Estratégia Concursos

Aula 01

TJ-RJ (Analista de TI - Analista de Projetos) Segurança da Informação - 2021 (Pós-Edital)

Autor:
André Castro, Diego Carvalho, Equipe Informática e TI

09 de Outubro de 2021

ISO 27001 E ISO 27002

A norma ISO 27001 de define os **requisitos de um Sistema de Gestão de Segurança da Informação – SGSI**. Veremos esse termo constantemente ao longo da nossa aula.

Essa norma é um padrão e referência Internacional para a gestão da Segurança da Informação. Possui como objetivo a provisão de requisitos para **ESTABELECER, IMPLEMENTAR, MANTER E MELHORAR CONTINUAMENTE** um SGSI.

A família 27000 possui uma visão integrada de diversas outras normas e boas práticas de segurança e governança. Então constantemente veremos termos que nos remetem a essas ações, como é o próprio ciclo do PDCA, representado pelas 4 etapas do parágrafo anterior.

A norma é dividida em 10 tópicos e 1 anexo de referência. Os tópicos são os seguintes:

1. **ESCOPO;**
2. **REFERÊNCIA NORMATIVA;**
3. **TERMOS e DEFINIÇÕES;**
4. **Contexto da ORGANIZAÇÃO;**
5. **LIDERANÇA;**
6. **PLANEJAMENTO;**
7. **APOIO;**
8. **OPERAÇÃO;**
9. **AVALIAÇÃO do DESEMPENHO;**
10. **MELHORIA;**

1) ESCOPO

Nesta parte da norma é onde encontramos, além dos itens já apresentados no objetivo, outros pontos que também são considerados em relação à Segurança da Informação por intermédio do SGSI. Quais sejam:

ESTABELECER
IMPLEMENTAR
OPERAR
MONITORAR
REVISAR
MANTER
MELHORAR

Ainda no escopo, podemos encontrar requisitos para avaliação e tratamento de riscos.

Um ponto de destaque é que **os itens de 4 a 10 da norma são obrigatórios** para fins de CONFORMIDADE, ou seja, para uma instituição poder estar adaptada à norma, deve considerar esses itens.

Obviamente, a construção da norma deve contemplar qualquer tipo de organização, sem restrição de tipo, tamanho ou natureza. Por isso ela é considerada genérica nesse sentido.

2) REFERÊNCIA NORMATIVA

Aqui, temos apenas uma referência de que a norma está ancorada na família 27000, que abrange uma série de outras questões no âmbito da Segurança da Informação.

3) TERMOS DE DEFINIÇÕES

Mais uma vez, tem-se a mera referência aos termos e definições presentes na família 27000. Veremos todos esses termos ao longo da nossa aula e complementaremos em nossos exercícios.

4) CONTEXTO DA ORGANIZAÇÃO

O SGSI não pode ser um documento avulso na organização. Para a sua construção, deve-se levar em conta a realidade da organização.

Por isso é importante **ENTENDER A ORGANIZAÇÃO E SEU CONTEXTO**, bem como as **NECESSIDADES E EXPECTATIVAS DAS PARTES INTERESSADAS.** Obviamente, deve-se determinar também quem são as partes interessadas.

Assim, deve-se considerar questões internas e externas relevantes para a organização alcançar os resultados esperados.

Por fim, deve-se considerar o escopo do SGSI, tudo devidamente documentado e disponível.

5) LIDERANÇA

Como todo bom processo e robusto em uma instituição, a abordagem TOP-DOWN é fundamental, ou seja, é preciso que alta direção da organização esteja devidamente alinhada e comprometida com a causa, exercendo, de fato, a liderança na condução do processo.

Então a liderança também deverá atuar na construção da Política de Segurança da Informação – POSIC (falaremos mais sobre ela adiante), deverá participar no processo de decisão das autoridades, responsabilidades e papéis organizacionais que serão os atores diretos relacionados a assuntos de Segurança da Informação.

Um ponto que merece destaque é em relação à Política de Segurança da Informação. Na subseção 2 deste tópico, temos que a Alta Direção deve estabelecer uma Política que:

1. Seja apropriada ao propósito da organização;
2. Inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação;
3. Inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a SI;
4. Inclua o comprometimento com a melhoria contínua do sistema de gestão da SI;

Ainda em relação à POSIC, ela deve:

a) Estar disponível como informação documentada;
b) Ser comunicada dentro da organização; e
c) Estar disponível para as partes interessadas, conforme apropriado.

6) PLANEJAMENTO

Como já é de amplo conhecimento, aspectos relacionados a tecnologia da informação e, especificamente nesse contexto, a Segurança da Informação, dependem de ações planejadas e programadas.

Por esse motivo há um rito muito bem definido na construção de um SGSI, onde se tem o alinhamento da Alta Direção... Depois a determinação das diretrizes em uma POSIC, para então dar seguimentos às demais ações.

Assim, o planejamento é importante para mapear os riscos e oportunidades no âmbito do SGSI, com rotinas de avaliação contínua nesse processo.

Quando se conhece os riscos e oportunidades, é possível acompanha-los e medi-los, com definições claras de como trata-los em caso de ocorrência.

Assim, no processo de avaliação dos riscos, deve-se determinar critérios claros para a **ACEITAÇÃO DO RISCO e para o DESEMPENHO DAS AVALIAÇÕES DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO.**

Nesse processo, é sempre necessário, após a identificação dos riscos, mapear os responsáveis por eles.

7) APOIO

Quando falamos de APOIO, temos uma visão vertical e horizontal. Temos algumas ações que precisam ser consideradas no âmbito desse apoio:

a) RECURSOS
   a. A organização deve determinar e prover recursos necessários para o **estabelecimento, implementação, manutenção e melhoria contínua do SGSI.**
b) COMPETÊNCIA
   a. A partir da determinação da competência necessárias para as ações, deve-se assegurar que os responsáveis também tenham a competência devida,

provendo a educação e capacitação necessárias, com a devida documentação dos processos.

c) CONSCIENTIZAÇÃO
   a. Todas as pessoas da organização devem conhecer a POSIC e os demais documentos, criando uma ação integrada da organização.

d) COMUNICAÇÃO
   a. Deve-se ter rotinas muito bem definidas de comunicações internas e externas para o SGSI, considerando “O QUE”, “QUANDO”, “QUEM” e o “PROCESSO”.

e) INFORMAÇÃO DOCUMENTADA
   a. Por ser um procedimento formal e relevante na organização, deve-se estabelecer rotinas de documentação para o SGSI, permitindo a criação e atualização de maneira facilitada, com o devido controle e versionamento.

A partir das próximas seções, veremos os conceitos de maneira conjugada entre a norma 27001 e 27002.

Antes disso, vamos aproveitar para também termos uma visão da estrutura da norma 27002.

A ISO 27002 apresenta **um código de boas práticas com controles de Segurança da Informação para o SGSI**.

Em sua estrutura, temos um correlacionamento direto com a ISO 27001, até porque, ela trata das boas práticas, certo? Todas os controles e objetivos de controle estão previstos no ANEXO da 27001 e são detalhados na 27002.

Esta última é dividida em 14 seções de controle de Segurança da Informação, de um total de 35 objetivos de controles e 114 controles, de fato.

As provas variam bastante em termos de nível de cobrança... Alguns pontos são bem batidos e alvos constantes de uma análise mais detalhada. Por isso, reforço, a importância de fazermos bastante exercícios.

Para termos uma visão, vou apresentar a relação de todos itens, considerando os objetivos de controle e seus respectivos controles. É importante que vocês tenham uma visão geral de todos os itens que são abordados na norma para detalharmos e fazermos as considerações posteriormente.

Um ponto que gostaria de chamar sua atenção é para o fato de você realizar a leitura pensando, de fato, como isso acontece na sua organização de trabalho (para você que trabalha) ou, então, tente mentalizar as possibilidades.

A melhor forma de “decorar/aprender” os conceitos, é entendendo que tudo faz sentido!!!

“QUE SACADA ANDRÉ!!! A RECEITA DO SUCESSO...”

Brincadeiras à parte, você entender o porquê é necessário definir responsabilidades.... O porquê é importante ter rotinas para controle de uso de dispositivos móveis... O porquê da necessidade de rotinas de backup... O porquê é necessário se preocupar com funcionário antes, durante e depois da contratação...

Então quando uma questão cair na prova, ainda que você não lembre a literalidade da norma, o assunto e afirmação fará algum sentido. Portanto, vamos conhecer a estrutura da Norma...

---

1. **Políticas de segurança da informação**
    a. Orientação da Direção para segurança da informação
        i. Políticas para segurança da Informação
        ii. Análise crítica das políticas para Segurança da Informação;
2. **Organização da Segurança da Informação**
    a. Organização Interna
        i. Responsabilidades e papéis pela Segurança da Informação;
        ii. Segregação de Funções;
        iii. Contato com Autoridades;
        iv. Contato com grupos Especiais;
        v. Segurança da Informação no gerenciamento de projetos;
    b. Dispositivos móveis e trabalho remoto
        i. Política para uso de dispositivo móvel
        ii. Trabalho Remoto
3. **Segurança em Recursos Humanos**
    a. Antes da Contratação
        i. Seleção
        ii. Termos e Condições de Contratação;
    b. Durante a Contratação
        i. Responsabilidades da Direção
        ii. Conscientização, educação e treinamento em segurança da informação;
        iii. Processo disciplinar;

c. Encerramento e mudança da contratação
    i. Responsabilidades pelo encerramento ou mudança da contratação;

4. Gestão de Ativos

a. Responsabilidade pelos ativos
    i. Inventário dos ativos
    ii. Proprietário dos ativos
    iii. Uso aceitável dos ativos
    iv. Devolução dos ativos
b. Classificação da Informação
    i. Classificação da Informação
    ii. Rótulos e tratamento da Informação
    iii. Tratamento dos Ativos
c. Tratamento de Mídias
    i. Gerenciamento de mídias removíveis
    ii. Descarte de mídias
    iii. Transferência física de mídias

5. Controle de Acesso

a. Requisitos do negócio para controle de acesso
    i. Política de controle de acesso
    ii. Acesso às redes e aos serviços de rede
b. Gerenciamento de acesso do usuário
    i. Registro e cancelamento de usuário
    ii. Provisionamento para acesso de usuário
    iii. Gerenciamento de direitos de acesso privilegiados
    iv. Gerenciamento da informação de autenticação secreta de usuários
    v. Análise crítica dos direitos de acesso de usuário
    vi. Retirada ou ajuste dos direitos de acesso
c. Responsabilidades dos usuários
    i. Uso da informação de autenticação secreta
d. Controle de acesso ao sistema e à aplicação
    i. Restrição de acesso à informação
    ii. Procedimentos seguros de entrada no sistema (log-on)
    iii. Sistema de Gerenciamento de senha
    iv. Uso de programas utilitários privilegiados
    v. Controle de acesso ao código-fonte de programas

6. Criptografia

a. Controles criptográficos
    i. Política para o uso de controles criptográficos
    ii. Gerenciamento de chaves

7. Segurança física e do ambiente

a. Áreas Seguras
    i. Perímetro de segurança física
    ii. Controles de entrada física
    iii. Segurança em escritórios, salas e instalações
    iv. Proteção contra ameaças externas e do meio ambiente
    v. Trabalhando em áreas seguras

vi. Áreas de entrega e de carregamento

b. Equipamento
   i. Localização e proteção do equipamento
   ii. Utilidades
   iii. Segurança do cabeamento
   iv. Manutenção dos equipamentos
   v. Remoção de ativos
   vi. Segurança de equipamentos e ativos fora das dependências da organização
   vii. Reutilização ou descarte seguro de equipamentos
   viii. Equipamento de usuário sem monitoração
   ix. Política de mesa limpa e tela limpa

