CONHECIMENTOS ESPECÍFICOS

A equipe de analistas apresentou um plano de segurança da informação a um dos mais tradicionais e capilarizados ministérios do Brasil, desenvolvido após um extenso trabalho de pesquisa, ao longo de alguns meses. O documento, que aborda um grande número de tópicos sobre segurança da informação no ministério, contém análises, diagnósticos, problemas, soluções possíveis e propostas, organizados na forma de capítulos. Alguns dos capítulos são listados a seguir.

- Conceitos de segurança da informação
- Proposta de política de segurança
- Classificação de informações
- Auditoria e conformidade
- Controle de acessos físicos e lógicos
- Indicadores e métricas
- Gestão de vulnerabilidades
- Gestão de riscos
- Criptografia
- Gestão de continuidade de negócio
- Terceirização de atividades ligadas à segurança da informação
- Segurança em bancos de dados
- Segurança no desenvolvimento de aplicações *web*
- Segurança em redes de computadores
- Resposta a incidentes computacionais em redes

O plano também contém um capítulo de revisão de normas brasileiras de segurança da informação, da série NBR da ABNT, tais como NBR 27001, NBR 27002 e NBR 27005.

Após a apresentação do plano de segurança à administração superior do ministério, aos assessores e aos convidados por meio de chamada pública, vários debates foram realizados, e foi variado o grau de conhecimento sobre os conceitos e as características do plano, de sua elaboração e do projeto de implantação.

Tendo como referência a situação hipotética apresentada, julgue os itens a seguir, acerca de conceitos de segurança da informação possivelmente articulados no plano.

61 Os procedimentos de auditoria interna de segurança da informação precisam levar em consideração não só os requisitos normatizados em normas aplicáveis como a NBR 27001:2006, mas também a legislação aplicável e existente sobre o tema, no âmbito da administração pública federal.

62 Os procedimentos de produção de métricas e indicadores de gestão de segurança da informação devem ser mais bem orientados pelo conjunto de prescrições encontradas na norma NBR 27005, de gestão de riscos de segurança da informação, que pelos processos descritos na norma NBR 27001.

63 Os procedimentos de classificação da informação quanto ao sigilo não podem ser concluídos sem que sejam investigados os riscos à perda de confidencialidade, integridade e disponibilidade da informação.

Acerca de problemas e soluções possivelmente presentes no capítulo sobre políticas de segurança da informação, julgue os próximos itens.

64 A fim de ampliar o acesso a fontes de informação para detecção de vulnerabilidades organizacionais, a política de segurança da informação proposta deve evidenciar a importância dos resultados de testes de auditoria.

65 No controle de acessos, tanto físico quanto lógico, às instalações prediais e aos sistemas de computação do ministério, deve ser considerado o uso de autenticação por múltiplos fatores, pois esse é procedimento descrito na norma NBR 27001, no seu guia de implementação de vários controles, entre eles os relacionados ao objetivo Controle de Acesso à Rede.

Julgue os itens a seguir, considerando que o capítulo sobre criptografia contenha problemas e sugestões para o uso de criptografia simétrica, criptografia assimétrica e funções *hash*, na plataforma de sistemas de computação do ministério.

66 A prescrição para banimento do uso da função MD5, em favor da adoção de SHA-1, pode ser recomendada, especialmente porque a facilidade de produção de ataques de colisão em sistemas que usam MD5 tornaria mais simples a implementação de ataques de dicionário em sistemas de armazenamento de senhas criptografadas nos bancos de dados de autenticação de usuários do ministério.

67 Em comunicações seguras com os cidadãos que são afetados pelas políticas públicas conduzidas pelo ministério, efetuadas predominantemente com o uso de navegadores e servidores *web*, devem ser adotados sistemas criptográficos assimétricos, de chave pública, mas não sistemas criptográficos simétricos, pois esses últimos exigiriam que os cidadãos tivessem prévio acesso às chaves criptográficas dos sítios do ministério, ou que o ministério tivesse acesso prévio às chaves criptográficas dos cidadãos, sendo esses acessos inviáveis na prática. Política inversa deve ser adotada internamente ao ministério, com a adoção de sistemas criptográficos simétricos.

