POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0

Prof. Me. Wallace Rodrigues de Santana

neutronica.com.br

2016

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”?

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. Qual o objetivo da norma ISO/IEC 27001?
2. O que é abordagem de processo?
3. Como as partes interessadas interagem com o modelo PDCA?
4. Como o PDCA é aplicado para estruturar todos os processos do SGSI?
5. Quais requisitos a organização deve cumprir ao reivindicar conformidade com a norma ISO/IEC 27001?
6. Quais são os requisitos gerais para se adotar um Sistema de Gestão de Segurança da Informação (SGSI)?
7. O que a organização deve fazer para estabelecer e gerenciar o SGSI?
8. O que a organização deve fazer para implementar e operar o SGSI?
9. O que a organização deve fazer para monitorar e analisar criticamente o SGSI?
10. O que a organização deve fazer para manter e melhorar o SGSI?
11. O que a documentação deve incluir?
12. O que é Declaração de Aplicabilidade?
13. Por que deve haver comprometimento da direção?
14. Por que deve haver uma provisão adequada de recursos?
15. Qual a importância do treinamento e conscientização e a quem deve ser direcionados?
16. Como devem ser organizadas e atribuídas as responsabilidades?
17. Qual a importância das auditorias?
18. O que é análise crítica?
19. Como se dá a melhoria contínua?
20. O que são objetivos de controle e controles. Qual a diferença?

V. Melhores Práticas de Segurança da Informação

1. O que é Segurança da Informação?
2. De acordo com a ISO/IEC 27002, por quê segurança da informação é necessária?
3. Quais são as fontes para se estabelecer os requisitos de uma política de segurança da informação?
4. O que significa dizer que os gastos com os controles precisam ser balanceados?
5. Quais etapas a análise/avaliação de riscos deve incluir?
6. Por que a análise/avaliação de riscos deve ser repetida periodicamente?
7. Qual(is) a(s) diferença(s) entre análise de riscos e avaliação do risco?
8. Em qual momento os controles devem ser selecionados?
9. Os controles podem ser selecionados de quais fontes?
10. Quais são as opções possíveis que uma organização pode adotar para o tratamento de riscos?
11. Quais controles podem ser considerados essenciais para uma organização do ponto de vista legal?
12. Quais controles podem ser considerados melhores práticas para a segurança da informação?
13. Como é possível obter melhorias a partir da Gestão de Incidentes de Segurança da Informação?
14. Quais fatores críticos de sucesso estão diretamente ligados ao nível estratégico da organização? E ao nível tático? E ao nível operacional?
15. Como é possível obter melhorias a partir da implementação de um sistema de medição?

PARTE II

VI. Política de Segurança da Informação

1. Qual o objetivo da Política de Segurança da Informação?
2. Quais são as diretrizes para se implementar o documento da política de segurança da informação?
3. Por que deve haver comprometimento da direção?
4. Por que a política de segurança da informação deve ser comunicada para toda a organização?
5. Por que deve se tomar cuidado ao divulgar a Política de Segurança da Informação para o público externo?
6. Por que a análise crítica deve ser realizada a intervalos regulares?
7. Por que é necessário haver um gestor responsável pela Política de Segurança da Informação da organização?
8. Quais são as entradas para análise crítica? E as saídas?

VII. Organizando a Segurança da Informação

1. Por que é conveniente que seja estabelecida uma estrutura de gerenciamento do SGSI?
2. Por que é fundamental que haja comprometimento da direção da organização com a política de segurança da informação?
3. Por que as atividades de segurança da informação devem envolver representantes de outras áreas da organização ao invés de envolver somente a TI?
4. Qual o objetivo de se atribuir responsabilidades de forma claramente definida?
5. Por que é necessário que seja implantado um processo de autorização para novos recursos?
6. O que os acordos de confidencialidade procuram proteger?
7. Escreva uma definição para “autoridades”, dentro do contexto do SGSI.
8. Qual a diferença entre “autoridades” e “grupos especiais”?
9. O que significa dizer que a análise crítica deve ser independente da segurança da informação?
10. Por que é necessário identificar e implementar controles apropriados a processos de negócio antes de se conceder acesso a partes externas?
11. No contexto da seção “Organizando a Segurança da Informação”, qual a diferença entre “partes externas”, “clientes” e “terceiros”?
12. A identificação de riscos relativos ao acesso da parte externa deve levar em consideração quais aspectos?
13. Qual(is) problema(s) pode(m) ocorrer caso a organização tenha um alto grau de terceirização?
14. O que deve ser considerado antes de se conceder aos clientes o acesso a quaisquer ativos da organização?
15. Quais termos devem estar presentes em um acordo com terceiros?
16. Os acordos podem ser elaborados por quem?