8. Segurança nas operações

a. Responsabilidades e procedimentos operacionais
   i. Documentação dos procedimentos de operação
   ii. Gestão de mudanças
   iii. Gestão de capacidade
   iv. Separação dos ambientes de desenvolvimento, teste e produção
b. Proteção contra malware
   i. Controles contra malware
c. Cópias de Segurança
   i. Cópias de segurança das informações
d. Registros e monitoramento
   i. Registros de eventos
   ii. Proteção das informações dos registros de eventos (logs)
   iii. Registros de eventos (log) de administrador e operador
   iv. Sincronização dos relógios
e. Controle de software operacional
   i. Instalação de software nos sistemas operacionais
f. Gestão de vulnerabilidades técnicas
   i. Gestão de vulnerabilidades técnicas
   ii. Restrições quanto à instalação de software
g. Considerações quanto à auditoria de sistemas da informação
   i. Controles de auditoria de sistemas de informação

9. Segurança das comunicações

a. Gerenciamento da segurança em redes
   i. Controles de redes
   ii. Segurança dos serviços de rede
   iii. Segregação de redes
b. Transferência de informação
   i. Políticas e procedimentos para transferência de informações
   ii. Acordos para transferência de informações
   iii. Mensagens eletrônicas
   iv. Acordos de confidencialidade e não divulgação

10. Aquisição, Desenvolvimento e Manutenção de Sistemas

a. Requisitos de Segurança de sistemas de informação

i. Análise e especificação dos requisitos de segurança da informação
ii. Serviços de aplicação seguros em redes públicas
iii. Protegendo as transações nos aplicativos de serviços

b. Segurança em processos de desenvolvimento e de suporte
i. Política de desenvolvimento seguro
ii. Procedimentos para controle de mudanças de sistemas
iii. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
iv. Restrições sobre mudanças em pacotes de software
v. Princípios para projetar sistemas seguros
vi. Ambiente seguro para desenvolvimento
vii. Desenvolvimento terceirizado
viii. Teste de segurança do sistema
ix. Teste de aceitação de sistemas

c. Dados para teste
i. Proteção dos dados para teste

11. Relacionamento na Cadeia de Suprimento

a. Segurança da informação na cadeia de suprimento
i. Política de segurança da informação no relacionamento com os fornecedores
ii. Identificando segurança da informação nos acordos com fornecedores
iii. Cadeia de suprimento na tecnologia da informação e comunicação

b. Gerenciamento da entrega do serviço do fornecedor
i. Monitoramento e análise crítica de serviços com fornecedores
ii. Gerenciamento de mudanças para serviços com fornecedores

12. Gestão de Incidentes de Segurança da Informação

a. Gestão de incidentes de segurança da informação e melhorias
i. Responsabilidades e procedimentos
ii. Notificação de eventos de segurança da informação
iii. Notificando fragilidades de segurança da informação
iv. Avaliação e decisão dos eventos de segurança da informação
v. Resposta aos incidentes de segurança da informação
vi. Aprendendo com os incidentes de segurança da informação
vii. Coleta de evidências

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

a. Continuidade da Segurança da Informação
i. Planejando a continuidade da segurança da informação
ii. Implementando a continuidade da segurança da informação
iii. Verificação, análise crítica e avaliação da continuidade da segurança da informação

b. Redundâncias
i. Disponibilidade dos recursos de processamento da informação

14. Conformidade

a. Conformidade com requisitos legais e contratuais
i. Identificação da legislação aplicável e de requisitos contratuais

ii. Direitos de propriedade intelectual
iii. Proteção de registros
iv. Proteção e privacidade de informações de identificação pessoal
v. Regulamentação de controles de criptografia

b. Análise crítica da segurança da informação
i. Análise crítica independente da segurança da informação
ii. Conformidade com as políticas e procedimentos de segurança da informação
iii. Análise crítica da conformidade técnica

UFAAA!!!! Chegamos ao término da lista topicalizada que já nos ajuda a responder boa parte das questões.

Agora nós avançaremos com nossa aula destacando os principais objetivos e controles para efeito de provas de concursos.

Vocês perceberão nas questões, que muitas delas são intuitivas e, com o mínimo de bom senso, é possível responde-las.

Acrescentando um outro aspecto à nossa discussão é que em todo o tempo, considerando os controles, podemos perceber a norma utilizar o termo “CONVÉM”, justamente porque são ações e controles que merecem a atenção por parte das organizações.

---

1) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ESTRUTURA

a. Orientação da Direção para segurança da informação
i. Políticas para segurança da Informação
ii. Análise crítica das políticas para Segurança da Informação;

A Política de Segurança da Informação (POSIC) é o principal instrumento de uma instituição no que tange à Segurança.

Ela servirá de base para a construção de outras políticas internas, normas operacionais e padrões de ações dos agentes de uma instituição.

Ela prima ainda por um outro fator que é a determinação do GESTOR DE SEGURANÇA de uma organização. Esse será o responsável pelas tomadas de decisão referentes ao assunto.

Além disso, um fator que sempre surge nas realidades de tecnologia das organizações é a questão do apoio estratégico da alta direção. Na POSIC, há o firmamento do compromisso da alta direção em relação à pauta, principalmente no que tange a investimentos financeiros que se façam necessários.

Esta Seção possui um único objetivo:

1. Orientação da Direção para a Segurança da Informação

OBJETIVO

Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevante.

Esse objetivo é dividido em dois controles:

i. Políticas para segurança da Informação

CONTROLE

Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

ii. Análise crítica das políticas para Segurança da Informação

CONTROLE

Convém que as políticas de segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Nesses controles, é importante destacar a aprovação da POSIC pela direção da instituição, **com posterior publicação e comunicação a todos os funcionários e às partes externas envolvidas.**

Então, cuidado... A POSIC alcança a todos que possuem alguma relação com a instituição, seja internamente, seja externamente.

Além disso, diz-se que a POSIC é um documento vivo. Em sua construção, deve-se conter um tópico específico que determine a periodicidade de revisão e atualização, podendo ser de 2 em 2 anos, ou 3 em 3, por exemplo.

Entretanto, como a POSIC deve representar o contexto estratégico da organização, caso haja mudanças significativas, obviamente a POSIC também deve acompanhar essa realidade, podendo ser, nesse horizonte, atualizada a qualquer tempo.

2) ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

ESTRUTURA

a. Organização Interna
   i. Responsabilidades e papéis pela Segurança da Informação;
   ii. Segregação de Funções;
   iii. Contato com Autoridades;
   iv. Contato com grupos Especiais;
   v. Segurança da Informação no gerenciamento de projetos;
b. Dispositivos móveis e trabalho remoto
   i. Política para uso de dispositivo móvel
   ii. Trabalho Remoto

Esta Seção possui dois objetivos:

1. Organização Interna

OBJETIVO

Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

Esse objetivo é dividido em cinco controles:

i. Responsabilidades e papéis pela Segurança da Informação;

CONTROLE

Convém que todas as responsabilidades pela segurança da informação sejam definidas.

ii. Segregação de Funções;

CONTROLE

Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

iii. Contato com Autoridades;

CONTROLE

Convém que contatos apropriados com autoridades relevantes sejam mantidos.

iv. Contato com grupos Especiais;

CONTROLE

Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.

v. Segurança da Informação no gerenciamento de projetos;

CONTROLE

Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo de projeto.

Dispositivos móveis e trabalho remoto

OBJETIVO

Garantir a segurança das informações no trabalho remoto e no uso de dispositivo móveis.

Esse objetivo é dividido em dois controles:

i. *Política para uso de dispositivo móvel*

CONTROLE

Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.

ii. *Trabalho Remoto*

CONTROLE

Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

3) SEGURANÇA EM RECURSOS HUMANOS

ESTRUTURA

a. Antes da Contratação
    i. Seleção
    ii. Termos e Condições de Contratação;
b. Durante a Contratação
    i. Responsabilidades da Direção
    ii. Conscientização, educação e treinamento em segurança da informação;
    iii. Processo disciplinar;
c. Encerramento e mudança da contratação
    i. Responsabilidades pelo encerramento ou mudança da contratação;

Esta Seção possui três objetivos:

1. Antes da Contratação

OBJETIVO

Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Esse objetivo é dividido em dois controles:

i. Seleção

CONTROLE

Convém que **verificações do histórico sejam realizadas para todos os candidatos a emprego**, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.

ii. Termos e Condições de Contratação;

CONTROLE

Convém que as obrigações contratuais com funcionários e partes externas declarem a sua responsabilidade e as da organização para a segurança da informação.

2. Durante a Contratação

OBJETIVO

Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

Esse objetivo é dividido em três controles:

i. Responsabilidades da Direção

CONTROLE

Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

ii. Conscientização, educação e treinamento em segurança da informação;

CONTROLE

Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as

iii. Processo disciplinar;

CONTROLE

Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.

3. Encerramento e mudança da contratação

OBJETIVO

Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

Esse objetivo possui um único controle:

i. *Responsabilidades pelo encerramento ou mudança da contratação;*

CONTROLE

Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas.

4) GESTÃO DE ATIVOS

ESTRUTURA

a. Responsabilidade pelos ativos
   i. Inventário dos ativos
   ii. Proprietário dos ativos
   iii. Uso aceitável dos ativos
   iv. Devolução dos ativos
b. Classificação da Informação
   i. Classificação da Informação
   ii. Rótulos e tratamento da Informação
   iii. Tratamento dos Ativos
c. Tratamento de Mídias
   i. Gerenciamento de mídias removíveis
   ii. Descarte de mídias
   iii. Transferência física de mídias

Esta seção é muito importante para efeitos de provas e constante tem caído. Portanto, leia com atenção especial a sua estrutura e termos utilizados.

Esta Seção possui três objetivos:

1. Responsabilidade pelos Ativos

OBJETIVO

Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

Esse objetivo é dividido em quatro controles:

i. *Inventários dos ativos*

CONTROLE

Convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estruturado e mantido.

ii. *Proprietário dos ativos*

CONTROLE

Convém que os ativos mantidos no inventário tenham um proprietário.

iii. *Uso aceitável dos ativos*

CONTROLE

Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas.

iv. Devolução dos ativos

CONTROLE

Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

2. Classificação da Informação

OBJETIVO

Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Esse objetivo é dividido em três controles:

i. Classificação da Informação

CONTROLE

Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Esse controle específico recorrentemente cai em prova, seja no âmbito da ISO 27002, seja nos próprios conceitos relacionados à classificação da informação.

Por isso, vamos falar um pouco mais sobre ele à luz da ISO 27002. Quando falamos de segurança da informação, obviamente vinculamos ao conceito de Tecnologia da Informação.

Entretanto, no que tange à informação, o responsável por definir a criticidade, sensibilidade, aspectos legais, entre outros, é a área de negócio responsável por aquela informação. Uma vez definida e enquadrada na categoria devida, dá-se o devido tratamento conforme política e diretrizes de tratamento da informação definidas.

Um outro ponto, é que a norma sugere que os proprietários da informação e ativos sejam os próprios responsáveis por sua classificação.

Desta feita, um padrão definido para as categorias deve contemplar todas as áreas da organização, fazendo sentido para todos, mantendo um entendimento em comum. Não há uma restrição apenas para a alta gerência.

A informação e classificação são instrumentos dinâmicos, podendo mudar, conforme valor, criticidade, sensibilidade e requisitos legais.

Um outro ponto importante é em relação à troca de informações entre organizações. Quando uma informação da organização B, com um determinado nível de classificação

passa para a organização A, deve-se realizar um trabalho de análise e rotulação da informação para verificar a equivalência e aplicação dos níveis referentes ao valor, sensibilidade e criticidade, não necessariamente mantendo o padrão da origem.

ii. Rótulos e tratamento da informação

CONTROLE

Convém que um conjunto apropriado de procedimento para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotada pela organização.

iii. Tratamento dos ativos

CONTROLE

Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.

