Aula 2
ISO 27001/27002

[FORA DO EDITAL 2023] Segurança da Informação para Câmara dos Deputados

Prof. Victor Dalton

DIREÇÃO CONCURSOS

Feito para você estudar de verdade!

Sumário

Norma ISO 27002

Considerações iniciais

O estudo de Segurança da informação envolve várias frentes. Uma delas, que corresponde à **gestão de política de segurança** a ser adotada por uma organização, para proteger os seus ativos e recuperar-se de um desastre, é norteada pela NORMA ISO/IEC 27002, que é um Código de Prática para a Gestão da Segurança da Informação.

A ISO/IEC 27002 recebeu a atual numeração em julho de 2007, e foi revisada em 2013. É uma norma de Segurança da Informação revisada em 2005 pela International Standards Organization e pela International Electrotechnical Commission, chamada anteriormente de ISO/IEC 17799. A versão original foi publicada em 2000, que por sua vez era uma cópia fiel do padrão britânico BS 7799-1:1999.

A ISO/IEC-17799 tem como objetivos a **confidencialidade, integridade e disponibilidade** das informações, os quais são fatores muito importantes para a segurança da informação.

Enfim, vamos passar por algumas ideias da norma, procurando destacar os procedimentos que mais aparecem em prova. Além disso, esta análise despertará o seu senso crítico em relação ao "espírito" da norma, fazendo que o seu bom senso possa colaborar para acertar questões sobre o assunto.

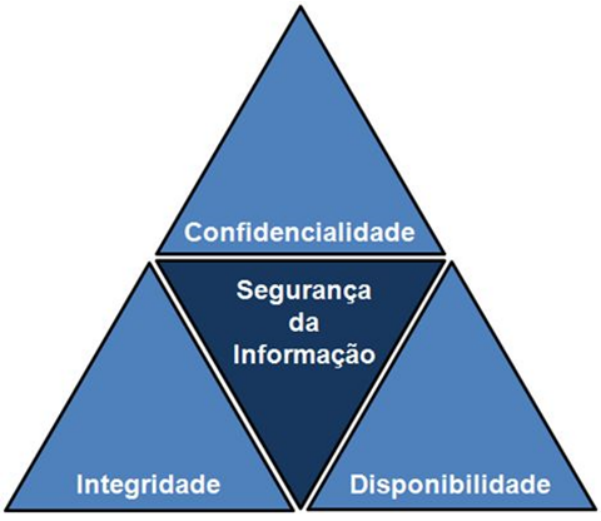
Vamos lá?

Introdução

A norma ISO 27002 ressalta que a informação é um ativo muito valioso para uma organização. Diferentemente de outros ativos, ela pode ser impressa, escrita em papel, armazenada em via eletrônica, ou até mesmo conversada. Isto posto, ela deve ser protegida com adequação.

Nesse contexto, a **segurança da informação** é alcançada por um **conjunto adequado de controles**, nos quais se incluem políticas, processos, funções de software e hardware e estruturas organizacionais, aplicados com o intuito de **proteger a informação** dos vários tipos de ameaças, para garantir a continuidade do negócio em caso de desastre, maximizar o ROI e as oportunidades de negócio.

Destaque para a tríade da segurança da informação:



Segundo a norma:

Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Glossário

Para uniformização da linguagem, é interessante ter em mente as definições abaixo, uma vez que os controles recomendados utilizam e repetem (e muito) os termos abaixo citados. Já vi, inclusive, questões de prova em cima apenas desses entendimentos!

Ativo – qualquer elemento que possua valor para a organização

Controle – forma de gerenciar o risco, seja ele uma política, diretriz, procedimento, prática...

Evento – ocorrência em um sistema, serviço ou rede, que indica uma probabilidade de violação da política de Seg Info, ou uma falha de controles, ou outra coisa, ainda desconhecida

Incidente – um evento ou série de eventos indesejados ou inesperados, com grande probabilidade de ameaçar a Seg Info e comprometer o negócio. Todo incidente é um evento, mas nem todo evento é um incidente. **Ex:** uma porta indevidamente aberta é um evento. Se a porta aberta mostra uma sala violada, com mesas e gavetas mexidas, temos um incidente.