VIII. Gestão de Ativos

1. Qual o objetivo da gestão de ativos?
2. Quais ativos devem ser inventariados?
3. Quais informações o inventário do ativo deve incluir?
4. Quais são os tipos de ativos?
5. Quem é o proprietário do(s) ativo(s)?
6. Quais são as responsabilidades do proprietário do(s) ativo(s)?
7. O que o proprietário do(s) ativo(s) deve analisar periodicamente?
8. O proprietário do(s) ativo(s) pode delegar sua responsabilidade a outras pessoas? Justifique.
9. O que são grupo de ativos? Dê exemplos.
10. Qual o objetivo do controle “uso aceitável dos ativos”?
11. Quais regras podem ser definidas para o uso permitido de informações e de ativos associados aos recursos de processamento de informações?
12. Quem deve fornecer tais regras?
13. Por que funcionários, fornecedores e terceiros devem estar conscientes dos limites que existem para os usos das informações e ativos associados da organização aos recursos de processamento da informação?
14. A informação deve ser classificada em quais termos?
15. A classificação da informação e seus respectivos controles de proteção devem levar em consideração o quê?
16. De quem é a responsabilidade por definir a classificação de um ativo?
17. Como o nível de proteção de um ativo pode ser avaliado?
18. Qual a importância de se rotular a informação?
19. Os procedimentos de rotulação precisam abranger quais ativos?
20. Os procedimentos para o tratamento da informação em cada nível de classificação devem contemplar o quê?
21. A rotulação e o tratamento seguro da classificação da informação é um requisito chave para qual procedimento?

IX. Segurança em Recursos Humanos

1. Qual o significado da palavra “contratação” dentro do contexto da Segurança da Informação?
2. Quais são os objetivos do objetivo de controle “Antes da contratação”?
3. Os papéis e responsabilidades pela segurança da informação devem incluir quais requisitos?
4. Por que os papéis e responsabilidades pela segurança da informação devem ser definidos e claramente comunicados aos candidatos durante o processo de pré-contratação?
5. O que pode ser usado para documentar as responsabilidades?
6. Como se deve proceder a seleção de pessoal dentro do contexto da Segurança da Informação?
7. Quais verificações podem ser realizadas durante o processo de seleção?
8. O processo de seleção deve se limitar apenas a contratação de funcionários? Justifique.
9. Por que é importante levar em consideração a legislação pertinente?
10. Qual a importância dos termos e condições de contratação?
11. Quais declarações os termos e condições de trabalho devem incluir?
12. Como a organização pode assegurar-se que os funcionários, fornecedores e terceiros concordam com os termos e condições relativas à segurança da informação?
13. Em quais circunstâncias as responsabilidades contidas nos termos e condições de contratação deveriam continuar por um período de tempo definido, após o término da contratação?
14. Para que serve um código de conduta?
15. Quais são os objetivos do objetivo de controle “Durante a contratação”?
16. O que a responsabilidade da direção deve assegurar?
17. Com qual outra seção da norma ISO/IEC 27002 o controle Responsabilidades da direção se alinha?
18. O que o treinamento deve incluir?
19. O treinamento e conscientização devem ser iguais para todos os funcionários e colaboradores? Justifique.
20. Para que serve o processo disciplinar?
21. O que significa dizer que o processo disciplinar pode ser usado como uma forma de dissuasão?
22. Quais são os objetivos do objetivo de controle “Encerramento ou mudança da contratação”?
23. Com quem a função Recursos Humanos trabalha em conjunto no processo global de encerramento?
24. Como deve se dar o processo de devolução de ativos?