3. Tratamento de mídias

OBJETIVO

Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Esse objetivo é dividido em três controles:

i. Gerenciamento de mídias removíveis

CONTROLE

Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis de acordo com o esquema de classificação adotado pela organização.

ii. Descarte de mídias

CONTROLE

Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

iii. Transferência física de mídias

CONTROLE

Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

5) CONTROLE DE ACESSO

ESTRUTURA

a. Requisitos do negócio para controle de acesso
    i. Política de controle de acesso
    ii. Acesso às redes e aos serviços de rede
b. Gerenciamento de acesso do usuário
    i. Registro e cancelamento de usuário
    ii. Provisionamento para acesso de usuário
    iii. Gerenciamento de direitos de acesso privilegiados
    iv. Gerenciamento da informação de autenticação secreta de usuários
    v. Análise crítica dos direitos de acesso de usuário
    vi. Retirada ou ajuste dos direitos de acesso
c. Responsabilidades dos usuários
    i. Uso da informação de autenticação secreta
d. Controle de acesso ao sistema e à aplicação
    i. Restrição de acesso à informação
    ii. Procedimentos seguros de entrada no sistema (log-on)
    iii. Sistema de Gerenciamento de senha
    iv. Uso de programas utilitários privilegiados
    v. Controle de acesso ao código-fonte de programas

Esta Seção possui quatro objetivos:

1. Requisitos do negócio para controle de acesso

OBJETIVO

Limitar o acesso à informação e aos recursos de processamento da informação.

Esse objetivo é dividido em dois controles:

i. Política de controle de acesso

CONTROLE

Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

Esse um ponto que recorrentemente cai em prova tratando do CONTROLE em questão e alguns aspectos operacionais. Vamos ver um pouco mais sobre isso nos exercícios uma vez que há uma consideração direta para cada banca.

Um outro ponto que quero fazer destaque é em relação ao que deve ser considerado nessa política. **Na Norma, há uma consideração nas informações adicionais que temos o fato de que deve ser considerado, de maneira conjunta, a segurança física e lógica.** Tais aspectos operacionais são tratados na Seção **de SEGURANÇA FÍSICA E DO AMBIENTE,** que veremos logo mais.

ii. Acesso às redes e aos serviços de rede

CONTROLE

Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

2. Gerenciamento de acesso do usuário

OBJETIVO

Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

Esse objetivo é dividido em seis controles:

i. Registro e cancelamento de usuário

CONTROLE

Convém que um processo formal de registro e cancelamento de usuários seja implementado para permitir atribuição dos direitos de acesso.

ii. Provisionamento para acesso de usuário

CONTROLE

Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os teipos de sistemas e serviços.

iii. Gerenciamento de direitos de acesso privilegiados

CONTROLE

Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados.

iv. Gerenciamento da informação de autenticação secreta de usuários

CONTROLE

Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

v. Análise crítica dos direitos de acesso de usuário

CONTROLE

Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

vi. Retirada ou ajuste dos direitos de acesso

CONTROLE

Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos eou acordos, ou ajustados após a mudança destas atividades.

3. Responsabilidades dos Usuários

OBJETIVO

Tornar os usuários responsáveis pela proteção das suas informações de autenticação.

Esse objetivo possui um único controle:

i. Uso da informação de autenticação secreta

CONTROLE

Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

4. Controle de acesso ao sistema e à aplicação

OBJETIVO

Prevenir o acesso não autorizado aos sistemas e aplicações.

Esse objetivo é dividido em cinco controles:

i. Restrição de acesso à informação

CONTROLE

Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

ii. Procedimentos seguros de entrada no sistema (log-on)

CONTROLE

Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on).

Um ponto que tem aparecido em prova é a lista de procedimentos a serem considerados no procedimento de LOG-ON. Portanto, é importante trazer o conteúdo exato da norma para absorvermos o conhecimento:

a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso;

b) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;

c) não forneça mensagens de ajuda durante o procedimento de entrada (log-on) que poderiam auxiliar um usuário não autorizado;

d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correto ou incorreto;

e) proteja contra tentativas forçadas de entrada no sistema (log-on);

f) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida;

g) comunique um evento de segurança caso uma tentativa potencial ou uma violação bem sucedida de entrada no sistema (log-on), seja detectada;

h) mostre as seguintes informações quando o procedimento de entrada no sistema (log-on) finalizar com sucesso:

1) data e hora da última entrada no sistema (log-on) com sucesso;

2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (log-on) desde o último acesso com sucesso;

i) não mostre a senha que está sendo informada;

j) não transmita senhas em texto claro pela rede;

k) encerre sessões inativas após um período definido de inatividade, especialmente em locais de alto risco, tais como, locais públicos, ou àreas externas ao gerenciamento de segurança da organização ou quando do uso de dispositivos móveis;

l) restrinja os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e reduzir a janela de oportunidade para acesso não autorizado.

iii. Sistema de Gerenciamento de senha

CONTROLE

Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

iv. Uso de programas utilitários privilegiados

CONTROLE

Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado.

v. Controle de acesso ao código-fonte de programas

CONTROLE

Convém que o acesso ao código-fonte de programa seja restrito.

Não é muito difícil imaginar que o acesso ao código-fonte deve ser restrito. Entretanto, nesse quesito, o que costuma aparecer em prova é em termos operacionais de como proceder.

A norma traz algumas orientações que merecem destaque:

- Considerar um repositório centralizado para tal procedimento. Semelhante ao processo de gerenciamento de LOG's;
- Evitar manter as bibliotecas de programas-fonte no mesmo ambiente dos sistemas operacionais;

- Não permitir um controle irrestrito das equipes de suporte aos programas-fonte;
- A listagem dos programas seja mantida em ambiente seguro;

---

6) CRIPTOGRAFIA

ESTRUTURA

a. Controles criptográficos
   i. Política para o uso de controles criptográficos
   ii. Gerenciamento de chaves

Esta Seção um único objetivo:

1. Controles criptográficos

OBJETIVO

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação.

Esse objetivo é dividido em dois controles:

i. Política para o uso de controles criptográficos

CONTROLE

Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação.

A norma traz um rol de objetivos dos controles criptográficos. A saber:

1. **Confidencialidade** – Usa a criptografia para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;
2. **Integridade/Autenticidade** – Referência ao uso de assinaturas digitais;

3. **Não Repúdio –** Uso de técnicas para obter evidência da ocorrência ou não ocorrência de um evento ou ação;
4. **Autenticação –** Uso de técnicas para autenticas usuários e outras camadas sistêmicas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

ii. Gerenciamento de chaves

CONTROLE

Convém que uma política sobre o uso, proteção e tempo de vida das chaves criptográficas seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

7) SEGURANÇA FÍSICA E DO AMBIENTE

ESTRUTURA

a. Áreas Seguras
   i. Perímetro de segurança física
   ii. Controles de entrada física
   iii. Segurança em escritórios, salas e instalações
   iv. Proteção contra ameaças externas e do meio ambiente
   v. Trabalhando em áreas seguras
   vi. Áreas de entrega e de carregamento
b. Equipamento
   i. Localização e proteção do equipamento
   ii. Utilidades
   iii. Segurança do cabeamento
   iv. Manutenção dos equipamentos
   v. Remoção de ativos
   vi. Segurança de equipamentos e ativos fora das dependências da organização
   vii. Reutilização ou descarte seguro de equipamentos
   viii. Equipamento de usuário sem monitoração

Esta Seção é dividida em dois objetivos:

1. Áreas Seguras

OBJETIVO

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.

Esse objetivo é dividido em cinco controles:

i. Perímetro de segurança física

CONTROLE

Convém que perímetros de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.

ii. Controles de entrada física

CONTROLE

Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

iii. Segurança em escritórios, salas e instalações

CONTROLE

Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

iv. Proteção contra ameaças externas e do meio ambiente

CONTROLE

Convém que seja projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes.

v. Trabalhando em áreas seguras

CONTROLE

Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras.

vi. Áreas de entrega e de carregamento

CONTROLE

Convém que pontos de acesso, como áreas de entrada e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

2. EQUIPAMENTO

OBJETIVO

Impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações da organização.

Esse objetivo é dividido em nove controles:

i. Localização e proteção do equipamento

CONTROLE

Convém que os equipamentos sejam protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

ii. Utilidades

CONTROLE

Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

iii. Segurança do cabeamento

CONTROLE

Convém que o cabeamento de energia e de telecomunicações que transporte dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.

iv. Manutenção dos equipamentos

CONTROLE

Convém que os equipamentos tenham uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.

v. *Remoção de ativos*

CONTROLE

Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

vi. *Segurança de equipamentos e ativos fora das dependências da organização*

CONTROLE

Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

vii. *Reutilização ou descarte seguro de equipamentos*

CONTROLE

Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes da reutilização, para assegurar que todos os dados sensíveis e software licenciados tenham sido removidos ou sobregravados com segurança.

viii. *Equipamento de usuário sem monitoração*

CONTROLE

Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

ix. Política de mesa limpa e tela limpa

CONTROLE

Convém que sejam adotadas políticas de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

8) SEGURANÇA NAS OPERAÇÕES

ESTRUTURA

a. Responsabilidades e procedimentos operacionais
    i. Documentação dos procedimentos de operação
    ii. Gestão de mudanças
    iii. Gestão de capacidade
    iv. Separação dos ambientes de desenvolvimento, teste e produção
b. Proteção contra malware
    i. Controles contra malware
c. Cópias de Segurança
    i. Cópias de segurança das informações
d. Registros e monitoramento
    i. Registros de eventos
    ii. Proteção das informações dos registros de eventos (logs)
    iii. Registros de eventos (log) de administrador e operador
    iv. Sincronização dos relógios
e. Controle de software operacional
    i. Instalação de software nos sistemas operacionais
f. Gestão de vulnerabilidades técnicas
    i. Gestão de vulnerabilidades técnicas
    ii. Restrições quanto à instalação de software
g. Considerações quanto à auditoria de sistemas da informação
    i. Controles de auditoria de sistemas de informação

Esta Seção é dividida em sete objetivos:

1. Responsabilidades e procedimentos operacionais

OBJETIVO

Garantir a operação segura e correta dos recursos de processamento da informação.

Esse objetivo é dividido em quatro controles:

i. Documentação dos procedimentos de operação

CONTROLE

Convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles.

ii. Gestão de mudanças

CONTROLE

Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.

iii. Gestão de capacidade

CONTROLE

Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para a necessidade de capacidade futura para garantir o desempenho requerido do sistema.

iv. Separação dos ambientes de desenvolvimento, teste e produção

CONTROLE

Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

2. Proteção contra códigos maliciosos

OBJETIVO

Assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware.

Esse objetivo possui um único controle:

i. Controles contra códigos maliciosos

CONTROLE

Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário.

3. Cópias de Segurança

OBJETIVO

Proteger contra perda de dados.

Esse objetivo possui um único controle:

i. Cópias de segurança das informações

CONTROLE

Convém que cópias de segurança das informações, dos softwares e das imagens do sistema sejam efetuadas e testadas regularmente conforma a política de geração de cópias de segurança definida.

4. Registros e monitoramento

OBJETIVO

Registrar eventos e gerar evidências.

Esse objetivo possui quatro controles:

i. *Registros de eventos*

CONTROLE

Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.

ii. *Proteção das informações dos registros de eventos (logs)*

CONTROLE

Convém que as informações dos registros de eventos (log) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração.

iii. *Registros de eventos (log) de administrador e operador*

CONTROLE

Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

iv. Sincronização dos relógios

CONTROLE

Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.

5. Controle de software operacional

OBJETIVO

Assegurar a integridade dos sistemas operacionais.

Esse objetivo possui um único controle:

i. Instalação de software nos sistemas operacionais

CONTROLE

Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

6. Gestão de vulnerabilidades técnicas

OBJETIVO

Prevenir a exploração de vulnerabilidade técnicas.

