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 são abordados alguns indicadores que podemos observar quando estamos a avaliar controlos de segurança de informação e algumas dissertações académicas relacionadas com os controlos do anexo A da norma ISO27001.

1 Consciêncialização da norma ISO 27001

Para avaliarmos a organização e a implementação de controlos de segurança de informação precisamos de traduzir o que a empresa é realmente para números. Ou seja, tentamos perceber o funcionamento de uma empresa e os controlos que esta aplica através de indicadores. Estes indicadores dão-nos informações que facilmente podem ser comparáveis com métricas de sucessos empresariais.

Para mitigarmos riscos e vulnerabilidades que possam estar associadas a um contexto empresarial, são precisos estudos e provas de conceitos práticos que nos darão certezas que conseguimos evitar vulnerabilidades e reduzir a superfície de ataque. Para isto, a investigação académica tem grande relevância visto que muitas dissertações abordam novas metodologias de ataques e possíveis mitigações para as mesmas.

Na tabela seguinte mostramos alguns indicadores e dissertações relacionadas com o anexo A da norma ISO27001.

Áreas ISO	**Indicadores**	**Dissertações**
Politicas de segurança de Informação	1 - Quantas vezes as políticas foram revistas até à data? 2- Quantas vezes as políticas foram alteradas até à data?	Information Security Policy - The National Payment System in Libya
Organização de segurança de informação	1 - A percentagem de objetivos empresariais defendidos. 2 - Percentagem de ações de tratamento de risco com estimativas de custo/benfício.	

Áreas ISO	Indicadores	Dissertações
Segurança na gestão de Recursos Humanos	1 - Número de utilizadores que passaram no exame-treino de sensibilização. 2 - Percentagem de contratos com cláusulas protetoras das políticas empresariais. 3 - Quantidade de palestras existem por ano para educar os empregados.	The role of human resource management in imporving public sector performances, a case study on central bank of Bosnia and Herzegovina
Gestão de ativos	1 - Percentagem de ativos na documentação de inventário. 2 - Percentagem de software e dependencias documentadas.	
Controlos de Acessos	1 - Quantas tentativas de violações de controlo de acessos existiram até à data e quantas sucederam. 2 - Quantos pedidos de alterações de controlo de acessos existiram. 3 - Quantas das anteriores foram aceites e rejeitadas. 4 - Quantas pessoas têm um controlo de acesso crítico, moderado, etc. 5 - Com que frequência são revistos os controlos de acesso?	A study on role-based access control

Áreas ISO	Indicadores	Dissertações
Criptografia	1 - Quantas chaves criptográficas existem na empresa? 2 - Quanto tempo são utilizadas as chaves. 3 - Quantas chaves estão na lista negra?	On Some Symmetric Lightweight Cryptographic Designs
Segurança física e ambiental	1 - Quantos desastres naturais ocorreram em locais onde a empresa possui ativos. 2 - Quantos destes resultaram em elevado prejuízo e pouco? 3 - Quantas vezes os detetores de intrusão foram acionados e quantos destes foram alarmes falsos positivos e reais?	Analytical foundations of physical security system assessment
Segurança de Operações	1- Número de riscos monitorizados. 2 - Número de vulnerabilidades tem sido encontradas encontradas pela equipa de segurança. 3 - Tempo estimado para encontrar vulnerabilidades pela equipa. 4 - o número de perdas de produtividade relacionada com a segurança (% redução vulnerabilidades face a outros anos) 5 - Probabilidade de encontrar falsos positivos.	Security Enhancing Technologies for Cloud-of-Clouds

Áreas ISO	Indicadores	Dissertações
Segurança de comunicações	1 - Quantos serviços estão disponíveis à empresa sobre Internet? 2 - Quantos acordos de confidencialidade foram feitos?	Communities and Anomaly Detection in Large Edged-Labeled Graphs
Aquisição, desenvolvimento e manutenção de sistemas	1 - Quantos ambientes de desenvolvimento existe? 2 - Percentagem de sistemas atualizados. 3 - Número de atualizações feitas anualmente.	A Provable Security Treatment of Isolated Execution Environments and Applications to Secure Computation
Relação com fornecedores	1 - Quantos fornecedores a empresa matmém contacto? 2 - Quanto é importante cada recurso que é fornecido pelas empresas terceiras?	Improving Supplier Relationship Management with Supplier Portals in the Automative Industry
Gestão de incidentes de segurança de informação	1 - Números de incidentes nos último 30 dias. 2 - Número de quedas de serviço. 3 - Duração de interrupções de serviço. 4 - Tempo de resolução de incidente.	Planning and Evaluation of Information Security Investments

Áreas ISO	Perguntas	Respostas
Aspetos de segurança da informação na gestão da continuidade de negócio	1 - Númer ode iniciativas de melhoria. 2 - Qual é o período para efectuarem um novo backup? 3 - Quantos serviços redudantes existem na empresa?	Business Continuity Management - The perspective of management science
Conformidade	1 - Percentagem de controlos GDPR aplicados.	