POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Versão 2.0

Prof. Me. Wallace Rodrigues de Santana

neutronica.com.br

2017

Sumário

Políticas de Segurança da Informação

OBJETIVO GERAL:

- Compreender a necessidade da definição de Políticas de Segurança da Informação nas organizações e quais as possíveis consequências da falta de seu planejamento e implementação;
- Conhecer e ser capaz de interpretar as principais normas brasileiras e internacionais utilizadas na definição de Políticas de Segurança da Informação;
- Definir Políticas de Segurança da Informação para ambientes diversos, baseando-se em melhores práticas e normas adotadas pelo mercado e na realidade da organização.

EMENTA:

- Apresentar a importância e a relevância da formulação de políticas como instrumento norteador da Segurança da Informação dentro das organizações;
- Introduzir métodos baseados em práticas adequadas para a elaboração e implementação dessas políticas, além de serem discutidas medidas que podem ser tomadas para sua divulgação na organização e conscientização de seus integrantes.

REFERÊNCIAS:

Básicas

BARMAN, Scott. **Writing Information Security Policies**. New Riders Publishing, 2001.

FERREIRA, Fernando Nicolau; ARAUJO, Marcio. **Política de Segurança da Informação**. 2.ed. Rio de Janeiro: Ciência Moderna, 2008.

PELTIER, Thomas R. **Information Security Policies and Procedures: A Practitioner's Reference**, Second Edition. 2.ed. Auerbach Publications, 2004.

Complementar

WOOD, Charles Cresson. **Information Security Policies Made Easy**, 11th Edition. Information Shield, 2009.

Adicionais

ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços**. Rio de Janeiro: Brasport, 2006.

SANTOS Jr, Arthur Roberto dos; FONSECA, Fernando Sérgio Santos; COELHO, Paulo Estáquio Soares. **Academia Latino Americana de Segurança da Informação – Introdução à ABNT NBR ISO/IEC 17799:2005**. Microsoft Technet, 2006.

PARTE I

I. Introdução

1. Defina, com suas próprias palavras, o que é Política de Segurança da Informação.
2. Quais são as premissas para implantar um Sistema de Gestão de Segurança da Informação na organização?
3. O que significa irrevogabilidade?
4. Por que os ativos são tão importantes para a organização?
5. Explique, com suas próprias palavras, o que é Confidencialidade, Integridade e Disponibilidade.
6. Qual a diferença entre Integridade e Autenticidade?
7. Dentro do Ciclo de Segurança da Informação, qual o elemento que se deseja mitigar e por quê?
8. O que é o Ciclo de Deming?
9. O que a Governança Corporativa tem de diferente da Governança de TI?
10. Quem é responsável pela Governança de TI?
11. Como as tarefas Avaliar, Dirigir e Monitorar se relacionam entre si?
12. Por que o COBIT separa a Gestão da Governança?
13. Em quais aspectos a Governança se diferencia da Gestão?
14. Como o COBIT se relaciona com as demais Normas e Guias de Boas Práticas?

II. Melhores Práticas de Governança

1. O que é o COBIT e a que se propõe?
2. Quem são as Partes Interessadas?
3. O que significa “cobrir a empresa de ponta a ponta”?
4. Qual princípio permite o alinhamento do COBIT com outros padrões e modelos de Gestão de TI?
5. O que significa Abordagem Holística?
6. O que são Habilitadores?
7. Qual(is) a(s) diferença(s) entre Governança e Gestão?
8. Quais são os dois princípios do COBIT que procuram abranger toda a organização?
9. Quais são os domínios do COBIT?
10. Descreva os cinco domínios do COBIT.
11. Faça uma correlação entre os domínios de Gestão do COBIT e o ciclo de Deming.
12. Os processos de segurança encontram-se em quais domínios do COBIT?
13. Qual a diferença entre os processos “Gerenciar a Segurança” e “Gerenciar Serviços de Segurança”?
14. Explique, com suas próprias palavras, os papéis da matriz de responsabilidade RACI.

