44 – Novembro de 2002

Teste: sua empresa está em conformidade com a ISO17799?

O artigo deste mês tem cunho prático e o objetivo de auxiliá-lo a perceber o grau de aderência de sua empresa em relação às recomendações de Segurança da Informação da norma internacional BS7799 ou de sua versão brasileira, a NBR ISO/IEC 17799. Pela superficialidade natural deste tipo de teste, poderíamos apelidá-lo de ISO17799 Gap Analysis Light, ou seja, um diagnóstico simples e rápido, baseado em perguntas objetivas com pontuação associada que irá revelar seu índice de conformidade.

Para os que desconhecem o assunto, a norma BS7799, assim como a versão brasileira NBR/ISO 17799, define na parte 1 um Código de Prática para a Gestão de Segurança da Informação. São ao todo 10 domínios divididos em mais 36 grupos de controles. Por se tratar de um código de prática, esta parte da norma não é objeto de certificação, mas fornece recomendações - ora aplicáveis, ora não - para os responsáveis pela introdução, implementação ou manutenção da segurança na empresa. Desta forma, estabelece uma base comum para a sustentação e o desenvolvimento de normas de segurança e atividades de gestão.
A BS7799 parte 2, por sua vez, define um SGSI – Sistema de Gestão de Segurança da Informação, servindo assim de objeto para a certificação. O processo de adoção da parte 2 como norma ISO está em estudo e não há previsão para conclusão dos trabalhos em curto prazo. Desta forma, para quem busca a certificação em Segurança da Informação, a alternativa é definir o *framework* de segurança (SGSI) e certificar-se na BS7799. Portanto, arregace as mangas e boa sorte.

Objetivo do Teste

Permitir a sua percepção quanto ao grau de conformidade que a organização tem em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ISO/IEC 17799.

Instruções

Escolha apenas uma resposta para cada pergunta e contabilize os pontos ao final.
Sua empresa possui:

POLÍTICA DE SEGURANÇA

1. Política de segurança?
   - A- Sim
   - B- Sim, porém desatualizada
   - C- Não
2. Algum responsável pela gestão da política de segurança?
   - A- Sim
   - B- Sim, porém não está desempenhando esta função
   - C- Não

SEGURANÇA ORGANIZACIONAL

3. Infra-estrutura de segurança da informação para gerenciar as ações corporativas?
   A- Sim
   B- Sim, porém desatualizada
   C- Não
4. Fórum de segurança formado pelo corpo diretor a fim de gerir mudanças estratégicas?
   A- Sim
   B- Sim, mas não está sendo utilizado atualmente.
   C- Não
5. Definição clara das atribuições de responsabilidade associadas à segurança da informação?
   A- Sim
   B- Sim, porém desatualizada
   C- Não
6. Identificação dos riscos no acesso de prestadores de serviço?
   A- Sim
   B- Sim, porém desatualizada
   C- Não
7. Controle de acesso específico para os prestadores de serviço?
   A- Sim
   B- Sim, porém desatualizado
   C- Não
8. Requisitos de segurança dos contratos de terceirização?
   A- Sim
   B- Sim, porém desatualizados
   C- Não

CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

9. Inventário dos ativos físicos, tecnológicos e humanos?
   A- Sim
   B- Sim, porém desatualizado
   C- Não
10. Critérios de classificação da informação?
   A- Sim
   B- Sim, porém desatualizados
   C- Não

SEGURANÇA EM PESSOAS

11. Critérios de seleção e política de pessoal?
   A- Sim
   B- Sim, porém desatualizados
   C- Não
12. Acordo de confidencialidade, termos e condições de trabalho?
   A- Sim
   B- Sim, porém desatualizados

C- Não

13. Processos para capacitação e treinamento de usuários?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
14. Estrutura para notificar e responder aos incidentes e falhas de segurança?
    A- Sim
    B- Sim, porém desatualizada
    C- Não

SEGURANÇA FÍSICA E DE AMBIENTE

15. Definição de perímetros e controles de acesso físico aos ambientes?
    A- Sim
    B- Sim, porém desatualizada
    C- Não
16. Recursos para segurança e manutenção dos equipamentos?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
17. Estrutura para fornecimento adequado de energia?
    A- Sim
    B- Sim, porém desatualizada
    C- Não
18. Segurança do cabeamento?
    A- Sim
    B- Sim, porém desatualizada
    C- Não

GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

19. Procedimentos e responsabilidades operacionais?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
20. Controle de mudanças operacionais?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
21. Segregação de funções e ambientes?
    A- Sim
    B- Sim, porém desatualizada
    C- Não
22. Planejamento e aceitação de sistemas?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
23. Procedimentos para cópias de segurança?

