informação não-autorizada da FW.	Prevenir a divulgação de informação não-autorizada da WAF.	Prevenir a divulgação de informação não-autorizada do IDS.	Documentar inventário de software	Documentar inventário de software	Prevenir a divulgação de informação não-autorizada da AWS.

Áreas ISO	**BD**	**AD**	**Router**	**FW Proxy**	**WAF**	**IDS IPS**	**Linux**	**Windows**	**AWS**
Controlos de Acessos	Quantas pessoas têm acesso privilegiado ao BD?	Quantas pessoas têm acesso privilegiado ao AD?	Quantas pessoas têm acesso privilegiado ao Router?	Quantas pessoas têm acesso privilegiado à FW?	Quantas pessoas têm acesso privilegiado à WAF?	Quantas pessoas têm acesso privilegiado ao IDS?	Quantas pessoas têm acesso privilegiado nos hosts Linux?	Quantas pessoas têm acesso privilegiado nos hosts Windows?	Quantas pessoas têm acesso privilegiado à AWS?
	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores	Não partilhar credencias com outros utilizadores
Criptografia									

Áreas ISO	BD	AD	Router	FW Proxy	WAF	IDS IPS	Linux	Windows	AWS
Segurança de recursos humanos e ambientais									
Segurança de recursos humanos e ambientais									

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