III. Melhores Práticas de Entrega de Serviços

1. O que é o ITIL e a que se propõe?
2. O que é um Serviço de TI e por que ele é importante para a organização?
3. Como se dá a Criação de Valor?
4. Qual a diferença entre Utilidade e Garantia?
5. O que a Estratégia de Serviço fornece?
6. Qual o objetivo do Desenho de Serviço?
7. Qual o papel da Transição de Serviço?
8. O que a Operação de Serviço descreve?
9. Para que serve a Melhoria Contínua de Serviço?
10. Faça uma correlação entre o ciclo de vida do ITIL e o ciclo de Deming.
11. Por que se considera que os objetivos estratégicos são realizados por meio da operação de serviço?
12. Qual a finalidade do processo de “Gestão de Segurança da Informação” presente no ITIL?

IV. Guia para Certificação de Sistemas de Gestão de Segurança da Informação

1. O estabelecimento e a implementação do Sistema de Gestão de Segurança da Informação (SGSI) são influenciados pelo quê?
2. O que é um processo?
3. O que é abordagem de processo?
4. Quais são as implicações para a organização na transição do SGSI baseado na ISO/IEC 27001:2006 para a ISO/IEC 27001:2013?
5. Descreva o processo PDCA da abordagem de processo da ISO/IEC 27001:2006.
6. O que é Declaração de Aplicabilidade?
7. Por que é necessário ouvir as Partes Interessadas para implantação do SGSI?
8. O que deve ser levado em consideração quando se determina o escopo do SGSI?
9. Como a alta direção pode demonstrar liderança e comprometimento?
10. O que deve conter a Política de Segurança da Informação?
11. O que um processo de avaliação de riscos de segurança da informação deve fazer?
12. O que um processo de tratamento dos riscos de segurança da informação deve fazer?
13. Quem deve prover os recursos necessários para estabelecer, implementar, manter e melhorar continuamente o SGSI?
14. Quem determina as competências necessárias das pessoas?
15. Por que o processo de conscientização é importante?
16. As comunicações internas e externas relevantes devem incluir o quê?
17. Quando da criação e atualização da informação documentada, o que a organização deve assegurar?
18. Quais atividades devem ser consideradas quando do controle da informação documentada?
19. Por que a organização deve assegurar que os processos terceirizados são controlados?
20. Por que as avaliações de riscos de segurança da informação devem ser realizados a intervalos regulares e planejados?
21. Qual a diferença entre Tratamento de Riscos e Plano de Tratamento de Riscos?
22. O que deve ser levado em consideração no processo de monitoramento, medição, análise e avaliação?
23. Qual o objetivo de uma auditoria interna? Como ela deve ser conduzida?
24. O que é uma análise crítica conduzida pela direção? O que ela deve incluir?
25. O que a organização deve fazer quando uma não conformidade ocorre?

V. Melhores Práticas de Segurança da Informação

1. O que é Segurança da Informação? Como ela pode ser alcançada?
2. Quais são as três fontes principais de requisitos de segurança da informação?
3. De acordo com a ISO/IEC 27002:2005, o que as análises/avaliações de risco devem fazer?
4. Explique, com suas próprias palavras, o diagrama do Processo de Gerenciamento de Risco de Segurança da Informação da ISO/IEC 27005:2013.
5. Quais são os critérios para seleção dos controles?

PARTE II

VI. Políticas de Segurança da Informação

1. Qual

VII. Organização da Segurança da Informação

1. Por

VIII. Segurança em Recursos Humanos

1. Qual

IX. Gestão de Ativos

1. Qual

X. Controle de Acesso

1. Qual

XI. Criptografia

1. Qual

XII. Segurança Física e do Ambiente

1. Por

XIII. Segurança nas Operações

1. O

XIV. Segurança nas Comunicações

1. O

XV.Aquisição, Desenvolvimento e Manutenção de Sistemas

1. O

XVI. Relacionamento na Cadeia de Suprimento

1. O

XVII. Gestão de Incidentes de Segurança da Informação

1. Como

XVIII. Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio

1. Qual

XIX. Conformidade

1. Qual

PARTE III

XX. Políticas de Segurança da Informação

Escolha até 3 (três) documentos de Política de Segurança da Informação disponíveis no site www.neutronica.com.br e procure identificar as seguintes declarações para cada documento, de acordo com o controle "5.1.1 – Documento da política de segurança da informação", presente na ISO/IEC 27002:2005.

1. Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.
2. Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio.
3. Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco.
4. Breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
   - Conformidade com a legislação e com requisitos regulamentares e contratuais;
   - Requisitos de conscientização, treinamento e educação em segurança da informação;
   - Gestão da continuidade do negócio;
   - Consequências das violações na política de segurança da informação.
5. Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação.
6. Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.