

Questionário de Segurança

Conforme Gil, em seu livro “Segurança em informática”, editora Atlas, com o objetivo de facilitar a otimização/auditoria da qualidade da segurança em informática, foi relacionado uma série de perguntas.

1. ADMINISTRAÇÃO DA SEGURANÇA	Sim	Não	N/A
a) Existe norma definindo autoridade e responsabilidades para o analista de segurança em informática?			
b) É feita, regularmente, auditoria da qualidade da segurança em informática, nas plataformas de informática?			
c) Estão, claramente, definidas as obrigações operacionais e gerenciais das áreas de informática, segurança, auditoria e usuários?			
d) Está atualizada e existem diretrizes padronizadas para a documentação de informática?			
e) Existe, e é cumprido, um plano de <i>backup</i> para documentação e arquivo de programas e dados, contra acesso indevido e catástrofes, em todos os ambientes e plataformas de informática?			
f) A administração de dados estabelece normas para classificação dos dados quanto a segurança e sigilo?			
g) Há normas para a atividade de terceiros no ambiente/plataforma de informática?			
h) A emissão de relatórios confidenciais é protegida por rigoroso esquema de <i>password</i> e sua emissão, tramitação e destruição física é objetos de normas específicas?			
i) Há proibição de uso de equipamentos (aparelhos eletrônicos) junto aos dispositivos integrantes das plataformas de informática?			
j) Há limitações para que os usuários e profissionais de informática não tenham uma visão total do sistema de segurança de dos e ambiente/plataforma de informática?			
k) Há práticas de análise rotineira, de picos e vales a cada configuração/ <i>link</i> /banco de dados integrante da plataforma de informática?			
l) Há controles específicos nos ambientes computacionais para visitantes, profissionais contratados de terceiros, entrega de mercadorias, ocasiões de festas e feriados?			
m) Existem providências ou dispositivos que evitem a entrada de imãs., objetos pesados de ferro, armas de fogo ou ainda a saída de relatórios não autorizados e volumes estratégicos?			
n) Há diretrizes para alienação de microcomputadores, meios magnéticos e destruição de relatórios, papel carbono e fitas de impressoras?			
o) Há normas para tratamento de <i>log's</i> e para geração, uso e cancelamento de senhas?			
p) Há diretrizes para o estabelecimento de cláusulas em			

contratos de aquisição de <i>software</i> e de <i>hardware</i> e para contratação de serviços de terceiros?			
q) Há diretrizes claras quanto a controles e segurança lógica que devam ser contemplados em nível de desenvolvimento e operação de sistemas aplicativos?			
r) Há um plano geral, com um conjunto de normas, diretrizes, procedimentos, em sua empresa, para segurança em informática?			
s) Existe e está em uso um programa formal de administração/análise de risco em ambiente/plataformas de informática?			
t) Na segurança em informática de sua empresa são estabelecidas ligações efetivas com entidades externas de apoio à segurança, nas seguintes áreas: - equipamentos e dispositivos de instalação, de construção, elétricos, de ar condicionado e de infra-estrutura em geral? - segurança pública? - empresa seguradora? Empresas de serviços de água e esgotos, comunicações, energia elétrica?			

2. SEGURANÇA DO HARWARE	Sim	Não	N/A
a) Há esquema de <i>no-break</i> e geradores, que garantam o suprimento de força para a operação das plataformas de informática, de forma ininterrupta ou com tempo hábil, para desativação dos sistemas aplicativos em operação?			
b) Os dispositivos integrantes das plataformas de informática têm sua manutenção e limpeza regularmente realizada segundo normas e contratos de manutenção?			
c) Existem registros das ocorrências técnicas quanto aos equipamentos, cabos e sensores integrantes das plataformas de informática?			
d) Existem estabilizadores para proteção dos equipamentos integrantes das plataformas computacionais existentes nos ambientes de informática da organização?			
e) Existe estoque mínimo ou suprimento imediato de insumos operacionais para as plataformas de informática?			
f) A instalação onde está a plataforma de informática está adequadamente, protegida contra sabotagem, através de ondas de rádio, radar, impulsos de interrupção?			
g) Foram testados, para supressão de interferências, os pares eletro-eletrônicos usados e operados junto aos dispositivos componentes da configuração da plataforma de informática?			
h) Existe esquema de <i>backup</i> dos equipamentos da plataforma de informática?			
i) Existem controles, físicos e lógicos, para prevenção e detenção do uso indevido do <i>hardware</i> a cada ambiente computacional?			