Esse objetivo possui dois controles:

i. *Gestão de vulnerabilidades técnicas*

CONTROLE

Convém que as informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades seja avaliada e que sejam tomadas as medidas apropriadas para lidas com os riscos associados.

ii. *Restrições quanto à instalação de software*

CONTROLE

Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.

7. Considerações quanto à auditoria de sistemas da informação

OBJETIVO

Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

Esse objetivo possui um único controle:

i. *Controles de auditoria de sistemas de informação*

CONTROLE

Convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

9) SEGURANÇA DAS COMUNICAÇÕES

ESTRUTURA

a. Gerenciamento da segurança em redes
   i. Controles de redes
   ii. Segurança dos serviços de rede
   iii. Segregação de redes
b. Transferência de informação
   i. Políticas e procedimentos para transferência de informações
   ii. Acordos para transferência de informações
   iii. Mensagens eletrônicas
   iv. Acordos de confidencialidade e não divulgação

Esta Seção é dividida em dois objetivos:

1. Gerenciamento da segurança em redes

OBJETIVO

Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.

Esse objetivo é dividido em três controles:

i. Controles de redes

CONTROLE

Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

ii. Segurança dos serviços de rede

CONTROLE

Convém que mecanismos de segurança, níveis de serviços e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

iii. Segregação de redes

CONTROLE

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

2. Transferência de Informação

OBJETIVO

Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

Esse objetivo é dividido em quatro controles:

i. Políticas e procedimentos para transferência de informações

CONTROLE

Convém que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

ii. Acordos para transferência de informações

CONTROLE

Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e as partes externas.

iii. Mensagens eletrônicas

CONTROLE

Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

iv. Acordos de confidencialidade e não divulgação

CONTROLE

Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidadess da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.

10) AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

ESTRUTURA

a. Requisitos de Segurança de sistemas de informação
   i. Análise e especificação dos requisitos de segurança da informação
   ii. Serviços de aplicação seguros em redes públicas
   iii. Protegendo as transações nos aplicativos de serviços
b. Segurança em processos de desenvolvimento e de suporte
   i. Política de desenvolvimento seguro
   ii. Procedimentos para controle de mudanças de sistemas
   iii. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
   iv. Restrições sobre mudanças em pacotes de software
   v. Princípios para projetar sistemas seguros
   vi. Ambiente seguro para desenvolvimento
   vii. Desenvolvimento terceirizado
   viii. Teste de segurança do sistema
   ix. Teste de aceitação de sistemas
c. Dados para teste
   i. Proteção dos dados para teste

Esta Seção é dividida em dois objetivos:

1. Requisitos de Segurança de sistemas de informação

OBJETIVO

Garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviço sobre as redes públicas.

Esse objetivo é dividido em três controles:

i. *Análise e especificação dos requisitos de segurança da informação*

CONTROLE

Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

ii. *Serviços de aplicação seguros em redes públicas*

CONTROLE

Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

iii. *Protegendo as transações nos aplicativos de serviços*

CONTROLE

Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

2. Segurança em processos de desenvolvimento e de suporte

OBJETIVO

Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.

Esse objetivo é dividido em quatro controles:

i. Política de desenvolvimento seguro

CONTROLE

Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

Neste objetivo, há um rol de aspectos que devem ser considerados no que tange aos aspectos de segurança dentro da política de segurança de desenvolvimento seguro, e, constantemente, há itens dessa lista que aparecem na prova:

a) segurança do ambiente de desenvolvimento;

b) orientações sobre a segurança no ciclo de vida do desenvolvimento do software:
1) segurança na metodologia de desenvolvimento do software;
2) diretrizes de códigos seguro para cada linguagem de programação usada.

c) requisitos de segurança na fase do projeto;

d) pontos de verificação de segurança no cronograma do projeto;

e) repositórios seguros;

f) segurança no controle de versões;

g) necessários conhecimentos de segurança de aplicações;

h) capacidade dos desenvolvedores de evitar, encontrar e corrigir vulnerabilidades.

ii. Procedimentos para controle de mudanças de sistemas

CONTROLE

Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.

iii. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

CONTROLE

Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para garantir que não haverá qualquer impacto adverso na operação da organização ou na segurança.

iv. Restrições sobre mudanças em pacotes de software

CONTROLE

Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.

v. Princípios para projetar sistemas seguros

CONTROLE

Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

vi. Ambiente seguro para desenvolvimento

CONTROLE

Convém que as organizações estabeleçam e protejam adequadamente ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.

vii. Desenvolvimento terceirizado

CONTROLE

Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.

viii. Teste de segurança do sistema

CONTROLE

Convém que os testes das funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.

ix. Teste de aceitação de sistemas

CONTROLE

Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.

3. Dados para teste

OBJETIVO

Assegurar a proteção dos dados usados para teste.

Esse objetivo possui um único controle:

i. Proteção dos dados para teste

CONTROLE

Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

11) RELACIONAMENTO NA CADEIA DE SUPRIMENTO

ESTRUTURA

a. Segurança da informação na cadeira de suprimento
   i. Política de segurança da informação no relacionamento com os fornecedores
   ii. Identificando segurança da informação nos acordos com fornecedores
   iii. Cadeia de suprimento na tecnologia da informação e comunicação
b. Gerenciamento da entrega do serviço do fornecedor
   i. Monitoramento e análise crítica de serviços com fornecedores
   ii. Gerenciamento de mudanças para serviços com fornecedores

Esta Seção é dividida em dois objetivos:

1. Segurança da informação na cadeia de suprimento

OBJETIVO

Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.

Esse objetivo é dividido em três controles:

i. Política de segurança da informação no relacionamento com os fornecedores

CONTROLE

Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor

ii. Identificando segurança da informação nos acordos com fornecedores

CONTROLE

Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

iii. Cadeia de suprimento na tecnologia da informação e comunicação

CONTROLE

Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados à cadeia de produtos e serviços de tecnologia da informação e comunicação.

2. Gerenciamento da entrega do serviço do fornecedor

OBJETIVO

Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Esse objetivo é dividido em dois controles:

i. Monitoramento e análise crítica de serviços com fornecedores

CONTROLE

Convém que as organizações monitorem, analisem criticamente e auditem, a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

ii. Gerenciamento de mudanças para serviços com fornecedores

CONTROLE

Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação dos riscos.

12) GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

ESTRUTURA

a. Gestão de incidentes de segurança da informação e melhorias
   i. Responsabilidades e procedimentos
   ii. Notificação de eventos de segurança da informação
   iii. Notificando fragilidades de segurança da informação
   iv. Avaliação e decisão dos eventos de segurança da informação
   v. Resposta aos incidentes de segurança da informação
   vi. Aprendendo com os incidentes de segurança da informação
   vii. Coleta de evidências

Esta Seção possui um único objetivo:

1. Gestão de incidentes de segurança da informação e melhorias

OBJETIVO

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo comunicação sobre fragilidades e eventos de segurança da informação.

Esse objetivo é dividido em sete controles:

i. Responsabilidades e procedimentos

CONTROLE

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

ii. Notificação de eventos de segurança da informação

CONTROLE

Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível.

iii. Notificando fragilidades de segurança da informação

CONTROLE

Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

iv. Avaliação e decisão dos eventos de segurança da informação

CONTROLE

Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

v. *Resposta aos incidentes de segurança da informação*

CONTROLE

Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

vi. *Aprendendo com os incidentes de segurança da informação*

CONTROLE

Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

vii. *Coleta de evidências*

CONTROLE

Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

13) ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

ESTRUTURA

a. Continuidade da Segurança da Informação
   i. Planejando a continuidade da segurança da informação
   ii. Implementando a continuidade da segurança da informação
   iii. Verificação, análise crítica e avaliação da continuidade da segurança da informação
b. Redundâncias
   i. Disponibilidade dos recursos de processamento da informação

Esta Seção possui dois objetivos:

1. Continuidade da Segurança da Informação

OBJETIVO

Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização.

Esse objetivo é dividido em três controles:

i. Planejando a continuidade da segurança da informação

CONTROLE

Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

ii. Implementando a continuidade da segurança da informação

CONTROLE

Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

iii. Verificação, análise crítica e avaliação da continuidade da segurança da informação

CONTROLE

Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas.

2. Redundâncias

OBJETIVO

Assegurar a disponibilidade dos recursos de processamento da informação.

Esse objetivo possui um único controle:

i. Disponibilidade dos recursos de processamento da informação

CONTROLE

Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

14) CONFORMIDADE

ESTRUTURA

a. Conformidade com requisitos legais e contratuais
   i. Identificação da legislação aplicável e de requisitos contratuais
   ii. Direitos de propriedade intelectual
   iii. Proteção de registros
   iv. Proteção e privacidade de informações de identificação pessoal
   v. Regulamentação de controles de criptografia
b. Análise crítica da segurança da informação
   i. Análise crítica independente da segurança da informação
   ii. Conformidade com as políticas e procedimentos de segurança da informação
   iii. Análise crítica da conformidade técnica

Esta Seção possui dois objetivos:

1. Conformidade com requisitos legais e contratuais

OBJETIVO

Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

Esse objetivo é dividido em cinco controles:

i. Identificação da legislação aplicável e de requisitos contratuais

CONTROLE

Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

ii. Direitos de propriedade intelectual

CONTROLE

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de softwares proprietários.

iii. Proteção de registros

CONTROLE

Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

iv. Proteção e privacidade de informações de identificação pessoal

CONTROLE

Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

v. Regulamentação de controles de criptografia

CONTROLE

Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

2. Análise crítica da segurança da informação

OBJETIVO

Assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

Esse objetivo é dividido em três controles:

i. Análise crítica independente da segurança da informação

CONTROLE

Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processo e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

ii. Conformidade com as políticas e procedimentos de segurança da informação

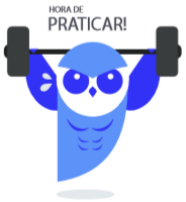
CONTROLE

Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

iii. Análise crítica da conformidade técnica

CONTROLE

Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.



EXERCÍCIOS COMENTADOS

ISO 27001

1. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

As organizações devem estabelecer os objetivos de segurança da informação de forma independente de sua política de segurança da informação.

Comentários:

Pessoal, vimos que todos os princípios, objetos e controles da ISO 27001 deve estar ancorada na Política de Segurança da organização.

Este último trata-se do principal documento relacionado à Segurança da Informação.

Gabarito: E

---

2. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

A organização deve determinar e prover recursos necessários a estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão de segurança da informação (SGSI).

Comentários:

Pessoal, antes de decorarmos a norma, percebamos como faz total sentido a afirmação do enunciado. É a rotina do PDCA (Plan, do, check e act) aplicada à ISO 27001.

Olhando para a norma, encontramos essa afirmação no capítulo 7, quando a norma define aspectos de APOIO. Essa frase foi retirada exatamente de como está escrito na norma.

Gabarito: C

---

3. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

A norma 27001 prevê que as organizações estabeleçam e mantenham critérios de riscos de segurança da informação que incluam os critérios de aceitação do risco.

Comentários:

Extrapolando um pouco a norma, quando falamos de riscos, nos remetemos a 4 aspectos básicos para definição:

1. Aceitação do Risco;
2. Prevenção do Risco;
3. Mitigação do Risco;
4. Transferência do Risco;

A norma, em seu capítulo 6, item 2, traz, na seção de planejamento, que se deve estabelecer aspectos para AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO. Nessa parte, temos que a organização deve então definir os critérios para aceitação e para o desempenho das avaliações dos riscos.

Gabarito: C

---

4. CESPE – TRT – 7ª Região (CE)/ Analista Judiciário - TI/2017

De acordo com a ABNT NBR ISO/IEC 27001, entre os controles da organização interna da segurança da informação inclui-se

a) verificar o histórico de candidatos em processo de seleção antes da contratação.

b) criar processo disciplinar formal para punir funcionários que cometam infração de segurança da informação.

c) descartar qualquer tipo de mídia com informações confidenciais.

d) considerar a segurança da informação em qualquer tipo de projeto.

