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 várias cenários reais que podem acontecer num contexto empresarial. Através destes, tentamos relacionar controlos se devemm adotar e que comportamentos não se devem ter para que se cumpra com a norma.

1 Consciêncialização da norma ISO 27001

Neste trabalho apresentamos algumas perguntas e respostas sobre cada área de controlo da norma de gestão de segurança de informação. As perguntas foram feitas para que seja mais fácil perceber o contexto prático de cada controlo e também para termos alguma preparação para o teste final da unidade curricular.

Áreas ISO	Perguntas	Respostas
Politicas de segurança de Informação	Que tipo de especificações deve ter uma política de segurança de informação?	As políticas devem especificar a regulamentação, as responsabilidades e possíveis penalidades do descumprimento da mesma.
	O uso aceitável de ativos empresariais, evitando a exposição dos mesmos a riscos de Segurança de Informação com potencial impacto de comprometerem a continuidade de negócio, é uma política de segurança de informação	Verdadeiro
Organização de segurança de informação	Um colaborador está em regime de teletrabalho. Localmente, armazena informação sensível mas utiliza uma VPN para assegurar a confidencialidade nas comunicações com a rede de trabalho. A informação está segura?	Mesmo que a segurança da informação esteja assegurada na comunicação dos dois pontos, através da VPN, existe um risco de a informação ser comprometida no local do teletrabalho.
	Numa boa organização empresarial, a infra-estrutura de SegInf é composta pelo Gestor de Segurança de Informação.	Falso. A infra-estrutura é um grupo de trabalho composto por analistas, consultores, auditores, CSO e por uma estrutura organizacional que representam outras áreas que têm interação com SegInf.

Áreas ISO	Perguntas	Respostas
Segurança na gestão de Recursos Humanos	Uma empresa sofreu um ataque de pishing. Qual é o controlo da norma para mitigir o risco?	Treinos educativos para que os colaboradores estejam sensibilizados para ataques deste tipo.
	Um colaboradores após a cessação do seu contrato não tem de suportar mais responsabilidades de segurança de informação.	Falso. Se existir uma cláusula de sigilo que preserva a SegInf nos contratos dos colaboradores, os colaboradores que exponham informações da empresa estão a cometer um ato ilícito.
Gestão de ativos	Uma empresa que fornece computadores aos seus colaboradores, está a cumprir com a norma?	Caso os colaboradores trabalhem com informação relevante nos mesmos, então a empresa não cumpre a norma. Deve criar regras para a utilização, devolução dos ativos e ainda regras de responsabilização.
	Um colaborador tem em sua posse um computador oferecido pela empresa. No computador estão informações sobre os antigos fornecedores da empresa. Após terminar contrato com a empresa, o colaborador ficou com o ativo da empresa e pensa em divulgar a informação que tem em posse. A empresa cumpre com a norma porque considera essa informação por não ter impacto no negócio e porque os fornecedores não são os mesmos.	Verdadeiro

Áreas ISO	Perguntas	Respostas
Controlos de Acessos	Um colaborador é contratado para trabalhar numa empresa. De acordo com a norma a empresa deve fornecer livre acesso aos recursos e serviços da empresa.	Falso. Devem ser atribuídos "Roles" a todos os novos colaboradores, permitindo assim apenas os acessos necessários aos serviços que o colaborador precisar para exercer a sua função.
	Um sistema de autenticação é acedido fisicamente através de smartcards com acessos autorizados. O SysAdmin entrou no sistema de autenticação para realizar atualizações ao serviço e deparou-se com o cartão do seu colega CISO que permite fazer alterações nos registos de autenticação. Com este cartão, o SysAdmin promoveu as suas permissões de acessos na empresa. Quem tem de assumir responsabilidades nesta ocorrência?	O SysAdmin porque viola políticas de controlos de acessos e o CISO porque foi irresponsável ao esquecer-se do seu cartão no sistema.
Criptografia	Uma empresa utiliza HTTPS configurado com SSL 3.0 no seu webserver. A empresa cumpre com a norma?	Não, apesar de implementar controlos criptográficos, a informação continua vulnerável. Uma solução seria configurar o HTTPS com o TLS1.2
	As chaves criptográficas de acesso remoto devem ser válidas de acordo com o tempo dos contratos dos colaboradores.	Falso. Devem ter uma validade de aproximadamente 1 ano e devem ser renovadas.