Política – recomendações formais da direção da organização

Recurso de processamento da informação – qualquer sistema que processe informações, serviço ou infraestrutura, incluindo aí as instalações físicas nas quais eles estão instalados

Risco – é a probabilidade de um evento + consequências

Ameaça – causa potencial de um incidente não desejado

Vulnerabilidade – fragilidade que pode ser explorada por ameaças

A partir de agora, veremos um resumo das **14 seções de controles de segurança da informação que, juntas, totalizam 35 objetivos de controle e 114 controles**. Cada seção contém um número de categorias principais de segurança da informação e cada categoria principal de segurança da informação contém:

a) **um objetivo de controle** que define o que deve ser alcançado; e

b) **um ou mais controles** que podem ser aplicados para se alcançar o objetivo do controle.

As descrições dos controles estão estruturadas da seguinte forma:

Controle

Define qual o controle específico para atender ao objetivo do controle. Veremos **todos** a seguir, **em azul**.

Diretrizes para a implementação

Contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas. As diretrizes mais relevantes serão ilustradas ao longo dos próximos capítulos.

Políticas de Segurança da Informação

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

· **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 envolvidas;**

· **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;**

Orientação da Direção para Segurança da Informação

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

· **Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas** (ativos e processos de segurança claramente definidos, e pessoas competentes e capazes de cumprir com as responsabilidades definidas)

· **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** (dentro daquele espírito que, ao concentrar poder em uma pessoa isolada, será ela quem poderá violar a segurança da informação)

· **Convém que contatos apropriados com as autoridades relevantes sejam mantidos** (corpo de bombeiros, autoridades fiscalizadoras)

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

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

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

· **Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis** (considerar registro dos dispositivos móveis, restrição a instalação de software, proteção contra malware e outros)

· **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** (caso a organização permita tal tipo de trabalho)

Segurança em Recursos Humanos

Antes da contratação - Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papeis para os quais eles foram selecionados

· **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** (podendo inclusive **verificar crédito ou registros criminais**)

· **Convém que as obrigações contratuais com funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando, dentre outros:**

a) Termo de confidencialidade ou de não divulgação, para funcionários, fornecedores e partes externas; e

b) Responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização;

Durante a contratação - Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação

· 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

· 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 suas funções

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

Encerramento e mudança da contratação – Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação

· 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 (ou seja, podem existir procedimentos em acordos de confidencialidade que devem ser respeitados, mesmo após o encerramento do vínculo de trabalho)

Gestão de ativos

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

· 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

· Convém que os ativos mantidos no inventário tenham um proprietário (que será o responsável pelo ativo durante o seu ciclo de vida)

· 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 (para que todos tenham consciência da responsabilidade em utilizar aquele ativo)

· 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

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

· Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada (convém que os proprietários dos ativos sejam responsáveis por esta classificação).

· Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização A norma não sugere um esquema de classificação dos ativos, mas indica que deve ser criado um esquema consistente para toda a organização, e que esse nível de proteção seja baseado na confidencialidade, integridade, disponibilidade e quaisquer outros requisitos. (Exemplos de rótulos: pública, interna, confidencial, secreta)

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

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

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

· **Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais** (guarda e/ou destruição de forma segura e protegida, com registro, para possibilitar auditoria)

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

Controle de acesso

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

· **Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios** (considerando acessos lógico e físico; filosofia do "tudo é proibido a menos que expressamente permitido"). A política do controle de acesso deve ser orientada por dois princípios:

o Necessidade de conhecer: permissão para acesso à informação porque precisa dela para desempenhar suas tarefas;

o Necessidade de uso: permissão para acesso aos recursos de processamento da informação para desempenhar suas tarefas.