25. Em quais circunstâncias o conhecimento que um funcionário, fornecedor ou terceiro detém deve ser documentado?
26. Como deve se dar o processo de retirada de direitos de acesso?
27. A retirada de direitos de acesso ocorre em qual(is) situação(ões)?
28. A redução de direitos de acesso ocorre em qual(is) situação(ões)?
29. Os cuidados ao se desligar um funcionário ou fornecedor devem ser os mesmos? Justifique.

X. Segurança Física e do Ambiente

1. Qual o objetivo da segurança física e do ambiente?
2. O que são áreas seguras?
3. O que significa dizer que “a proteção oferecida seja compatível com os riscos identificados”?
4. O que é um perímetro de segurança? Dê exemplos.
5. De quais ameaças o perímetro de segurança visa proteger?
6. Quais mecanismos de controle podem usados para proteger as portas externas?
7. Para que serve a área de recepção?
8. Por que as instalações de processamento da informação gerenciadas pela organização devem ficar fisicamente separadas daquelas que são gerenciadas por terceiros?
9. O que são barreiras múltiplas? Dê exemplos.
10. Qual a importância do controle de entrada física?
11. Quais informações devem ser registradas quando do ingresso dos visitantes às instalações da organização?
12. A segurança em escritórios, salas e instalações devem levar em consideração diversos regulamentos e normas. Cite alguns exemplos.
13. Quais são as principais formas de ameaças externas e de meio ambiente? Cite exemplos.
14. Quando as instalações vizinhas podem representar uma fonte de ameaças?
15. Quais cuidados devem ser tomados ao se trabalhar em áreas seguras?
16. Por que o uso de máquinas fotográficas e gravadores de áudio e vídeo dentro das instalações da organização não deve ser permitido?
17. Qual a finalidade de se restringir o acesso ao público em determinadas áreas da organização?
18. Por que a área de entrega e de carregamento deve ser isolada e o acesso restrito ao pessoal identificado e autorizado?
19. Por que as remessas entregues devem ser segregadas fisicamente das remessas que saem?
20. Qual a finalidade de se proteger os equipamentos destinados ao processamento de informações?
21. O que significa dizer que “os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho”?
22. Quais são as ameaças físicas potenciais que podem comprometer os equipamentos destinados ao processamento de informações?
23. O que vem a ser “utilidades” dentro do contexto da Segurança da Informação? Dê exemplos.
24. Em quais situações um suprimento de água estável e adequado é desejável?

25. Qual a importância de se ter múltiplas linhas de fornecimento de energia e de serviços de telecomunicações?
26. Por que o cabeamento de energia e de telecomunicações deve ser protegido?
27. Quando se trata de segurança do cabeamento, quais controles podem ser implementados em sistemas sensíveis ou críticos?
28. Qual a importância de se realizar uma manutenção periódica nos equipamentos destinados ao processamento de informações?
29. Quais cuidados devem ser tomados com equipamentos que estão fora das dependências da organização?
30. Quem deve autorizar a utilização de quaisquer equipamentos de processamento de informações fora das dependências da organização?
31. Quais são as formas armazenagem e processamento de informações possíveis? Dê exemplos.
32. Quais cuidados devem ser tomados quando do descarte de equipamentos que contenham mídias de armazenamento?
33. Quais cuidados devem ser tomados quando da retirada de equipamentos, informações e *software* de dentro das instalações da organização?