3. SEGURANÇA GERAL DE INFORMÁTICA	Sim	Não	N/A
a) Existe um sistema seguro de distribuição de relatórios que impeça uma pessoa, não autorizada de receber relatórios confidenciais?			
b) Há estratificação dos eventos de insegurança registrados pelo <i>help-desk</i> ?			
c) A área de planejamento e controle da produção estabelece seqüências de processamento alternativas, para efeito de continuidade operacional das plataformas de informática?			
d) A estrutura orgânica e desenvolvimento das funções da área de informática contemplam adequada segregação de funções?			
e) Há espírito de segurança junto aos profissionais que atuam nas plataformas de informática?			

4. ARQUIVO DE SEGURANÇA (MÍDIAS)	Sim	Não	N/A
a) Há adequada proteção quanto às portas de acesso, em termos de alcance do ambientes de segurança das mídias magnéticas?			
b) As portas de acesso possuem código de acesso por cartão magnético, ou, outro dispositivo eletrônico?			
c) As portas possuem sistema de destravamento para caso de pânico?			
d) As pessoas com acesso autorizado são aquelas mínimas e indispensáveis?			
e) Os funcionários com acesso aos arquivos de segurança em conhecimento da sensibilidade das mídias magnéticas contra influências físicas e gases corrosivos?			

5. OUTROS DESASTRES	Sim	Não	N/A
a) O prédio e as plataformas de informática são estruturalmente seguros e resistem a ventanias, inundações e estão devidamente aterrados para evitar danos provocados por raios?			
b) Existe probabilidade de tumultos, motins, sabotagens, greve, chantagem, terrorismo, junto as plataformas de informática?			
c) Há sistema de sensoriamento eletrônico amparado por <i>software</i> e ainda, conjugado com circuito fechado de televisão para proteção do ambiente informatizado?			
d) Existe norma sobre comportamento operacional no ambiente de informática, contemplando restrições a comida, bebida e fumo junto aos equipamentos?			
e) Existe seguro com cláusulas e valores financeiros adequados para cobertura contra fogo, desastres naturais, danos provocados por água e sabotagens?			
f) Os equipamentos são protegidos por capa plástica ou outro tipo de proteção contra poeira, água e sujeira em geral?			
g) O seguro cobre todos os tipos de perdas, inclusive destruição			

de dados e paralisação total ou parcial dos negócios?			
h) Equipamentos e áreas de trabalho são limpos rotineiramente?			
i) As plataformas de informáticas estão excluídas de áreas de subsolo?			
j) As portas e as janelas externas ao ambiente de informática são a prova de água?			
k) Existe proteção contra o acúmulo de águas pluviais, vazamentos no teto ou tem torres de resfriamento de ar-condicionado, junto ao ambiente de informática?			
l) Onde está localizado e quem tem acesso ao quadro de alimentação elétrica das plataformas de informática?			
m) Qual a autonomia do gerador de energia em função da quantidade de combustível estocada?			
n) O gerador e as chaves disjuntoras suportam os picos de voltagem?			
o) Os cabos de energia possuem proteção especial (conduites blindados)?			
p) A central de avisos de incêndio é monitorada e está adequadamente protegida?			
q) Existem plantas das instalações e dos comandos elétricos?			
r) Existe iluminação de emergência, para facilitar a retirada do pessoal, no ambiente de informática?			
s) O sistema de alimentação elétrica de ar-condicionado, iluminação e elevadores é independente do sistema que fornece energia às plataformas computacionais?			
t) Os quadros de força, luz, telefonia, teleprocessamento e de controles de emergência/alarme/alerta estão identificados e devidamente trancados com chave numerada sob controle da área usuária ou da área de segurança?			
u) As máquinas, equipamentos e dispositivos integrantes das plataformas de informática estão devidamente instaladas, localizadas e ligadas às fontes de energia e água?			
v) Os equipamentos e dispositivos para prevenção e combate a sinistros estão bem localizados, instalados, identificados e têm sido testados e verificados nos prazos estabelecidos pelos fabricantes?			
w) O pessoal da segurança e que trabalha nas plataformas de informática sabe como agir em situação de distúrbios civis?			
x) Existe um esquema de ligação entre o pessoal das plataformas de informática e as entidades locais de polícia, corpo de bombeiros, defesa civil e hospitais?			
y) Os profissionais que atuam nos ambientes de informática sabem como se comportar diante de ameaças telefônicas de atentado a bomba?			