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

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

· **Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição dos direitos de acesso** (ID único de usuário; IDs compartilhados apenas por necessidades operacionais ou de negócios)

· **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 tipos de sistemas e serviços**

· **Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados** (tais IDs devem ser diferentes dos IDs "comuns", para que o usuário não fique utilizando um ID privilegiado para atividades rotineiras)

· **Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal** (declaração de confidencialidade, responsabilizando o usuário quanto às implicações do uso indevido da senha).

· **Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares** (e também depois de promoções, remanejamento ou encerramento do contrato)

· **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 ou acordos, ou ajustados após a mudança destas atividades**

Tornar os usuários responsáveis pela proteção das suas informações de autenticação

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

o senhas fáceis de lembrar;

o não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;

o não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário);

o isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

o caso a senha seja temporária, ela deve ser mudada no primeiro acesso(log-on);

o não compartilhar a informação de senhas de usuários individuais;

Prevenir o acesso não autorizado aos sistemas e aplicações

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

· **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)**

· **Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade** (procedimentos que evitem erros, exijam mudança de senha no primeiro acesso e em intervalos regulares, não mostra as senhas quando forem digitadas)

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

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

Criptografia

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

· **Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação** (identificar o nível requerido de proteção dos dados, papéis e responsáveis). Controles criptográficos podem ser usados para alcançar diferentes objetivos de segurança da informação, como, por exemplo:

o **confidencialidade:** usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

o **integridade/autenticidade**: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;

o **não repúdio:** usando técnicas de criptografia para obter evidência da ocorrência ou não ocorrência de um evento ou ação;

o **autenticação:** usando técnicas criptográficas para autenticar usuários e outras camadas sistêmicas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

· **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** (geração, armazenamento, arquivo, recuperação, distribuição, retirada e destruição das chaves)

Segurança Física e do Ambiente

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

· **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** (barreiras físicas onde aplicável, alarmes, sistemas de detecção de intrusos)

· **Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido** (registros de data/hora de entrada/saída, auditoria

eletrônica, uso de identificação visível por funcionários e outros - crachás)

· **Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações** (evitar acesso do público, instalações discretas com a menor identificação possível de sua finalidade)

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

· **Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras** (ex: áreas não ocupadas devem ser trancadas e verificadas periodicamente, não permitir a utilização de equipamentos de gravação)

· **Convém que pontos de acesso, como áreas de entrega 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**

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

· **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**

· **Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades** (suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado)

· **Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos** (cabeamento preferencialmente subterrâneo, ou proteção alternativa adequada; cabeamento de energia segregado do cabeamento de comunicações para evitar interferência; cabeamento blindado em sistemas sensíveis ou críticos)

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

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

· **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** (controles adequados, ex: política de mesa limpa, controles de acesso a computadores, comunicação segura com o escritório)

· **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**

· **Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada** (encerrar as sessões ativas, desconectar dos serviços de rede ou usar tela de bloqueio, quando os equipamentos não estiverem em uso)

· **Convém que sejam adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação** (cofres, armários ou outros para papéis e mídias sensíveis, bloqueio de computadores com senha, token ou mecanismo de autenticação similar quando não usados, evitar uso não autorizado de fotocopiadoras, remover documentos sensíveis imediatamente de impressoras. Considerar o uso de impressoras com código PIN, para que apenas os requerentes possam pegar suas impressões)

Segurança nas Operações

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

· **Convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles** (instalação e configuração de sistemas, cópias de segurança, procedimentos em caso de falha do sistema, e outros)

· **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** (gestão de mudanças formal)

· **Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema** (gestão de capacidade)

· **Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção** (softwares executados em diferentes sistemas, usuários com perfis diferentes para cada ambiente, dados sensíveis não devem ser copiados para ambientes de teste sem o devido controle)

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

· **Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra *malware*, combinados com um adequado programa de conscientização do usuário** (proibir software não autorizado, prevenir ou detectar websites maliciosos, instalar e utilizar periodicamente software de remoção de malware, dentre outros)