XI. Gerenciamento das Operações e Comunicações

1. Qual a importância de se manter documentados todos os procedimentos de operação? Dê exemplos de tarefas e/ou atividades que devem ser documentadas.
2. Por que é importante ter um processo de Gestão de Mudanças no gerenciamento das operações e comunicações?
3. Quando as mudanças envolvendo sistemas operacionais devem ser realizadas?
4. O que significa Segregação de Funções no contexto da Segurança da Informação? Qual o seu objetivo?
5. Do ponto de vista da Segurança da Informação, porque é importante segregar os ambientes de desenvolvimento, teste (homologação) e produção?
6. Por que os dados sensíveis não devem ser copiados do ambiente de produção para o ambiente de testes?
7. Quais os objetivos que se deseja alcançar quando se implementam os controles de gerenciamento de serviços terceirizados?
8. Por que se deve monitorar e analisar criticamente os serviços terceirizados?
9. De quem é a responsabilidade final pela informação processada por um parceiro de terceirização?
10. O que o processo de gerenciamento de mudanças para serviços terceirizados precisa levar em conta?
11. Do ponto de vista da Segurança da Informação, qual a importância da Gestão de Capacidade?
12. Como se dá o processo de Aceitação de Sistemas?
13. Quais são as formas para se proteger contra códigos maliciosos e códigos móveis?
14. O que é um código móvel?
15. Quais cuidados devem ser tomados na geração, guarda e restauro de cópias de segurança?
16. As cópias de segurança são requisitos para quais atividades?
17. Quais as formas de se proteger as redes de comunicação?
18. Por que a responsabilidade operacional pela rede deve ser separada da operação dos recursos computacionais?
19. Dê exemplos de serviços de rede.
20. Quais cuidados devem ser tomados no manuseio e descarte de mídias?
21. Dê exemplos de mídias.
22. A quais riscos a organização pode se expor ao trocar informações com terceiros? Quais são as formas de se proteger contra estes riscos?

23. Por que a documentação dos sistemas deve ser protegida?
24. Dê exemplos de procedimentos que devam ser considerados em uma política para troca de informações.
25. O que um acordo para a troca de informações deve conter?
26. Quais são as recomendações para proteger as mídias que são transportadas entre localidades?
27. Quais são as recomendações para proteger o envio de mensagens eletrônicas?
28. O que são sistemas de informações do negócio? O que este controle procura proteger?
29. Quais itens devem ser levados em consideração ao tratar a segurança da informação em sistemas de comércio eletrônico?
30. Quais são as formas de se proteger transações online?
31. Informações publicamente disponíveis são protegidas sob o aspecto da integridade, disponibilidade ou confidencialidade? Justifique.
32. Qual o objetivo do monitoramento?
33. Dê exemplos de equipamentos ou sistemas que produzem e mantem registros de log.
34. Por que o monitoramento do uso do sistema deve ser realizado analisado criticamente a intervalos regulares?
35. Para que servem os registros (*logs*) e porque devem ser protegidos?
36. Qual a diferença entre registros de administrator, de operador e de falhas?
37. Por que é importante que os relógios dos computadores estejam sincronizados?

XII. Controle de Acessos

1. Por que o controle de acesso à informação deve ser controlado com base nos requisitos de negócio e segurança da informação?
2. Qual a diferença entre as premissas “Tudo é proibido, a menos que expressamente permitido” e “Tudo é permitido, a menos que expressamente proibido”?
3. Por que é importante que exista um procedimento formal de registro e cancelamento de usuários?
4. Quem é o responsável por autorizar ou não o acesso do usuário a um determinado recurso?
5. Por que é necessário manter um registro formal de todas as pessoas registradas para usar um determinado recurso ou serviço?
6. O que é um perfil de acesso típico de usuário?
7. O que são privilégios?
8. Como se pode garantir que a concessão e o uso de privilégios sejam restritos e controlados?
9. Quais são as principais diretrizes para o gerenciamento de senha dos usuários?
10. Dê exemplos de procedimentos para verificar a identidade de um usuário.
11. Quais considerações devem ser levadas em conta quando da análise crítica dos direitos de acesso de usuário?
12. Quais são as responsabilidades dos usuários quanto ao uso de senhas, uso de equipamentos sem monitoração e à política de mesa limpa?
13. Quais características uma senha de qualidade ou senha forte deve conter?
14. Qual o objetivo do controle de acesso à rede?
15. Quais tecnologias podem ser usadas para implementar controles para autenticação segura de usuários, proteção de portas e segregação de redes?
16. Por que é importante controlar o acesso de usuários ao sistema operacional?
17. Quais diretrizes devem ser levadas em consideração quanto aos procedimentos seguros de entrada no sistema (*logon*)?
18. Como se pode controlar a identificação e a autenticação de usuários? Quais tecnologias podem ser usadas? Quando se deve optar por uma ou outra?
19. Quais são os objetivos ao se implantar um sistema de gerenciamento de senhas e implementar um limite de tempo de sessão e de horário de conexão?
20. Quais diretrizes devem ser seguidas ao se implementar controles de restrição de acesso à informação?
21. Por que se devem isolar sistemas sensíveis?
22. Quais cuidados devem ser tomados ao lidar com computação móvel e trabalho remoto?