Considere que a apresentação do capítulo sobre gestão de riscos tenha sido precedida pela indicação de que há pouca disponibilidade de registros históricos quanto a incidentes de segurança no ministério. Nesse contexto, julgue os itens subsecutivos.

68 Para o planejamento da gestão de riscos no ministério, é recomendável a adoção inicial de uma metodologia de riscos quantitativa, em detrimento de metodologia qualitativa, tendo em vista a pouca disponibilidade de registros históricos de incidentes.

69 O estudo das ameaças à segurança da informação será mais efetivo se forem previamente identificados os ativos de informação mais relevantes para o ministério, que são os ativos ligados ao funcionamento do setor de tecnologia da informação (TI) do órgão.

70 O tratamento dos riscos de segurança da informação será efetivo se forem consideradas as várias alternativas para tratamento de todos os riscos vinculados a cada um dos ativos de informação do ministério, tais como mitigar ou reduzir, reter ou aceitar, transferir ou compartilhar, além de ação de evitar o risco.

Julgue os seguintes itens, considerando que o capítulo sobre gestão de continuidade de negócios contenha uma proposta em aderência à norma NBR 15999-1 – Gestão de Continuidade de Negócios.

71 A elaboração de um estudo de análise de impacto nos negócios (BIA) pode ser precedida por uma análise de riscos de segurança da informação, especialmente se for focado na indisponibilidade de ativos, pois, se o BIA identifica de forma mais precisa os impactos de uma interrupção, ele também demanda investigações detalhadas sobre os custos da interrupção de processos, e será mais efetivo se for focado nos processos de negócios associados aos riscos de maior magnitude.

72 No processo de terceirização de serviços de segurança da informação, a contratação de um estudo de análise de impacto nos negócios apresenta maior risco à continuidade ou sustentação organizacional, quando comparada à contratação de um serviço terceirizado para a gestão de riscos de segurança da informação.

73 O emprego de instrumentos e processos de comunicação social se faz mais necessário na formulação de um plano de administração de crises para o ministério do que na formulação de um plano de continuidade operacional.

Considere que o capítulo sobre segurança de bancos de dados contenha recomendação de adoção de arquiteturas seguras, modelos e sistemas de controle de acesso e procedimentos de classificação, entre outros. A esse respeito, julgue os itens subsequentes.

74 O fortalecimento da segurança de bancos de dados do ministério envolve primariamente a adoção de controle de acesso às conexões das aplicações aos servidores de bancos de dados, especialmente se efetuadas por meio de *firewalls*, sendo de importância secundária a construção de dicionários de dados e os procedimentos de classificação da informação.

75 A adoção de controle de acessos a dados aderente ao modelo mandatório depende da adoção de procedimentos de rotulagem de segurança que sejam aplicáveis tanto aos usuários quanto aos dados.

76 Qualquer proposta de eliminação da presença de *software* em arquitetura cliente-servidor no parque das aplicações do ministério, em favor da adoção de arquiteturas *multitier*, não terá pleno sucesso, porque uma arquitetura *multitier* pode ser considerada uma composição de múltiplos sistemas em arquitetura cliente-servidor.

Considere que o capítulo sobre segurança de aplicações contenha proposta de adoção de uma metodologia de desenvolvimento de aplicações com segurança fundamentalmente embasada na metodologia OWASP (*open web application security project*), envolvendo uma proposta de processo de desenvolvimento de aplicações aderente ao arcabouço *software assurance maturity model* da OWASP, conhecido como SAMM ou OpenSAMM, em combinação com aspectos técnicos como arquiteturas seguras para aplicações *web*, análise de vulnerabilidades, testes de invasão, gestão de *patches* e ataques. Nesse contexto, julgue os itens seguintes.

77 No tópico segurança de aplicações *web*, o plano deve considerar o ataque de injeção como sendo um dos mais importantes em comparação aos demais, seja pela sua facilidade de explorabilidade (*explotability*) com o uso de *scanners* e *fuzzers*, seja pela facilidade com que podem ocorrer incidentes de alto impacto técnico, tais como vazamento de dados, perda de integridade (adulteração) e perda de contabilização.