6. SIGILO DOS DADOS	Sim	Não	N/A
a) Os documentos em processamento ou durante a remessa, ou após o uso, são resguardados contra acesso indevido?			

b) Estão em vigor medidas de segurança adequadas para proteger relatórios confidenciais como atitudes de investigação de tentativas não autorizadas, de cópia, de furto, ou de acesso indevido às plataformas computacionais?			
c) É adequada a política escrita com relação a marcação, manipulação e destruição de dados confidenciais?			
d) Existe normas determinando esquema de mesa limpa, bem como fechamento de arquivos e gavetas?			
e) Há esquema de proteção eficiente quanto à destruição do conteúdo de cesta de lixo?			
f) Os papéis, inclusive o papel carbono de formulário contínuo, e os relatórios sensíveis são destruídos através de queima ou fragmentação?			
g) Onde ficam depositados os dados aguardando destruição?			
h) Há destruição do conteúdo das mídias magnéticas quando de sua alienação?			
i) Há controles efetivos para o tráfego de mídias magnéticas dos ambientes de informática da empresa para seu ambiente externo?			
j) Há exigências de credenciamento para as pessoas que retiram e trazem mídias magnéticas?			

7. SEGURANÇA LÓGICA	Sim	Não	N/A
a) Os usuários de sistemas aplicativos especificam e são responsáveis pela segurança de seus sistemas?			
b) Os usuários de plataforma de informática são treinados quanto aos procedimentos de segurança, como uso de senhas, <i>log-on e log-off</i> ?			
c) Todos que tem acesso às plataformas de informática necessitam identificar-se?			
d) Todas as tentativas de acesso aos sistemas, autorizadas ou não, são registradas?			
e) Há normas com procedimentos e práticas para cancelamento de senhas dos usuários?			
f) Os dados de entrada são objeto de controles que assegurem sua integridade, via programa de crítica?			
g) Os campos-chaves são tratados via rotina de dígito verificador?			
h) São tomadas medidas para evitar que ocorram erros propositais?			
i) Há norma recomendando práticas de rodízio e segregação de funções ao nível de profissionais?			
j) Há norma estabelecendo o emprego de totais de controle e de arquivos de controle junto a cada sistema aplicativo?			
k) Há identificação de quem faz a verificação dos totais de controle para liberação de etapas de processamento?			
l) É documentada a retirada, o uso e a devolução de todos os arquivos de dados e de programas?			

m) Existem rotinas para a reconstrução de arquivos/banco de dados?			
n) Há definido para todos os arquivos os períodos de retenção?			
o) Existem procedimentos para submissão de disquetes e tráfego de arquivos?			

8. SEGURANÇA DO SISTEMA DE AR-CONDICIONADO	Sim	Não	N/A
a) Existem tampas corta-fogo dentro dos dutos de ar-condicionado?			
b) Os dutos de ar-condicionado possuem detectores de chama, de calor, de fumaça?			
c) Os dutos de entrada e saída de ar-condicionado são acessíveis a pessoas não autorizadas?			
d) O sistema de ar-condicionado é exclusivo para o ambiente computacional?			
e) Há realização de manutenção preventiva?			

9. CONTROLE DE ACESSO	Sim	Não	N/A
a) O ambiente de informática é protegido contra distúrbios e comoção civil?			
b) Há sistema de identificação físico (exemplo crachá com foto)?			
c) Existem portas de emergência nos ambientes de informática?			
d) Existe plano antigreve que garanta funcionamento mínimo?			
e) Há efetivo controle de visitantes às plataformas de informática?			
f) Há circuito fechado de televisão?			
g) É restrito o acesso a vendedores, parentes, conhecidos nas áreas sensíveis?			