XIII. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

1. O que os Sistemas de Informação incluem?
2. Quais diretrizes devem ser levadas em consideração ao contratar novos sistemas de informação ou melhorias em sistemas existentes?
3. Quais controles devem ser implementados para garantir que o objetivo de controle "Processamento correto das aplicações" seja alcançado?
4. Por que é importante validar os dados de entrada?
5. Quais técnicas podem ser usadas como um meio apropriado para a implementação da autenticação de mensagens?
6. Por que é importante validar os dados de saída?
7. Quais controles devem ser implementados para garantir que o objetivo de controle "Controles criptográficos" seja alcançado?
8. Controles criptográficos podem ser usados para alcançar quais objetivos de segurança?
9. Como o controle "Controle de software operacional" se relaciona com o processo de Gestão de Mudanças?
10. Por que é necessário controlar a instalação de software em sistemas operacionais?
11. Quando uma atualização de sistema operacional deve ser aplicada?
12. Com qual controle da ISO/IEC 27002 a "Proteção de dados para teste de sistema" se relaciona?
13. O que se pode fazer para proteger e controlar o acesso ao código fonte dos sistemas?
14. Quais diretrizes devem ser adotadas quando sistemas operacionais são mudados?
15. Por quais motivos as modificações em pacotes de software devem ser desencorajadas e limitadas?
16. Quais diretrizes podem ser levadas em consideração para prevenir o vazamento de informações?
17. O que a organização deve fazer ao terceirizar o desenvolvimento de *software*?
18. Quais diretrizes devem ser adotadas para se controlar as vulnerabilidades técnicas?

XIV. Gestão de Incidentes de Segurança da Informação

1. Como se dá o processo de notificação de eventos de segurança da informação?
2. O que é alarme de coação?
3. Quais são os exemplos de incidentes de segurança da informação?
4. O que são fragilidades de segurança da informação? Quais cuidados devem ser tomados?
5. Qual a importância de se ter responsabilidades e procedimentos estabelecidos, documentados e definidos?
6. Quais diretrizes para procedimentos de gestão de incidentes devem ser consideradas?
7. O que significa “Aprendendo com os incidentes de segurança da informação”?
8. Faça uma relação entre “Aprendendo com os incidentes de segurança da informação” com o processo de melhoria contínua.
9. Em quais situações deve-se proceder com a coleta de evidências e como ela deve ser feita?

XV. Gestão da Continuidade do Negócio

1. Qual(is) o(s) objetivo(s) da Gestão de Continuidade do Negócio?
2. Como a Gestão da Continuidade do Negócio se relaciona com a Política de Segurança da Informação?
3. Como a Gestão da Continuidade do Negócio se relaciona com a Análise/Avaliação de Riscos?
4. Como se dá o processo de desenvolver e implementar um plano de continuidade do negócio? Quais diretrizes devem ser levadas em consideração?
5. Como deve ser a estrutura de um plano de continuidade do negócio?
6. Quais diretrizes devem ser levadas em consideração quanto aos testes, manutenção e reavaliação dos planos de continuidade do negócio?

XVI. Conformidade

1. Qual o objetivo da conformidade da politica de segurança da organização em relação aos requisitos legais?
2. Quem de dentro da organização pode ajudar a identificar a legislação aplicável?
3. Como a pirataria de software se relaciona com os direitos de propriedade intelectual? O que a organização pode fazer para implementar controles que protejam o direito a propriedade intelectual?
4. Dê exemplos de registros organizacionais e por que eles devem ser protegidos.
5. Por que dados e informações pessoais devem ser protegidos?
6. Como fazer para prevenir o mau uso de recursos de processamento de informação?
7. Por que deve haver conformidade entre os controles de criptografia usados pela organização e a legislação vigente?
8. Como os gestores podem garantir a conformidade dos procedimentos de segurança de suas áreas com a política de segurança da organização?
9. Como se dá a verificação da conformidade técnica?
10. O que deve ser levado em consideração quanto à auditoria de sistemas de informação?

PARTE III

XVII. 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.