Comentários:

Típica questão que "mistura" os conceitos dos diversos capítulos presentes na norma. Assim, se você só olha e lembra de ter lido o primeiro aspecto na norma e marca a questão, você acaba errando. Então vamos lá, avaliando cada item e onde encontramos a informação:

A) verificar o histórico de candidatos em processo de seleção antes da contratação. (Segurança de recursos humanos – Antes da Contratação)

b) criar processo disciplinar formal para punir funcionários que cometam infração de segurança da informação. (Segurança de recursos humanos – Durante a Contratação)

c) descartar qualquer tipo de mídia com informações confidenciais. (Gestão de Ativos – Tratamento de Mídias)

d) considerar a segurança da informação em qualquer tipo de projeto. (Organização da Segurança da Informação – Organização Interna)

Gabarito: D

---

5. CESPE – TRT – 7ª Região (CE)/ Analista Judiciário - TI/2017

De acordo com a ABNT NBR ISO/IEC 27001, a alta direção da organização tem papel fundamental no sistema de gestão de segurança da informação (SGSI). Nesse contexto, ela deve estabelecer uma política de segurança da informação que

a) inclua o comprometimento com a melhoria contínua do SGSI.

b) reduza efeitos indesejados.

c) informe responsáveis por cada ativo de informação.

d) crie mecanismos de avaliação de riscos compatíveis com o framework Cobit 5.

Comentários:

A POSIC é um documento estratégico que envolver diretrizes a serem consideradas em todo o contexto da segurança da informação.

Percebam que as letras "B, C e D" tratam de aspectos mais práticos, do âmbito tático e operacional, enquanto a letra "A" possui um caráter mais de diretriz...

Gabarito: A

---

6. CESPE – TRE-BA/Analista Judiciário – Análise de Sistemas/2017

I A gestão dos ativos mantidos no inventário deve ser realizada por ente terceirizado.

II Ativos associados a informação, recursos e processamento da informação devem ser geridos por gestor com mais tempo de organização e mantidos fisicamente separados dos demais.

III Recursos de processamento da informação devem ser identificados, documentados e implementados, assim como as regras para o uso aceitável das informações e dos ativos associados à informação.

IV Os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, de contrato ou acordo.

Assinale a opção correta.

a) Apenas o item II está certo.

b) Apenas o item III está certo.

c) Apenas os itens I e II estão certos.

d) Apenas os itens I e IV estão certos.

e) Apenas os itens III e IV estão certos.

Comentários:

Questão mais tranquila pois não exige saber a seção da norma que trata dos assuntos, mas tão somente se eles estão presentes ou não. Então, mais uma vez, o bom senso fala alto na análise.

Item I – A norma não gera qualquer obrigatoriedade de em relação à gestão de ativos ser realizado por terceirizado. Diz tão somente que deve haver um proprietário com as devidas responsabilidades. ERRADO

Item II – Mais uma vez não há essa obrigatoriedade na norma. ERRADO

Item III – Exatamente o que define a subseção **RESPONSABILIDADE PELOS ATIVOS da seção GESTÃO DE ATIVOS.** Aqui, são definidas as questões de Inventariado, propriedade, uso aceitável e devolução. CERTO

Item IV – Conforme já mencionamos no item anterior. É o último ponto... CERTO

Como a questão é focada na gestão de ativos, vamos relembrar a estrutura:

ESTRUTURA

a. Responsabilidade pelos ativos
    i. Inventário dos ativos
    ii. Proprietário dos ativos
    iii. Uso aceitável dos ativos
    iv. Devolução dos ativos
b. Classificação da Informação
    i. Classificação da Informação
    ii. Rótulos e tratamento da Informação
    iii. Tratamento dos Ativos
c. Tratamento de Mídias
    i. Gerenciamento de mídias removíveis
    ii. Descarte de mídias

Gabarito: E

---

7. CESPE – SEDF/Analista de Gestão Educacional/2017

Todo documento requerido pelo sistema de gestão de segurança da informação (SGSI) precisa ter identificação e controle de versão de alteração, de modo que as diversas versões fiquem disponíveis nos locais de uso, sem que nada seja descartado.

Comentários:

Pessoal, a questão vai bem até o trecho final que afirma “sem que nada seja descartado.”

Imagine uma organização com alguns anos de existência e armazenando essas versões sem quaisquer critérios. Longe de ser razoável, certo?

Gabarito: E

---

8. CESPE – SEDF/Analista de Gestão Educacional/2017

Ao implantar um sistema de gestão de segurança da informação (SGSI), a empresa deve identificar falhas e incidentes de segurança da informação de forma mais rápida e precisa, a fim de agilizar o tempo de resposta e prevenir incidentes futuros.

Comentários:

Novamente, aplicando o bom senso, resolvemos a questão. Sem dúvida identificar as falhas e incidentes possuem dois objetivos básicos:

1. Prevenir que acontecem;
2. Agilizar o tempo de resposta;

Um outro destaque fica para o primeiro objetivo considerado na resposta aos incidentes: "Voltar ao nível de segurança normal", para só então iniciar a recuperação necessária.

Gabarito: C

---

9. CESPE – SEDF/Analista de Gestão Educacional/2017

Um analista de TI foi designado para promover ações que, mediante recursos criptográficos, visam à proteção da confidencialidade, da autenticidade e da integridade das informações de determinada organização.

No que se refere a essa situação hipotética, julgue o item seguinte.

De acordo com a ISO/IEC 27001, um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.

Comentários:

Para quem já estudou a matéria de criptografia, principalmente aspectos de certificação digital e a infraestrutura PKI, entende ainda mais a importância de se ter uma gestão de chaves de criptografia adequado.

Nesse sentido, a norma traz uma subseção específica que trata da gestão ou gerenciamento das chaves.

Gabarito: C

10.CESPE – TCE-PA/Auditor/2017

No que se refere a sistemas de gestão da segurança da informação (SGSI), julgue o item a seguir à luz da norma ISO/IEC 27001:2013.

Para reivindicar conformidade com a referida norma, uma organização poderá excluir, sem justificativas formais, requisitos especificados nas seções de análise crítica pela direção e de auditorias internas do SGSI.

Comentários:

Pessoal, estamos falando de uma norma que possui uma série de aspectos formais, inclusive no que tange à certificação de instituições em relação ao Sistema de Gestão de Segurança da Informação.

Então dizer, tão somente, para fins de conformidade, que poderá ser excluído requisitos especificados por causa da alta direção e auditorias internas é longe de ser razoável, muito menos ser justificativas formais.

Gabarito: E

11.CESPE – TCE-PA/Auditor/2017

Devido a seu conteúdo confidencial e estratégico, a política de segurança da informação de uma organização deve estar disponível, como informação documentada, exclusivamente para a alta gerência.

Comentários:

Já comentamos sobre o assunto. A política de segurança deve ser divulgada para todos da organização, inclusive para os stakeholders.

Gabarito: E

ISO 27002

12.CESPE – STJ/Técnico Judiciário – Suporte Técnico/2018

Os controles da segurança da informação elencados na NBR ISO/IEC 27002 englobam as ações realizadas na gestão de projetos específicos da área de segurança da informação, as quais, porém, não lidam com controles que visem proteger a informação processada em sítios de teletrabalho.

Comentários:

Pessoal, os controles definidos na ISO 27002 abarcam o Sistema de Gestão de Segurança da Informação, contemplando, inclusive, a informação processada em teletrabalho.

A questão está tratando especificamente do acesso remoto. Plenamente razoável definir regras e controles de acesso seguro por meio de empregados que acessem a rede interna a partir de uma rede externa, certo?

Tais definições são mapeadas na SEÇÃO ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO, subseção DISPOSITIVOS MÓVEIS E TRABALHO REMOTO.

Aqui encontramos o controle de trabalho remoto:

"Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto."

Gabarito: E

13.CESPE – STJ/Técnico Judiciário – Suporte Técnico/2018

A norma ISO 27002 estabelece que o objetivo da classificação das informações (atribuição de grau de confidencialidade) é a garantia de que os ativos de informação receberão um nível de proteção adequado. Ainda segundo a norma, as informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de proteção.

Com base nesse objetivo, a norma estabelece diretrizes para essa classificação, entre as quais se inclui a de

a) atribuir o processo de revisão do nível de confidencialidade de um documento à alta gerência.

b) manter a responsabilidade pela atribuição do nível de confidencialidade de um documento com o setor de TI.

c) manter os rótulos de classificação originais nos documentos oriundos de outras organizações.

d) manter o princípio de equidade que garante aos funcionários com funções similares o mesmo direito de acesso às informações classificadas.

e) rotular as informações e as saídas geradas pelos sistemas que tratam dados confidenciais, segundo seu valor e sensibilidade para a organização.

Comentários:

Excelente questão do CESPE tratando do conceito de classificação da informação.

a) A norma não traz aspectos detalhados no processo de revisão e não atribui à alta gerência. Lembrando que a responsabilidade pela classificação se dá pela área de negócio ou o seu representante. ERRADO.
b) Conforme mencionamos no item anterior e na nossa teoria. Não é responsabilidade do setor de TI. ERRADO
c) A norma traz a referência de que deve haver uma análise para fins de avaliação e equiparação da classificação utilizada pelas organizações, não restringindo, portanto, aos aspectos de manutenção da classificação original. ERRADO
d) Lembrando que a informação tem um caráter de negócio. Então não basta olhar apenas para a função, mas para a atribuição e alocação do profissional. ERRADO
e) A norma traz que a classificação não deve se restringir à informação, mas deve alcançar os ativos e processos que geram informação, categorizando-se nos mesmos padrões definidos de uma maneira geral na organização. CERTO

Gabarito: E

14.CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

As bibliotecas das fontes dos programas de uma organização devem ser mantidas no mesmo ambiente computacional do sistema operacional, com o objetivo de facilitar atividades de auditoria.

Comentários:

Na seção de CONTROLE DE ACESSO da norma, encontramos uma série de controles extremamente operacionais que são considerados e, recorrentemente caem em prova.

Temos aqui, o objetivo CONTROLE DE ACESSO AO SISTEMA E À APLICAÇÃO.

Não é difícil imaginas alguns controles básicos que necessitamos ter referentes aos sistemas, certo? Ter rotinas para restringir o acesso; Ter rotinas para definir procedimentos seguros de acesso (log-on); Criar um sistema de gerenciamento de senhas (como os conhecidos cofres de senhas para geração randômica); Tratar o Uso de programas utilitários privilegiados; e finalmente, tratar do controle de acesso ao código-fonte de programas.

Neste último ponto, especificamente, temos que norma nos traz em seu objetivo a simples restrição de acesso ao código fonte.

A norma zela por um repositório centralizado para armazenamento de códigos fontes, algo semelhante ao que a norma diz a respeito de gerenciamento de LOG's.

Além dessa, há uma série de orientações a respeito da mitigação de riscos em relação às bibliotecas, dentre os quais há a recomendação de se evitar manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais.

Gabarito: E

15.CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

As informações já armazenadas no histórico de acesso não devem ser mais editadas, servindo para coleta e retenção de evidências para auditoria.

