NOTAS DE AULA

*** DO LIVRO:** ***Gestão da Segurança da Informação: Uma visão executiva.***
Rio de Janeiro, Editora: Campus. Marcos Sêmola. 2ª ed.2014

TESTE DE CONFORMIDADE (ISO 27002)

Este instrumento vai auxiliá-lo a perceber o grau de aderência de sua empresa em relação às recomendações de segurança da informação da ISO 27002. Pela superficialidade natural desse tipo de teste, o mesmo é comumente referenciado como ISO 27002 *Gap Analysis Light*, ou seja, um diagnóstico simples e rápido, baseado em perguntas objetivas com pontuação associada que vai revelar seu índice de aderência.

Objetivos do teste

Permitir a percepção quanto ao grau de aderência da organização aos controles sugeridos pela norma ISO 27002.

Instruções

Escolha apenas uma resposta para cada pergunta e contabilize os pontos ao final.

Sua empresa possui:

1. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Política de segurança da informação?

- Sim
- Sim, porém desatualizada
- Não

2. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Um responsável pela gestão da política de segurança?

- Sim
- Sim, porém não está desempenhando essa função
- Não

Definição clara das atribuições de responsabilidade associadas à segurança da informação?

- Sim
- Sim, porém desatualizada
- Não

Política de segregação de funções e responsabilidade?

- Sim
- Sim, porém desatualizada
- Não

Acordos de cooperação com autoridades e grupos especiais?

- Sim
- Sim, porém desatualizados
- Não

Práticas de segurança em gerenciamento de projetos?

- Sim
- Sim, porém desatualizadas
- Não

Política definida para uso de dispositivos móveis e trabalho remoto?

- Sim
- Sim, porém desatualizada
- Não

3. SEGURANÇA EM RECURSOS HUMANOS

Critérios de seleção e contratação de pessoal?

- Sim
- Sim, porém desatualizados
- Não

Processos para capacitação e treinamento de usuários?

- Sim
- Sim, porém desatualizados
- Não

Processos disciplinares estabelecidos?

- Sim
- Sim, porém desatualizados
- Não

Procedimentos definidos para encerramento de contratações e desligamentos?

- Sim
- Sim, porém desatualizados
- Não

4. GESTÃO DE ATIVOS

Inventário dos ativos físicos, tecnológicos e humanos?

- Sim
- Sim, porém desatualizado
- Não

Critérios de classificação da informação?

- Sim
- Sim, porém desatualizados
- Não

Mecanismos de segurança e tratamento de mídias?

- Sim
- Sim, porém desatualizados
- Não

Procedimentos para descarte de mídias?

- Sim
- Sim, porém desatualizados
- Não

5. CONTROLE DE ACESSO

Requisitos do negócio para controle de acesso?

- Sim

- Sim, porém desatualizados
- Não

Gerenciamento de acessos do usuário?
- Sim
- Sim, porém desatualizado
- Não

Definição de responsabilidades dos usuários?
- Sim
- Sim, porém desatualizada
- Não

Controle de acesso à rede?
- Sim
- Sim, porém desatualizado
- Não

Controle de acesso ao sistema operacional?
- Sim
- Sim, porém desatualizado
- Não

Controle de acesso às aplicações?
- Sim
- Sim, porém desatualizado
- Não

6. CRIPTOGRAFIA

Política para uso de controles criptográficos?
- Sim
- Sim, porém desatualizada
- Não

Política de gestão do ciclo de vida das chaves criptográficas?
- Sim
- Sim, porém desatualizada
- Não

7. SEGURANÇA FÍSICA E DO AMBIENTE

Definição de perímetros e controles de acesso físico aos ambientes?
- Sim
- Sim, porém desatualizada
- Não

Recursos para segurança e manutenção dos equipamentos?
- Sim
- Sim, porém desatualizados
- Não

Estrutura para fornecimento adequado de energia?
- Sim
- Sim, porém desatualizada
- Não

Segurança do cabeamento?
- Sim
- Sim, porém desatualizada
- Não

Procedimentos para reutilização e alienação de equipamentos?
- Sim
- Sim, porém desatualizados
- Não

Política de mesa limpa e tela limpa?
- Sim
- Sim, porém desatualizada
- Não

B. SEGURANÇA NAS OPERAÇÕES

Procedimentos e responsabilidades operacionais definidos e documentados?
- Sim
- Sim, porém desatualizados
- Não

Processo de gestão de mudanças?
- Sim
- Sim, porém desatualizado
- Não

Processo de gestão de capacidade?
- Sim
- Sim, porém desatualizado
- Não

Processos para segregação entre ambientes de desenvolvimento, teste e produção?
- Sim
- Sim, porém desatualizados
- Não