10. MANIPULAÇÃO DE ARQUIVOS	Sim	Não	N/A
a) Há segurança no sistema de transporte de volumes magnéticos?			
b) Há correta identificação externa dos volumes magnéticos?			
c) Há atribuição de responsabilidade?			
d) São feitos inventários regulares dos volumes magnéticos?			

11. PLANJEMANETO E CONTROLE DA PRODUÇÃO	Sim	Não	N/A
a) Há cronograma para alimentação dos serviços?			
b) Existe monitoração dos trabalhos operacionalizados?			
c) Há definições de prioridades para execução de serviços?			
d) Há procedimentos de rateio de custo de utilização dos recursos computacionais?			

12. AMBIENTE ON-LINE/COMUNICAÇÃO DE DADOS	Sim	Não	N/A
a) Existem medidas visando controlar o acesso indevido à linhas de comunicação?			
b) Há procedimentos definidos para manutenção e substituição dos dispositivos computacionais?			
c) Há monitoração dos tempos de resposta?			
d) É analisado o tráfego de transações nos canais de comunicação?			
e) A transmissão de dados é identificada através de logs ?			

13. BANCO DE DADOS	Sim	Não	N/A
a) São identificadas as solicitações de acesso aos bancos de dados?			
b) Os requisitos de acesso aos bancos de dados são limitados a funções específicas (perfis)?			
c) Há funções especiais reservadas para auditoria interna?			
d) É usada criptografia dos dados, em especial em sua transferência?			
e) Todas as transações são registradas em <i>logs</i> ?			
f) Os conteúdos dos Bancos de Dados são copiados periodicamente?			
g) Há facilidade de recuperação de dados em caso de sua destruição?			
h) Existe dicionário de dados dativo?			

14. CONSTRUÇÃO E LOCALIZAÇÃO	Sim	Não	N/A
a) O layout do ambiente de informática permite adequado controle de acesso físico e dificulta a propagação de incêndio, inundações, vandalismo e sabotagem?			
b) Existe sistema de pára-raios?			
c) Todos os cabos são devidamente identificados?			
d) Foi evitado o uso de materiais halógenos (PVC)?			
e) Há proteção contra resíduos, poeira, fuligem?			
f) A capacidade de carga do piso é adequada?			
g) Existem saídas de emergência suficientes?			

15. INCENDIO	Sim	Não	N/A
a) Os tapetes, móveis, divisórias e janelas são a prova de fogo?			
b) Existem extintores adequados para cada tipo de fogo, em lugares convenientes e bem identificados?			
c) Os papeis e outros suprimentos são armazenados fora dos ambientes de informática?			
d) Realizam-se treinamento periodicamente?			
e) Há brigadas de incêndio?			
f) O ambiente das mídias magnéticas está protegido contra o fogo?			

g) Há sensores de fumaça, calor, umidade, temperatura?			
--	--	--	--

16. PESSOAL DE INFORMÁTICA	Sim	Não	N/A
a) Há treinamento sobre segurança periodicamente?			
b) É feita uma análise das credenciais dos profissionais que irão atuar na área?			
c) É aceito o trabalho de parentes junto à mesma plataforma de informática?			
d) Há cláusulas no contrato de trabalho quanto a ao sigilo?			
e) Os funcionários assinam um compromisso específico de sigilo?			
f) São examinadas as horas extras excessivas e a não-saída normal de férias em funções sensíveis?			
g) São alterados os códigos de segurança quando da dispensa de funcionários?			
h) É enfatizada a política de mesa limpa?			
i) Registram-se descontentamentos dos funcionários?			
j) Há políticas específicas para profissionais de limpeza e de manutenção?			

17. SEGURANÇA DE SOFTWARE	Sim	Não	N/A
a) É documentada a homologação e testes de novos programas ou de suas alterações?			
b) A relação custo/benefício da operação dos sistemas justifica os esforços de segurança?			
c) Existe uma biblioteca de programas fontes atualizada?			
d) É exercida formas de auditoria para assegurar que os controles de segurança estão sendo praticados?			
e) Identifica-se uma lista de programas/sistemas sensíveis?			