Comentários:

Como já adiantamos a conversa sobre o gerenciamento de Log's, aproveitamos para analisar mais uma questão sobre o assunto. Lembramos que quando falamos de LOG's, naturalmente nos remete a conceitos de operação... Então lembre-se aqui da seção SEGURANÇA NAS OPERAÇÕES, especificamente falando da seção de REGISTRO E MONITORAMENTO. Aqui, temos algumas recomendações na norma que nos dizem aspectos que devemos impedir em relação aos logs, quais sejam:

Convém que os controles implementados **objetivem a proteção contra modificações não autorizadas** às informações dos (logs) e problemas operacionais com os recursos dos registros (log), tais como:

a) alterações dos tipos de mensagens que são gravadas;

b) arquivos de registros (log) sendo editados ou excluídos;

Agora de uma maneira mais prática, é razoável pensarmos que os logs não devem ser alterados justamente para não adulterarem eventuais evidências para fins de auditoria, certo pessoal?

Gabarito: C

16.CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

Uma das premissas do controle de acesso na segurança da informação é a implementação da regra de que tudo é proibido, a menos que seja expressamente permitido.

Comentários:

Mais uma vez pessoal, com o nosso conhecimento em segurança, seria possível responder essa questão sem conhecer a norma.

Esse conceito é o do privilégio mínimo. Ou seja, você só terá acesso àquilo que for realmente necessário.

Bom, olhando para a norma, temos que tal assunto, obviamente, se encontra na seção de POLÍTICAS DE CONTROLE DE ACESSO. Para nos situarmos melhor, especificamente falamos dos REQUISITOS DO NEGÓCIO PARA CONTROLE DE ACESSO. Percebam mais uma vez a lógica, trata-se de uma política, uma regra de segurança, ou seja, é razoável assumirmos no âmbito de requisitos de negócio.

Bom, voltando para a norma, temos que ela nos traz exatamente o seguinte trecho:

"Estabelecer regra baseada na premissa de que "Tudo é proibido a menos que expressamente permitido" em lugar da regra mais fraca que "Tudo é permitido, a menos que expressamente proibido";

Gabarito: C

17.CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

Quando uma mídia removível não for mais necessária e vier a ser retirada da organização, recomenda-se que o conteúdo magnético seja deletado.

Comentários:

Questão bem maldosa e sutil do CESPE. Realmente a lógica aqui acaba levando o candidato ao erro por não saber os detalhes.

A norma zela pela política de descarte como medida de segurança. Desse modo, ela distingue em termos da necessidade da mídia.

a) **quando não for mais necessário**, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;

b) **quando necessário** e prático, seja requerida a autorização para remoção de qualquer mídia da organização e mantido o registro dessa remoção como trilha de auditoria;

Então fiquemos atentos com esse detalhe referente às mídias de uma organização.

Gabarito: E

18.CESPE – TRT - TO – Técnico Judiciário – Programação de Sistemas/2018

Segundo a norma ABNT NBR ISO/IEC 27002:2013, a segurança da informação deve ser apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização. A partir dessas informações, assinale a opção que apresenta um exemplo de política com tópico específico considerado pela referida norma.

a) desenvolvimento de software

b) segurança institucional

c) ética concorrencial

d) gestão de riscos

e) controles criptográficos

Comentários:

Pessoal, já comentamos na aula de hoje sobre a existência dos controles criptográficos como parte do SGSI, certo?

Lembrando que os CONTROLES CRIPTOGRÁFICOS se encontram na seção de CRIPTOGRAFIA.

Entretanto, o que merece destaque nessa questão é a descrição do capítulo de Políticas de Segurança da Informação que traz um rol de exemplos de políticas a serem criadas em uma organização e ancoradas na POSIC, a saber:

a) controle de acesso;

b) classificação e tratamento da informação;

c) segurança física e do ambiente;

d) tópicos orientados aos usuários finais:

- **1) uso aceitável dos ativos;**
- **2) mesa Limpa e Tela Limpa;**
- **3) transferência de informações;**
- **4) dispositivos móveis e trabalho remoto;**
- **5) restrições sobre o uso e instalação de software;**

e) backup;

f) transferência da informação;

g) proteção contra *códigos maliciosos;*

h) gerenciamento de vulnerabilidades técnicas;

i) Controles criptográficos;

j) segurança nas comunicações;

k) proteção e privacidade da informação de identificação pessoal;

l) relacionamento na cadeia de suprimento.

Gabarito: E

19.CESPE – TRE - BA – Analista Judiciário/2017

De acordo com a ABNT NBR ISO/IEC 27002 — norma de referência para a escolha de controles no processo de implementação de sistemas de gestão da segurança da informação —, o primeiro objetivo de resposta a incidente de segurança da informação é

a) qualificar técnicos locais para o trabalho de identificar, coletar e preservar as informações.

b) realizar o devido processo administrativo disciplinar para a apuração do fato.

c) listar as lições aprendidas para a divulgação entre os integrantes da organização.

d) voltar ao nível de segurança normal e, então, iniciar a recuperação.

e) suspender as atividades até que os fatos relacionados ao incidente sejam apurados.

Comentários:

Chegamos ao ponto de começar a repetir algumas questões da banca, certo? Já vimos que o primeiro passo é zelar pela segurança e, portanto, voltar ao nível de segurança normal para, só então, iniciar a recuperação.

É uma tendência natural de questões desse tipo quando se começa a realizar muitos exercícios.

Gabarito: D

20.CESPE – SEDF – Analista de Gestão Educacional - TI/2017

De acordo com a NBR ISO 27002, a política de controle de acesso deve tratar do controle de acesso lógico, enquanto a política de segurança física e do ambiente deve tratar do controle de acesso físico.

Comentários:

O índice de erro dessa questão foi altíssimo. A organização da frase realmente leva o candidato a uma interpretação equivocada.

Segundo a ISO, no tópico de POLÍTICA DE ACESSO, conforme vimos em nossa teoria, devem ser considerados na política a segurança física e lógica de maneira conjunta.

Gabarito: E

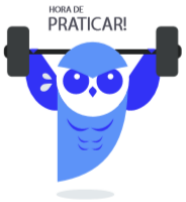
21.CESPE – TCE-SC/Auditor Fiscal de Controle Externo/2017

Ao elaborar, manter, melhorar e implantar um sistema de gestão de segurança da informação, a organização deve considerar as características técnicas de seu negócio, e o SGSI (sistema de gestão de segurança da informação) deve ser documentado dentro do contexto de suas atividades operacionais, sem, contudo, envolver a direção da organização.

Comentários:

Pessoal, questão bem tranquila, certo? Não envolver a direção da organização é um pouco demais. Os demais aspectos estão corretos em seus apontamentos.

Gabarito: E



EXERCÍCIOS COMENTADOS COMPLEMENTARES

ISO 27001 E 27002

1. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

O Técnico de Suporte foi designado para estabelecer, junto aos usuários da Defensoria, um código de prática para o controle de segurança da informação no gerenciamento de mídias removíveis, de acordo com a Norma NBR ISO/IEC 27002:2013. Uma das diretrizes mencionadas na Norma estabelece que

a) sejam usadas técnicas de criptografia, no caso em que a autenticidade ou disponibilidade dos dados sejam considerações importantes.

b) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído sempre.

c) as unidades de mídias removíveis sejam habilitadas somente se houver uma necessidade do negócio.

d) cópias múltiplas de dados valiosos sejam armazenadas na mesma mídia para reduzir riscos futuros de perda ou dano.

e) quando necessário e prático, seja requerida a autorização verbal para remoção de qualquer mídia da organização.

Comentário:

Típica questão da FCC que não busca vincular os controles aos objetivos, mas tão somente avaliar os controles. Desse modo, o jogo de palavras e substituição de uma pela outra é o recurso mais utilizado.

Muita atenção para as marcações por impulso... Uma ausência de palavra pode invalidar a questão. Vamos lá:

a) sejam usadas técnicas de criptografia, no caso em que a autenticidade ou ~~disponibilidade~~ dos dados sejam considerações importantes. ERRADO

b) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja ~~destruído sempre~~ destruído, caso venha a ser retirado da organização. ERRADO

c) as unidades de mídias removíveis sejam habilitadas somente se houver uma necessidade do negócio. CORRETO

d) cópias múltiplas de dados valiosos sejam armazenadas ~~na mesma mídia~~ em mídia separadas para reduzir riscos futuros de perda ou dano.

e) quando necessário e prático, seja requerida a autorização ~~verbal~~ para remoção de qualquer mídia da organização. ERRADO

Gabarito: C

---

2. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

O Técnico de Suporte encontrou o seguinte controle de segurança da informação na Norma NBR ISO/IEC 27002:2013: estabelecer uma política formal proibindo o uso de software não autorizados. Trata-se de um controle de

a) cópias de segurança.
b) software operacional.
c) direitos de propriedade intelectual.
d) proteção contra malware.
e) acordos de confidencialidade.

Comentário:

Pessoal, cuidado com o impulso...

Muito tranquilo em relação aos itens "a", "c" e "e", certo? Não guardam relação com o pedido.

Em relação ao item "b", nos leva a querer acreditar que é aspecto de software operacional. Entretanto, não há esse controle na norma, mas tão somente a proteção contra malware ou também referenciada como PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS. Lembrando que este se encontra na seção de SEGURANÇA NAS OPERAÇÕES.

Gabarito: D

---

3. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

A Norma ABNT NBR ISO/IEC 27002:2013 recomenda que um conjunto de políticas de segurança da informação seja definido. Segundo a Norma,

a) é necessário que estas políticas sejam aprovadas por todos os funcionários.

b) estas políticas só devem ser divulgadas e comunicadas aos funcionários internos da organização.
c) é recomendável contemplar requisitos oriundos de ações operacionais, independente da estratégia do negócio.
d) só devem ser contemplados requisitos oriundos do ambiente de ameaça da segurança da informação atual.
e) é recomendável que estas políticas contenham requisitos oriundos de regulamentações, legislação e contratos.

Comentário:

Vamos comentar os itens:

a) A POSIC deve ser aprovada pela ALTA DIREÇÃO e não por todos os funcionários. ERRADA
b) A Norma também considera os stakeholders, além dos funcionários. ERRADA
c) Todo o SGSI deve estar alinhado com a estratégia de negócio. ERRADA
d) Deve-se considerar também o futuro. ERRADA
e) CORRETO

Gabarito: E

---

4. FCC – TRT-24ª Região (MS)/Técnico Judiciário/2017

A norma ABNT NBR ISO/IEC 27001:2013 apresenta como anexo uma tabela com controles e objetivos de controle alinhados com os existentes na norma ABNT NBR ISO/IEC 27002:2013. Uma colaboradora de nível técnico, utilizando os controles relacionados à segurança em processos de desenvolvimento e de suporte dessa tabela deve saber que
a) modificações em pacotes de software devem ser encorajadas e não devem estar limitadas apenas às mudanças necessárias, porém, todas as mudanças devem ser documentadas.
b) mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas por procedimentos informais de controle de mudanças.
c) a organização não deve contratar empresas terceirizadas para realizar atividades de desenvolvimento de sistemas de informação.
d) testes de funcionalidade de segurança devem ser realizados somente quando o sistema estiver pronto.
e) programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões.

Comentário:

Vamos aos itens pessoal:

a) Pessoal, mudanças são sempre um risco para qualquer ambiente ou solução. Desse modo, dizer que elas devem ser encorajadas é um erro. Os outros aspectos estão corretos. ERRADO
b) Mais uma vez, não há o que se falar MUDANÇA e INFORMAL na mesma frase. ERRADO
c) Pessoal, não há qualquer restrição para contratação de terceirizadas para tal finalidade. Obviamente, deve-se tratar todos os aspectos da ISO 27002 no que tange à segurança da informação para stakeholders externos. Vale mencionar, inclusive, a seção **DESENVOLVIMENTO TERCEIRIZADO** que consta na parte de **SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE**. ERRADO
d) Não né pessoal? Aqui podemos invocar inclusive outras metodologias de desenvolvimento seguro como o SDL, por exemplo, que garante um acompanhamento e testes de segurança durante toda a fase de desenvolvimento. ERRADO
e) Exatamente o controle previsto no objetivo **TESTE DE ACEITAÇÃO DE SISTEMAS**. CORRETO

Gabarito: E

---

5. FCC – TRT-24ª Região (MS)/Técnico Judiciário/2017

Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema que respeitem normas de segurança. Dentro de uma política de desenvolvimento seguro, a norma ABNT NBR ISO/IEC 27002:2013 recomenda

a) que não é necessário considerar segurança na metodologia desenvolvimento do software, pois a segurança será considerada na fase de programação do software.
b) que não sejam considerados requisitos de segurança na fase do projeto, mas sim na fase de implementação do software.
c) levar em consideração a segurança no controle de versões.
d) levar em consideração mais a habilidade técnica dos desenvolvedores, do que a capacidade de evitar, encontrar e corrigir vulnerabilidades.
e) que o desenvolvimento de software nunca seja terceirizado.