78 No tópico segurança de aplicações *web*, o plano deve considerar o ataque de quebra de autenticação e de gerenciamento de sessão como sendo um dos mais importantes em relação aos demais, seja porque é comum aos desenvolvedores de *software* adotarem esquemas de autenticação e gerenciamento de sessão próprios e que contém falhas, seja porque possibilitam a execução de *scripts* nos navegadores das vítimas, facilitando a pichação de sítios *web* e o sequestro do navegador do usuário, entre outros impactos de negócio.

79 Em aderência ao arcabouço SAMM da OWASP, cada uma das práticas de segurança no desenvolvimento de *software* a serem desenvolvidas no ministério deve ser avaliada quanto à capacidade, em uma escala que varia de 0 a 5, e que são 0 – Incompleto; 1 – Executado; 2 – Gerenciado; 3 – Definido; 4 – Quantitativamente gerenciado; 5 – Otimizante.

80 A fim de melhor implementar a técnica de detecção de vulnerabilidades e gestão de *patches* em aplicações *web*, o plano deve recomendar a adoção da arquitetura AppSensor da OWASP.

81 Em aderência ao arcabouço SAMM da OWASP, o plano deve promover um processo de desenvolvimento seguro de *software* com base na adoção de práticas de segurança para quatro funções vinculadas ao negócio de desenvolvimento de *software*, as quais são: governança, construção, verificação e implantação (*deployment*). Para cada função, são prescritas três práticas.

Julgue os próximos itens, considerando que os capítulos sobre segurança em redes de computadores e sobre resposta a incidentes computacionais em redes contenham uma série de diretrizes organizacionais, técnicas e computacionais para o ministério.

82 Para a segurança na comunicação entre a sede do ministério e suas diversas representações dispersas pelas unidades da federação, é recomendável a adoção de redes virtuais privadas baseadas no IPSEC com modo de transporte. Dessa forma, na eventualidade de captura de tráfego entre o ministério e uma de suas representações por meio de um *sniffer*, não será possível a identificação dos endereços IP de origem e de destino das conexões TCP estabelecidas nas extremidades da rede, enquanto são garantidas ainda a autenticidade e sigilo dos dados trafegados.

83 A fim de proteger a segurança da informação do ministério, bem como auxiliar no cumprimento de sua missão de desenvolvedor de políticas públicas em sua área de atuação, o ministério deve se abster de desenvolver sua presença digital nas mídias sociais, bloqueando os acessos dos usuários de níveis operacionais e administrativos intermediários a essas mídias sociais, visando à redução da ocorrência de ataques de engenharia social, de *phishing*, *scams* e *spams*.

84 Entre as atividades típicas de uma equipe de tratamento de incidentes em redes de computadores, está a realização periódica de auditorias de conformidade, tomando por base o catálogo dos controles prescritos na norma ISO 27001:2006.

85 Considere que, para a defesa de perímetros na rede do ministério, tenha sido proposta uma solução com o uso dos seguintes dispositivos: *firewall* de aplicação *web* (WAF); sistemas de prevenção de intrusão (IPS) em rede; e *firewall* de filtragem de pacotes *stateful*. Nesse caso, seria recomendável a colocação do *firewall* de filtragem na camada mais externa; do WAF na camada mais interna; e de IPS na camada intermediária.

A respeito dos mecanismos de autenticação, julgue os seguintes itens.

86 Mecanismo que usa *token*, verificação biométrica de impressão digital e PIN é exemplo de mecanismo de três fatores.

87 Os protocolos criptográficos Diffie-Hellman e RSA são amplamente usados para fins de autenticação.

88 Os benefícios providos pelos mecanismos de autenticação incluem a corroboração da identidade das partes e da origem da informação e o controle de acesso.

No que se refere a ataques aos *logs* e registros de auditoria, julgue os próximos itens.

89 Os registros do Syslog e do Microsoft Event Viewer têm a eles agregados informações de integridade na forma de resumos criptográficos (*message authentication codes* – MAC).

90 O serviço Syslog, que utiliza o protocolo UDP, envia mensagens de confirmação para cada mensagem recebida.

91 No Windows 7, o Visualizador de Eventos registra as informações em vários *logs* diferentes, incluindo eventos de aplicativo — programas —, eventos relacionados à segurança, eventos de instalação e eventos do sistema.