A- Sim
B- Sim, porém desatualizados
C- Não

24. Controles e gerenciamento de Rede?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
25. Mecanismos de segurança e tratamento de mídias?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
26. Procedimentos para documentação de sistemas?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
27. Mecanismos de segurança do correio eletrônico?
    A- Sim
    B- Sim, porém desatualizados
    C- Não

CONTROLE DE ACESSO

28. Requisitos do negócio para controle de acesso?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
29. Gerenciamento de acessos do usuário?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
30. Controle de acesso à rede?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
31. Controle de acesso ao sistema operacional?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
32. Controle de acesso às aplicações?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
33. Monitoração do uso e acesso ao sistema?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
34. Critérios para computação móvel e trabalho remoto?

A- Sim
B- Sim, porém desatualizados
C- Não

DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

35. Requisitos de segurança de sistemas?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
36. Controles de criptografia?
    A- Sim
    B- Sim, porém desatualizados
    C- Não
37. Mecanismos de segurança nos processo de desenvolvimento e suporte?
    A- Sim
    B- Sim, porém desatualizados
    C- Não

GESTÃO DA CONTINUIDADE DO NEGÓCIO

38. Processo de gestão da continuidade do negócio?
    A- Sim
    B- Sim, porém desatualizado
    C- Não

CONFORMIDADE

39. Gestão de conformidades técnicas e legais?
    A- Sim
    B- Sim, porém desatualizado
    C- Não
40. Recursos e critérios para auditoria de sistemas?
    A- Sim
    B- Sim, porém desatualizado
    C- Não

Tabela de pontuação

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

Resposta A: some 2 pontos

Resposta B: some 1 ponto

Resposta C: não some nem subtraia pontos

Índices de Conformidade com a norma ISO 17799

Depois de preencher as 40 questões do teste, você deve ter notado a amplitude dos assuntos abordados pela norma e, obviamente, a complexidade em planejar, implementar e gerir

todos os controle de segurança a fim de proteger a confidencialidade, integridade e disponibilidade das informações. Fazê-lo conhecer todos os aspectos envolvidos orientando-o a dimensionar a grandeza dos desafios é o primeiro objetivo deste exercício.

Seria ingênuo prometer com este teste o mesmo resultado de uma análise de riscos mas, através dos índices obtidos com a pontuação final, será possível ver o quão distante sua empresa está do que vem sendo considerado referência nacional e internacional de gestão de segurança da informação.

É bem provável que sua empresa se saia bem em um ou mais domínios. Esta situação está presente na maioria das organizações e acontece comumente pela ausência de um diagnóstico abrangente e capaz de integrar o levantamento de ameaças, impactos, vulnerabilidades físicas, tecnológicas e humanas, associando-as às reais necessidades do negócio. Sem uma análise de riscos desse tipo, as ações tornam-se desorientadas, mal priorizadas, redundantes muitas vezes, e assim não pecam por não oferecer o retorno esperado e medido pelo nível de segurança da empresa.

Veja agora a que distância sua empresa está da conformidade com a norma.

Resultado entre 80-54
Parabéns! Sua empresa é uma exceção e deve estar em destaque em seu segmento de mercado por conta da abrangência dos controles que aplica no negócio. Apesar de não podermos ver a uniformidade das ações, distribuídas pelos 10 domínios, podemos dizer que sua empresa está conscientizada da importância da segurança para a saúde dos negócios. A situação estará ainda melhor se todas as ações e controles aplicados tiverem sido decididos com base em uma análise de riscos integrada e ainda sob a gestão de um Security Officer.

Resultado entre 53-27
Atenção! Este resultado pode ter sido alcançado de diversas formas. Sua empresa pode ter adotado quase que a totalidade dos controles, mas a maioria dos quesitos pode estar defasada, desatualizada ou inativa, o que demonstraria um bom nível de consciência, mas também deficiência na estrutura de gestão ou a falta de fôlego financeiro para subsidiar os recursos de administração. Poderia ainda ter parcela representativa dos controles em ordem, deixando os demais inoperantes, ou mesmo inexistentes. Diante disso, é conveniente alertarmos para a grande possibilidade de evolução, bem como a possibilidade de estagnação e de redução tendenciosa do nível de segurança por falta de orientação. Mais uma vez, a ausência de uma análise de riscos pode ser a causa para a desorientação dos investimentos e a dificuldade de priorização das atividades.

Resultado entre 26-0
Cuidado! A situação não é confortável para a empresa. A segurança da informação não está sendo tratada como prioridade e a pontuação indica a ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administraçãoArrisco dizer que seu segmento de mercado não vive um momento muito competitivo ou que a segurança não seja vista por seus clientes como um fator crítico de sucesso por conta da natureza de sua atividade. Outra hipótese é que devem estar ocorrendo ações isoladas - de um departamento

ou de outro - que apesar de louváveis, não distribuem uniformemente a segurança e acabam por minimizar o aumento do nível de segurança do negócio. Apesar de tudo, não é hora de desanimar. Sempre há tempo de reverter a situação. Comece com uma análise de riscos e boa sorte.

Marcos Sêmola *é Mestrando em Economia Empresarial, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente Nacional de Produtos e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br