Comentário:

Vamos aos itens:

a) Pessoal, não precisamos falar muito aqui, certo? Óbvio que é necessário considerar a segurança da informação. ERRADO

b) Basta olharmos para a letra A. ERRADO
c) Na Política de Desenvolvimento Seguro, há um rol de aspectos que devem ser considerados, entre eles, a segurança no controle de versões. CORRETO
d) Mais uma vez o item se apega ao item da política de desenvolvimento seguro. Lá temos expresso a CAPACIDADE DOS DESENVOLVEDORES DE EVITAR, ENCONTRAR E CORRIGIR VULNERABILIDADES. ERRADO
e) Para verificarmos a tendência da banca. Já mencionarmos esse item recentemente. ERRADO

Gabarito: C

---

6. FCC – TRT-11ª Região (AM e RR)/Analista Judiciário/2017

Um Analista Judiciário deve estabelecer um código de prática de segurança da informação no TRT para o controle e a prevenção de ataques de malwares. Considerando-se a Norma NBR ISO/IEC 27002:2013, é recomendável que o código de segurança inclua

a) a implementação de controles para prevenir o uso de software não autorizado, como o whitelisting que lista os softwares não permitidos.

b) a aplicação do princípio do privilégio máximo para os usuários pertinentes para a instalação de softwares.

c) o uso de dois ou mais tipos de software de controle contra malware de diferentes fornecedores para aumentar a eficácia na proteção.

d) o procedimento para a divulgação imediata de alertas relacionados a malwares provenientes de todos os meios de comunicação, incluindo os alertas preliminares como boatos.

e) a eliminação de qualquer atualização não autorizada de software crítico de forma imediata não sendo necessária uma investigação formal.

Comentário:

Questão que explora o item 12.2 da norma (PROTEÇÃO CONTRA CÓDIGOS MALICIOSO). Vamos aos itens

a) Pessoal, a WHITELIST apresenta aqueles permitidos. A questão inverteu os conceitos. ERRADO
b) Errado pessoal. Temos a aplicação do privilégio mínimo. Questão bem intuitiva. ERRADO
c) A norma traz uma diretriz específica em relação a esse item. O que cabe observar aqui é a intenção. Quando se tem dois fabricantes envolvidos, tem-se uma capacidade maior de detecção tendo em vista que serão duas bases diferentes para considerar na análise. CORRETO

d) A norma aponta para haver o devido cuidado na diferenciação do que é boato e o que é código malicioso, de fato. Assim, deve-se considerar, apenas, aquilo que seja real. ERRADO
e) Mais uma vez, não se deve deixar de considerar o processo formal para apuração dos aspectos relacionados à Segurança da Informação. ERRADO

Gabarito: C

---

7. FCC – TRE-SP/Analista Judiciário/2017

Um Analista de Sistemas do TRE-SP deve, hipoteticamente, estabelecer e especificar os controles de segurança de acordo com a Norma ABNT NBR ISO/IEC 27002:2013. Um dos controles apresenta, dentre outras, as seguintes diretrizes:
I. Mostrar um aviso geral informando que o computador seja acessado somente por usuários autorizados.
II. Não transmitir senhas em texto claro pela rede.
III. Restringir os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e para reduzir a janela de oportunidade para acesso não autorizado.
Trata-se do controle:
a) Responsabilidades dos usuários.
b) Acesso ao sistema e à aplicação.
c) Gerenciamento de acesso do usuário.
d) Acesso ao código-fonte de programas.
e) Entrada física de pessoas.

Comentário:

Pessoal, muita gente errou essa questão ao marcar a opção "A" por causa do item I, referenciando-se à seção de responsabilidades e papéis de segurança da informação.

Entretanto, tais itens são referentes ao CONTROLE DE ACESSO AO SISTEMA E À APLICAÇÃO, que tem como objetivo a prevenção de acessão não autorizado aos sistemas e aplicações. Sendo ainda mais específico, estamos falando da seção 9.4.2, do que trata dos PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA (LOG-ON).

Gabarito: B

---

8. FCC – TRE-SP/Analista Judiciário/2017

Supondo-se que o TRE-SP tenha concursado profissionais que irão realizar atividades em local de trabalho remoto. A fim de garantir a segurança da informação, esse Tribunal se pautou em recomendações previstas na Norma ABNT NBR ISO/IEC 27002:2013 cujo objeto, em suas diretrizes para implementação, reza que deve haver política, medidas e controles que apoiem a segurança da informação e que a organização deve estabelecer condições e restrições para uso em trabalho remoto. Assim, quando entendidos como aplicáveis e permitidos por lei, convém considerar:

I. Acordos de licenciamento de software que podem tornar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros.

II. Ambiente físico proposto para o trabalho remoto que inclui ambientes de trabalho não tradicionais, como aqueles referidos como: "ambientes de telecommuting", "local de trabalho flexível" e "trabalho remoto", excetuando-se, em todas as suas formas, o chamado "trabalho virtual".

III. Segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local.
Está de acordo com as recomendações previstas na norma o que consta APENAS em
a) I e III.
b) I e II.
c) II.
d) II e III.
e) III.

Comentário:

Encontramos nossa resposta na seção de TRABALHO REMOTO. Percebam que para o item "B", houve uma distorção ao excluir o trabalho virtual, que é justamente o conceito de acesso remoto.

Convém que a organização que permita a atividade de trabalho remoto publique uma política que defina as condições e restrições para o uso do trabalho remoto. Quando considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

a) a segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;

b) o ambiente físico proposto para o trabalho remoto;

i) acordos de licenciamento de software que podem tornar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros;

Gabarito: A

---

9. FCC – PGE-MT/Analista de Sistemas/2016

A norma ABNT NBR ISO/IEC 27002:2013 traz uma seção que trata da organização da segurança da informação nas organizações. Dentre os controles apresentados nessa seção está o que recomenda que

a) a segurança da informação seja analisada criticamente em intervalos planejados ou quando mudanças significativas ocorrem.

b) a segurança da informação seja considerada no gerenciamento de projetos, independente do tipo do projeto.

c) existam procedimentos definidos para o gerenciamento de mídias removíveis, de acordo com o sistema de classificação da informação.

d) um processo formal de registro e cancelamento de usuário seja definido para permitir atribuição dos direitos de acesso a esses usuários.

e) exista um processo disciplinar formal implantado e comunicado, para tomar ações contra funcionários que tenham cometido violações de segurança da informação.

Comentário:

Muita atenção pessoal quando a banca restringe a seção... No impulso podem cometer erros bobos. Então vamos aos itens:

a) Este item trata da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO. ERRADO
b) Exatamente como encontramos na seção de ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO. CORRETO
c) Está tratando de aspectos de mídias removíveis. A Seção correta é de TRATAMENTO DE MÍDIA. ERRADO
d) Estamos falando da seção de GERENCIAMENTO DE ACESSO DE USUÁRIO. ERRADO
e) Estamos tratando de aspectos de recursos humanos, durante a prestação de serviços. Logo, estamos na seção DURANTE A CONTRATAÇÃO. ERRADO

Gabarito: B

Chegamos ao término de mais uma aula!

Caso tenha ficado alguma dúvida, me procure no fórum que buscaremos respondê-lo o mais breve possível.

E se você está curtindo o nosso curso, não deixe de me seguir no Instagram.

@profandrecastro

Instagram YouTube

andrecastroprofessor@gmail.com
/professorandrecastro

LISTA DE EXERCÍCIOS

ISO 27001

1. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

As organizações devem estabelecer os objetivos de segurança da informação de forma independente de sua política de segurança da informação.

---

2. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

A organização deve determinar e prover recursos necessários a estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão de segurança da informação (SGSI).

---

3. CESPE – CGM/PB – Auditor Municipal de Controle Interno – Desenvolvimento de Sistemas/2018

A norma 27001 prevê que as organizações estabeleçam e mantenham critérios de riscos de segurança da informação que incluam os critérios de aceitação do risco.

---

4. CESPE – TRT – 7ª Região (CE)/ Analista Judiciário - TI/2017

De acordo com a ABNT NBR ISO/IEC 27001, entre os controles da organização interna da segurança da informação inclui-se

a) verificar o histórico de candidatos em processo de seleção antes da contratação.

b) criar processo disciplinar formal para punir funcionários que cometam infração de segurança da informação.

c) descartar qualquer tipo de mídia com informações confidenciais.

d) considerar a segurança da informação em qualquer tipo de projeto.

5. CESPE – TRT – 7ª Região (CE)/ Analista Judiciário - TI/2017

De acordo com a ABNT NBR ISO/IEC 27001, a alta direção da organização tem papel fundamental no sistema de gestão de segurança da informação (SGSI). Nesse contexto, ela deve estabelecer uma política de segurança da informação que

a) inclua o comprometimento com a melhoria contínua do SGSI.

b) reduza efeitos indesejados.

c) informe responsáveis por cada ativo de informação.

d) crie mecanismos de avaliação de riscos compatíveis com o framework Cobit 5.

6. CESPE – TRE-BA/Analista Judiciário – Análise de Sistemas/2017

I A gestão dos ativos mantidos no inventário deve ser realizada por ente terceirizado.

II Ativos associados a informação, recursos e processamento da informação devem ser geridos por gestor com mais tempo de organização e mantidos fisicamente separados dos demais.

III Recursos de processamento da informação devem ser identificados, documentados e implementados, assim como as regras para o uso aceitável das informações e dos ativos associados à informação.

IV Os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, de contrato ou acordo.

Assinale a opção correta.

a) Apenas o item II está certo.

b) Apenas o item III está certo.

c) Apenas os itens I e II estão certos.

d) Apenas os itens I e IV estão certos.

e) Apenas os itens III e IV estão certos.

7. CESPE – SEDF/Analista de Gestão Educacional/2017

Todo documento requerido pelo sistema de gestão de segurança da informação (SGSI) precisa ter identificação e controle de versão de alteração, de modo que as diversas versões fiquem disponíveis nos locais de uso, sem que nada seja descartado.

8. CESPE – SEDF/Analista de Gestão Educacional/2017

Ao implantar um sistema de gestão de segurança da informação (SGSI), a empresa deve identificar falhas e incidentes de segurança da informação de forma mais rápida e precisa, a fim de agilizar o tempo de resposta e prevenir incidentes futuros.

9. CESPE – SEDF/Analista de Gestão Educacional/2017

Um analista de TI foi designado para promover ações que, mediante recursos criptográficos, visam à proteção da confidencialidade, da autenticidade e da integridade das informações de determinada organização.

No que se refere a essa situação hipotética, julgue o item seguinte.

De acordo com a ISO/IEC 27001, um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.

10. CESPE – TCE-PA/Auditor/2017

No que se refere a sistemas de gestão da segurança da informação (SGSI), julgue o item a seguir à luz da norma ISO/IEC 27001:2013.

Para reivindicar conformidade com a referida norma, uma organização poderá excluir, sem justificativas formais, requisitos especificados nas seções de análise crítica pela direção e de auditorias internas do SGSI.