Julgue os itens subsequentes, referentes a segurança de infraestrutura de tecnologia da informação (TI) e de servidores.

92 As formas de proteger o servidor SMTP contra abusos e ataques incluem não configurar o servidor como *relay* aberto, implementar a autenticação de usuários e limitar o número de conexões.

93 Desabilitar a listagem de diretórios, regulando o acesso aos arquivos, é uma forma de melhorar a segurança de servidores WWW.

94 A configuração de servidores DNS em modo recursivo aberto é uma forma de evitar o uso desses servidores em ataques de negação de serviço por reflexão e amplificação.

Com relação aos sistemas de becape, julgue os itens que se seguem.

95 O becape incremental copia apenas os arquivos que não foram modificados desde o último becape.

96 Diferentemente dos becapes diferenciais, os becapes incrementais são acumulativos.

97 Um becape completo consiste na cópia de todos os arquivos para a mídia de becape.

Julgue os itens subsecutivos, relativos à segurança em redes sem fio.

98 Quando usados no WPA2, os padrões AES e TKIP conferem o mesmo nível de segurança.

99 Ataques realizados por meio de força bruta são os mais eficientes para burlar a segurança do WPA2.

Acerca de *softwares* maliciosos e antivírus, julgue os itens a seguir.

100 Os antivírus que utilizam assinaturas comportamentais são capazes de detectar vírus desconhecidos.

101 Vírus e *worms* são programas capazes de se propagar autonomamente.

Com referência aos ataques a redes de computadores e à proteção de redes e seus *hosts*, julgue os seguintes itens.

102 A renegociação frequente de chaves de sessão e o envio de dados de formulários em segmentos com poucos *bytes*, por meio do método POST, são técnicas usadas em ataques ao SSL/TLS e ao HTTP, as quais envolvem apenas endereços IP reais sem a necessidade de recorrer ao *spoofing*.

103 São medidas que fazem parte das recomendações para *hardening* de sistemas: desabilitação de serviços desnecessários ou sem uso; a minimização de privilégios de escrita, modificação e execução; e a configuração de execução em *jail* ou *sandbox*, sem privilégios administrativos.

104 Entre as formas de detectar ataques de *buffer overflow* inclui-se o uso de assinaturas baseadas na presença de sequências com 0×90, em hexadecimal, nos *payloads* dos datagramas.

105 A configuração de recursos como *Port Security* em *switches* é uma forma eficaz de evitar ataques de MAC *flooding* e *Arp spoofing.*

A respeito de gestão de mudanças, julgue os itens a seguir.

106 A fim de se obter uma transformação mais eficaz, completa e em menor tempo, é importante que o gerenciamento da mudança minimize as resistências.

107 A gestão de mudanças deve promover o equilíbrio entre o lado humano e o lado técnico, ao passo que a transição da situação atual para uma situação desejada futura deve ser definida no escopo do projeto.

108 Para que sejam eficientes, as mudanças tidas como operacionais devem estar alinhadas à estrutura do negócio organizacional e não aos objetivos estratégicos da organização.

Acerca de ataques do tipo *Zero-Day*, julgue os itens subsequentes.

109 Em redes de computadores, ataques do tipo *Zero-Day* são eliminados quando a falha prévia é corrigida no fluxo do pacote assim que ele entra na rede.

110 Ataques do tipo *Zero-Day* apresentam baixa taxa de sucesso na exploração da falha, já que ela é desconhecida do fabricante do produto explorado.

111 Ataques do tipo *Zero-Day* são detectados não só por meio de antivírus, mas também por meio de ferramentas de IDS.

Julgue os itens a seguir, a respeito de testes de invasão em aplicações *web*, banco de dados, sistemas operacionais e dispositivos de redes.

112 Um ataque do tipo CSRF (*cross-site request forgery*) permite que um usuário final execute ações não desejáveis em uma aplicação *web* falha.

113 Uma falha de XSS (*cross-site script)* permite que um atacante insira código malicioso em páginas *web*, de forma a redirecionar, por exemplo, uma resposta a um local controlado pelo atacante.