Proteção contra códigos maliciosos e códigos móveis?
- Sim
- Sim, porém desatualizada
- Não

Procedimentos para cópias de segurança?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para monitoramento e registro de logs?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para instalação e atualização de software?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para auditoria em sistemas de informação?
- Sim
- Sim, porém desatualizados
- Não

9. SEGURANÇA NAS COMUNICAÇÕES

Controles e gerenciamento de redes?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para segregação de redes?
- Sim
- Sim, porém desatualizados
- Não

Políticas para transferência de informações?
- Sim
- Sim, porém desatualizadas
- Não

Procedimentos para proteção de informações em mensagens eletrônicas?
- Sim
- Sim, porém desatualizados
- Não

Acordos de confidencialidade e não divulgação padronizados?
- Sim
- Sim, porém desatualizados
- Não

10. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Requisitos de segurança de sistemas?
- Sim
- Sim, porém desatualizados
- Não

Processos para garantia de segurança de aplicações em redes públicas?
- Sim
- Sim, porém desatualizados
- Não

Política e procedimentos para desenvolvimento seguro de sistemas?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para controle de mudanças em sistemas?
- Sim
- Sim, porém desatualizados
- Não

Testes documentados de aceitação e segurança de sistemas?
- Sim
- Sim, porém desatualizados
- Não

Procedimento de proteção a dados para teste?
- Sim
- Sim, porém desatualizado
- Não

11. RELACIONAMENTO NA CADEIA DE SUPRIMENTO

Requisitos de segurança para relacionamento com fornecedores?
- Sim
- Sim, porém desatualizados
- Não

Requisitos de segurança para a cadeia de suprimento de produtos e serviços?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos de gerenciamento da entrega de serviços?
- Sim
- Sim, porém desatualizados
- Não

12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Mecanismos de notificação de fragilidades e eventos de segurança da informação?
- Sim
- Sim, porém desatualizados
- Não

Procedimentos para gestão de incidentes de segurança da informação e melhorias?
- Sim
- Sim, porém desatualizados
- Não

13. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Procedimentos e requisitos para a gestão da continuidade da gestão da segurança da informação?
- Sim
- Sim, porém desatualizados
- Não

Redundâncias para garantia de disponibilidade de recursos de processamento da informação?
- Sim
- Sim, porém insuficientes
- Não

14. CONFORMIDADE

Requisitos de conformidade legal e contratual documentados?
- Sim
- Sim, porém desatualizados
- Não

Controles para a proteção da privacidade e direitos individuais definidos e implementados?
- Sim
- Sim, porém desatualizada
- Não

Procedimentos para analisar criticamente o enfoque e a implementação da segurança na empresa?
- Sim
- Sim, porém desatualizados
- Não

Tabela de Pontuação

Some os pontos correspondentes às respostas de acordo com a tabela a seguir:

Resposta **A:**	some ***2 pontos***
Resposta **B:**	some ***1 ponto***
Resposta **C:**	***não some nem subtraia pontos***

Índices de conformidade com a norma ISO 27002

Após preencher as 59 questões do teste, vimos que existe um amplitude dos assuntos abordados pela norma e, obviamente, uma grande complexidade em planejar, implementar e gerir todos os controles de segurança. Lembre-se de proteger: a confidencialidade, a integridade e a disponibilidade das informações.

Veja abaixo a que distância sua empresa está da conformidade com a norma:

Resultado entre: 78-118

Parabéns! Sua empresa deve estar em destaque em seu segmento de mercado por causa da abrangência dos controles de segurança que aplica ao negócio. A empresa apresenta uma consciência da importância da segurança para a saúde dos negócios.

Resultado entre: 39-77

Atenção! Esse resultado pode ter sido alcançado de diversas formas. Sua empresa pode ter adotado quase a totalidade dos controles, mas a maioria dos quesitos podem estar ***defasados***, ***desatualizados*** ou ***inativos***. Demonstra um bom nível de consciência, mas também deficiência na estrutura de gestão ou falta de fôlego financeiro para subsidiar os recursos de administração.

Resultado entre 0-38

Cuidado! A situação não é confortável para a empresa. A segurança da informação não está sendo tratada como prioridade. Essa pontuação demonstra ausência ou ineficácia de muitos dos controles recomendados pela norma. Pode ser desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração. É importante que os profissionais de TI estejam cientes desta situação e também tenham pulso e incentivo para criar a consciência e a valorização do processo do sistema de gerenciamento de segurança da informação.