11. CESPE – TCE-PA/Auditor/2017

Devido a seu conteúdo confidencial e estratégico, a política de segurança da informação de uma organização deve estar disponível, como informação documentada, exclusivamente para a alta gerência.

ISO 27002

12. CESPE – STJ/Técnico Judiciário – Suporte Técnico/2018

Os controles da segurança da informação elencados na NBR ISO/IEC 27002 englobam as ações realizadas na gestão de projetos específicos da área de segurança da informação, as quais, porém, não lidam com controles que visem proteger a informação processada em sítios de teletrabalho.

Comentários:

Já comentamos sobre o assunto. A política de segurança deve ser divulgada para todos da organização, inclusive para os stakeholders.

Gabarito: E

---

13. CESPE – STJ/Técnico Judiciário – Suporte Técnico/2018

A norma ISO 27002 estabelece que o objetivo da classificação das informações (atribuição de grau de confidencialidade) é a garantia de que os ativos de informação receberão um nível de proteção adequado. Ainda segundo a norma, as informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de proteção.

Com base nesse objetivo, a norma estabelece diretrizes para essa classificação, entre as quais se inclui a de

a) atribuir o processo de revisão do nível de confidencialidade de um documento à alta gerência.

b) manter a responsabilidade pela atribuição do nível de confidencialidade de um documento com o setor de TI.

c) manter os rótulos de classificação originais nos documentos oriundos de outras organizações.

d) manter o princípio de equidade que garante aos funcionários com funções similares o mesmo direito de acesso às informações classificadas.

e) rotular as informações e as saídas geradas pelos sistemas que tratam dados confidenciais, segundo seu valor e sensibilidade para a organização.

---

14. CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

As bibliotecas das fontes dos programas de uma organização devem ser mantidas no mesmo ambiente computacional do sistema operacional, com o objetivo de facilitar atividades de auditoria.

---

15. CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

As informações já armazenadas no histórico de acesso não devem ser mais editadas, servindo para coleta e retenção de evidências para auditoria.

---

16. CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

Uma das premissas do controle de acesso na segurança da informação é a implementação da regra de que tudo é proibido, a menos que seja expressamente permitido.

---

17. CESPE – ABIN – Oficial Técnico de Inteligência – Área 8/2018

Quando uma mídia removível não for mais necessária e vier a ser retirada da organização, recomenda-se que o conteúdo magnético seja deletado.

---

18. CESPE – TRT - TO – Técnico Judiciário – Programação de Sistemas/2018

Segundo a norma ABNT NBR ISO/IEC 27002:2013, a segurança da informação deve ser apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização. A partir dessas informações, assinale a opção que apresenta um exemplo de política com tópico específico considerado pela referida norma.

a) desenvolvimento de software

b) segurança institucional

c) ética concorrencial

d) gestão de riscos

e) controles criptográficos

---

19. CESPE – TRE - BA – Analista Judiciário/2017

De acordo com a ABNT NBR ISO/IEC 27002 — norma de referência para a escolha de controles no processo de implementação de sistemas de gestão da segurança da informação —, o primeiro objetivo de resposta a incidente de segurança da informação é

a) qualificar técnicos locais para o trabalho de identificar, coletar e preservar as informações.

b) realizar o devido processo administrativo disciplinar para a apuração do fato.

c) listar as lições aprendidas para a divulgação entre os integrantes da organização.

d) voltar ao nível de segurança normal e, então, iniciar a recuperação.

e) suspender as atividades até que os fatos relacionados ao incidente sejam apurados.

---

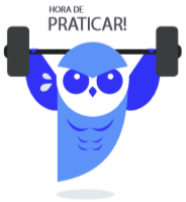
20. CESPE – SEDF – Analista de Gestão Educacional - TI/2017

De acordo com a NBR ISO 27002, a política de controle de acesso deve tratar do controle de acesso lógico, enquanto a política de segurança física e do ambiente deve tratar do controle de acesso físico.

---

21. CESPE – TCE-SC/Auditor Fiscal de Controle Externo/2017

Ao elaborar, manter, melhorar e implantar um sistema de gestão de segurança da informação, a organização deve considerar as características técnicas de seu negócio, e o SGSI (sistema de gestão de segurança da informação) deve ser documentado dentro do contexto de suas atividades operacionais, sem, contudo, envolver a direção da organização.



LISTA DE EXERCÍCIOS COMPLEMENTARES

ISO 27002

1. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

O Técnico de Suporte foi designado para estabelecer, junto aos usuários da Defensoria, um código de prática para o controle de segurança da informação no gerenciamento de mídias removíveis, de acordo com a Norma NBR ISO/IEC 27002:2013. Uma das diretrizes mencionadas na Norma estabelece que

a) sejam usadas técnicas de criptografia, no caso em que a autenticidade ou disponibilidade dos dados sejam considerações importantes.

b) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído sempre.

c) as unidades de mídias removíveis sejam habilitadas somente se houver uma necessidade do negócio.

d) cópias múltiplas de dados valiosos sejam armazenadas na mesma mídia para reduzir riscos futuros de perda ou dano.

e) quando necessário e prático, seja requerida a autorização verbal para remoção de qualquer mídia da organização.

---

2. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

O Técnico de Suporte encontrou o seguinte controle de segurança da informação na Norma NBR ISO/IEC 27002:2013: estabelecer uma política formal proibindo o uso de software não autorizados. Trata-se de um controle de

a) cópias de segurança.

b) software operacional.

c) direitos de propriedade intelectual.

d) proteção contra malware.

e) acordos de confidencialidade.

---

3. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

A Norma ABNT NBR ISO/IEC 27002:2013 recomenda que um conjunto de políticas de segurança da informação seja definido. Segundo a Norma,

a) é necessário que estas políticas sejam aprovadas por todos os funcionários.

b) estas políticas só devem ser divulgadas e comunicadas aos funcionários internos da organização.

c) é recomendável contemplar requisitos oriundos de ações operacionais, independente da estratégia do negócio.

d) só devem ser contemplados requisitos oriundos do ambiente de ameaça da segurança da informação atual.

e) é recomendável que estas políticas contenham requisitos oriundos de regulamentações, legislação e contratos.

---

4. FCC – DPE-AM/Assistente Técnico de Defensoria/2018

A norma ABNT NBR ISO/IEC 27001:2013 apresenta como anexo uma tabela com controles e objetivos de controle alinhados com os existentes na norma ABNT NBR ISO/IEC 27002:2013. Uma colaboradora de nível técnico, utilizando os controles relacionados à segurança em processos de desenvolvimento e de suporte dessa tabela deve saber que

a) modificações em pacotes de software devem ser encorajadas e não devem estar limitadas apenas às mudanças necessárias, porém, todas as mudanças devem ser documentadas.

b) mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas por procedimentos informais de controle de mudanças.

c) a organização não deve contratar empresas terceirizadas para realizar atividades de desenvolvimento de sistemas de informação.

d) testes de funcionalidade de segurança devem ser realizados somente quando o sistema estiver pronto.

e) programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões.

---

5. FCC – TRT-24ª Região (MS)/Técnico Judiciário/2017

Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema que respeitem normas de segurança. Dentro de uma política de desenvolvimento seguro, a norma ABNT NBR ISO/IEC 27002:2013 recomenda

a) que não é necessário considerar segurança na metodologia desenvolvimento do software, pois a segurança será considerada na fase de programação do software.

b) que não sejam considerados requisitos de segurança na fase do projeto, mas sim na fase de implementação do software.

c) levar em consideração a segurança no controle de versões.

d) levar em consideração mais a habilidade técnica dos desenvolvedores, do que a capacidade de evitar, encontrar e corrigir vulnerabilidades.

e) que o desenvolvimento de software nunca seja terceirizado.

---

6. FCC – TRT-11ª Região (AM e RR)/Analista Judiciário/2017

Um Analista Judiciário deve estabelecer um código de prática de segurança da informação no TRT para o controle e a prevenção de ataques de malwares. Considerando-se a Norma NBR ISO/IEC 27002:2013, é recomendável que o código de segurança inclua

a) a implementação de controles para prevenir o uso de software não autorizado, como o whitelisting que lista os softwares não permitidos.

b) a aplicação do princípio do privilégio máximo para os usuários pertinentes para a instalação de softwares.

c) o uso de dois ou mais tipos de software de controle contra malware de diferentes fornecedores para aumentar a eficácia na proteção.

d) o procedimento para a divulgação imediata de alertas relacionados a malwares provenientes de todos os meios de comunicação, incluindo os alertas preliminares como boatos.

e) a eliminação de qualquer atualização não autorizada de software crítico de forma imediata não sendo necessária uma investigação formal.

---

7. FCC – TRE-SP/Analista Judiciário/2017

Um Analista de Sistemas do TRE-SP deve, hipoteticamente, estabelecer e especificar os controles de segurança de acordo com a Norma ABNT NBR ISO/IEC 27002:2013. Um dos controles apresenta, dentre outras, as seguintes diretrizes:

I. Mostrar um aviso geral informando que o computador seja acessado somente por usuários autorizados.

II. Não transmitir senhas em texto claro pela rede.

III. Restringir os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e para reduzir a janela de oportunidade para acesso não autorizado.

Trata-se do controle:

a) Responsabilidades dos usuários.

b) Acesso ao sistema e à aplicação.

c) Gerenciamento de acesso do usuário.

d) Acesso ao código-fonte de programas.

e) Entrada física de pessoas.

---

8. FCC – TRE-SP/Analista Judiciário/2017

Supondo-se que o TRE-SP tenha concursado profissionais que irão realizar atividades em local de trabalho remoto. A fim de garantir a segurança da informação, esse Tribunal se pautou em recomendações previstas na Norma ABNT NBR ISO/IEC 27002:2013 cujo objeto, em suas diretrizes para implementação, reza que deve haver política, medidas e controles que apoiem a segurança da informação e que a organização deve estabelecer

condições e restrições para uso em trabalho remoto. Assim, quando entendidos como aplicáveis e permitidos por lei, convém considerar:

I. Acordos de licenciamento de software que podem tornar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros.

II. Ambiente físico proposto para o trabalho remoto que inclui ambientes de trabalho não tradicionais, como aqueles referidos como: "ambientes de telecommuting", "local de trabalho flexível" e "trabalho remoto", excetuando-se, em todas as suas formas, o chamado "trabalho virtual".

III. Segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local.
Está de acordo com as recomendações previstas na norma o que consta APENAS em
a) I e III.
b) I e II.
c) II.
d) II e III.
e) III.

---

9. FCC – PGE-MT/Analista de Sistemas/2016

A norma ABNT NBR ISO/IEC 27002:2013 traz uma seção que trata da organização da segurança da informação nas organizações. Dentre os controles apresentados nessa seção está o que recomenda que
a) a segurança da informação seja analisada criticamente em intervalos planejados ou quando mudanças significativas ocorrem.
b) a segurança da informação seja considerada no gerenciamento de projetos, independente do tipo do projeto.
c) existam procedimentos definidos para o gerenciamento de mídias removíveis, de acordo com o sistema de classificação da informação.
d) um processo formal de registro e cancelamento de usuário seja definido para permitir atribuição dos direitos de acesso a esses usuários.
e) exista um processo disciplinar formal implantado e comunicado, para tomar ações contra funcionários que tenham cometido violações de segurança da informação.

GABARITO

GABARITO – QUESTÕES CESPE

1	E
2	C
3	C
4	D
5	A
6	E
7	E
8	C
9	C
10	E
11	E
12	E
13	E
14	E
15	C
16	C
17	E

18	E
19	D
20	E
21	E

GABARITO – QUESTÕES FCC

1	C
2	D
3	E
4	E
5	C
6	C
7	B
8	A
9	B
10	

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.