114 Um ataque do tipo *path transversal* — o qual permite o acesso a arquivos ou diretórios que, em tese, deveriam ser inacessíveis — é eficiente somente em aplicações ASP e JSP.

Com relação a técnicas de segurança com NAC (*network access control*) e NAP (*network access protection*), julgue os itens que se seguem.

115 O protocolo IEEE 802.1X, que é utilizado para implementação de NAC em uma rede de computadores, define encapsulamento do EAP (*extensible authentication protocol*) no padrão IEEE 802.

116 Ao se utilizar uma política de restrição de acesso com NAC, uma VLAN de quarentena é utilizada como um local de acesso restrito, onde determinado cliente deve ser inserido para a aplicação de um *patch* de segurança ou para a atualização do *software* antivírus, antes de ingressar efetivamente na rede de computadores.

117 Uma solução de NAP é utilizada em conjunto com *switches* que possuam um agente NAP e um computador cuja placa de rede use o protocolo DHCP-NAP, que consiste em uma versão estendida do DHCP para autenticação de segurança em redes locais.

Julgue os itens subsequentes, a respeito de SIEM (*security information and event management*), uma tecnologia composta por *software* e sistemas que, entre outras funções, auxiliam no processo de segurança da informação de uma organização.

118 Considerando um fluxo normal, um SIEM é capaz de coletar dados de fontes heterogêneas, extrair informação importante desses dados, agregar valor de interpretação e correlação e apresentar esses dados na forma de relatórios ou informações estatísticas.

119 Um SIEM é capaz de coletar *logs* de diversos dispositivos e fazer a correlação entre eles; entretanto, um SIEM só trabalha com padrão Syslog, que é o padrão internacional de geração de eventos de *log*.

120 Um SIEM pode fazer uso de gerenciadores de banco de dados para armazenar grandes volumes de dados que foram previamente normalizados e que podem ser úteis na resolução de incidentes de rede.

Acerca do uso de SSH (*secure shell*) e TLS (*transport layer security*) em redes e de sistemas de computadores, julgue os próximos itens.

121 Tanto a versão 1 quanto a versão 2 do SSH são imunes a ataques de criptoanálise de tráfego.

122 O TLS, considerado uma evolução do SSL, atualmente está na versão 1.2, e suporta algoritmos como RSA e DH-RSA.

123 O uso de SSH é restrito a sistemas operacionais Unix e Linux. Equipamentos tais como roteadores e *switches* modernos usam apenas mecanismos diferenciados por meio de HTTPS.

A norma NBR 15999 especifica os requisitos de um plano para manter a operação em funcionamento em caso de alguma ocorrência grave no ambiente de negócio. A esse respeito, julgue os itens a seguir.

124 A NBR 15999 faz uso do modelo PDCA (*plan-do-check-act*), de forma a trabalhar o desenvolvimento, a implementação, a manutenção e a melhoria de um sistema de gestão de continuidade do negócio.

125 A NBR 15999 é baseada na ISO 27001, que é considerada como ponto focal da discussão de normas de gestão de continuidade de negócios.

Julgue os itens subsequentes com base no Decreto n.º 3.505/2000, que instituiu a Política de Segurança da Informação nos órgãos e nas entidades da administração pública federal.

126 A tarefa de realizar auditoria nos órgãos e nas entidades da administração pública federal envolvidos com a política de segurança da informação é atribuição exclusiva do Tribunal de Contas da União (TCU).

127 A Secretaria Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação, deve elaborar programas destinados à segurança da informação, de forma a garantir articulação entre os órgãos e as entidades da administração pública federal.

Julgue os próximos itens com base na Instrução Normativa MPOG n.º 4/2014, que dispõe acerca do processo de contratação de soluções de tecnologia da informação (TI) pelos órgãos integrantes do sistema de administração dos recursos de TI.

128 A referida instrução normativa não se aplica às contratações de soluções de TI que possam comprometer a segurança nacional.

129 A referida instrução normativa aplica-se aos casos em que as contratações têm estimativas de preços inferiores ao disposto no art. 23 da Lei n.º 8.666/1993.

130 Segundo a instrução, a área requisitante da solução é definida como a unidade do órgão ou da entidade que demande a contratação de uma solução de TI.