Áreas ISO	Perguntas	Respostas
Segurança física e ambiental	Uma empresa pretende construir um Datacenter nos Açores. Esta opção vai de encontro com a norma?	Não, isto porque os Açores é uma região instabilidade tectónica e tem vulcanismos ativos. Logo, esta localização é propícia a catástrofes naturais.
	Uma empresa implementa todas as proteções digitais para defender os servidores que contêm informação preciosa. Quando os fornecedores externos se deslocam à empresa em questão, estes negoceiam na mesma sala dos servidores críticos. A empresa cumpre com a norma?	Não. Os servidores com informação crítica devem estar protegidos por um perímetro de segurança física e controlos de entrada.
Segurança de Operações	A empresa deve implementar mecanismos de registos de eventos e evidências. No entanto, as atividades realizadas pelos administradores dos sistemas não devem ser registadas.	Falso
	Operações de escrever num disco informação legítima pode fazer com que um negócio empresarial fique em perigo.	Verdadeiro. Se a empresa não controlar e gerir a capacidade do disco, o disco pode ficar cheio e com isto, crashar o sistema e negar todo o serviço.

Áreas ISO	Perguntas	Respostas
Segurança de comunicações	Uma boa prática para aumentar a segurança de redes é centralizar todos os departamentos duma empresa numa só rede para assim ser mais fácil monitorizar incidentes.	Falso. Deve ser implementado segregação de redes. Por exemplo redes por departamentos, redes para utilizadores remotos....
	Uma empresa sofreu phishing porque não tinha SPF, qual o controlo da norma que mitiga este risco.	A.13.2) Manter a segurança da informação transferida dentro da organização e para qualquer entidade externa
Aquisição, desenvolvimento e manutenção de sistemas	No caso de desenvolvimento de software por terceiros, uma empresa não se tem de preocupar com riscos associados.	Falso
	Deve ser implementado controlo de versões para garantir a gestão e a segurança dos códigos fontes.	Verdadeiro.
Relação com fornecedores	Os fornecedores de uma empresa têm uma relação pessoal com o CEO. Como temos plena confiança nos fornecedores os ativos da empresa estão protegidos.	Falso. Devem ser implementadas políticas de segurança de informação e devem ser documentados todos os acessos feitos pelos fornecedores.
	Os fornecedores de uma empresa têm uma relação pessoal com o CEO. No entanto, é preciso criar mecanismos de monitoria e auditoria aos serviços fornecidos.	Verdadeiro.

Áreas ISO	Perguntas	Respostas
Gestão de incidentes de segurança de informação	Quando um serviço está protegido por IDS/IPS a informação está totalmente segura.	Falso. Um IDS/IPS consegue reportar, avaliar e responder a incidentes. O que torna o serviço mais protegido, contudo nunca podemos dizer que o serviço está totalmente protegido.
	Uma empresa foi atacada e estava a ser vítima de espionagem. Os especialistas em segurança detetaram e eliminaram todas as backdoors implantadas na rede da empresa. Este procedimento cumpre com a norma?	Falso. A empresa tem de aprender com as ocorrências que sofre e deve tentar solucionar o problema que causou o ataque.
Aspetos de segurança da informação na gestão da continuidade de negócio	Com um sistema de backups bem protegido e seguro, é garantido que a empresa consegue resistir a um ransomware e continuar o seu negócio.	Verdadeiro.
	Qual o controlo da norma que, quando implementado, obriga a que a organização determine os seus requisitos de segurança de informação e a continuidade da gestão dos mesmos em situações adversas?	A.17.1.1 - Planning information security continuity

Áreas ISO	**Perguntas**	**Respostas**
Conformidade	Qual o controlo da norma que exige que os controlos criptográficos devam ser utilizados em conformidade com todos os acordos, leis e regulamentos relevantes ?	A.18.1.5 - Regulation of cryptographic controls
	Qual o controlo da norma que exige que os sistemas de informação sejam revistos regularmente para verficar se estão em conformidade com as plíticas e padrões de segurança de informação da organização?	A.18.2.3 - Technical compliance review

Tabela 1. Perguntas e respostas de consciencialização das áreas do Anexo A da norma ISO 27001