Proteger contra a perda de dados

· **Convém que cópias de segurança das informações, dos software e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida** (**convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;** proteção física e ambiental apropriada para as instalações das cópias de segurança; política de backup (completa ou diferencial, por exemplo) que reflita os requisitos de negócio da organização)

Registrar eventos e gerar evidências

· **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**

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

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

· **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**

Assegurar a integridade dos sistemas operacionais

· **Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados** (implementação somente após testes exaustivos, estratégia de retorno às condições anteriores, arquivamento de versões antigas e outros)

Prevenir a exploração de vulnerabilidades técnicas

· **Convém que 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 lidar com os riscos associados**

· **Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários** (princípio do privilégio mínimo)

Minimizar o impacto das atividades de auditoria nos sistemas operacionais

· **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**

Segurança nas Comunicações

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

· **Convém que as redes sejam gerenciadas e controladas para proteger as ¡informações nos sistemas e aplicações** (responsabilidades e procedimentos, dentre outros)

· **Convém que mecanismos de segurança, níveis de serviço 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**

· **Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes** (tratar redes wireless como conexões externas, com políticas mais restritivas)

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

· **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**

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

· **Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas**

· **Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados** (acordos de confidencialidade e não-divulgação)

Aquisição, Desenvolvimento e Manutenção de Sistemas

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 serviços sobre as redes públicas

· **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**

· **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**

· **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** (caminho criptografado entre as partes envolvidas, assinaturas eletrônicas para as partes envolvidas nas transações, dentre outros)

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

· **Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização** (política de desenvolvimento seguro)

· **Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças** (obtenção de aprovação formal, controle de versão, trilha de auditoria e outros)

· **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** (plataformas operacionais incluem sistemas operacionais, banco de dados e plataformas intermediárias)

· **Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas** (quando possível e praticável, os pacotes de software providos pelos fornecedores sejam utilizados sem modificações, para evitar o risco que controles e processos de integridade embutidos no software sejam comprometidos)

· **Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação** (procedimentos para projetar sistemas de informação seguras, baseados nos princípios da engenharia de segurança, sejam estabelecidos, documentadas e aplicadas nas atividades internas de engenharia de sistemas de informação da organização. Convém que a segurança seja projetada em todas as camadas da arquitetura (negócios, dados, aplicações e tecnologia), novas tecnologias devem ser analisadas quanto aos riscos de segurança. Os princípios e os procedimentos de engenharia estabelecidos sejam analisados criticamente a intervalos regulares)

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

· **Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado** (acordos de licença, propriedade do código, testes de aceitação, e outros)

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

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

Assegurar a proteção dos dados usados para teste

Relacionamento na Cadeia de Suprimento

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

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

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

- **Convém que as organizações monitorem, analisem criticamente e auditem, a intervalos regulares, a entrega dos serviços executados pelos fornecedores**
- **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 de riscos**

Gestão de Incidentes de segurança da informação

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

- **Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação** (gestão de incidentes)
- **Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível** (gestão de eventos)
- **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**
- **Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação** (gestão de eventos)
- **Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados** (gestão de incidentes)
- **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** (gestão de incidentes – lições aprendidas)
- **Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências** (incluindo evidências forenses)

Aspectos da segurança da informação na Gestão da Continuidade do Negócio

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

· **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** (a organização deve avaliar se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre. Requisitos de segurança da informação podem ser determinados quando do planejamento da continuidade do negócio e da recuperação de desastre). **Na ausência de um planejamento formal de continuidade do negócio e de recuperação de desastre**, convém que a gestão da segurança da informação assuma que os requisitos de segurança da informação permanecem os mesmos, em situações adversas, comparadas com as condições de operação normal. Alternativamente, uma organização pode realizar uma **análise de impacto do negócio** (BIA) relativa aos aspectos de segurança da informação, para determinar os requisitos de segurança da informação que são aplicáveis nas situações adversas.

· **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** (instalação e configuração de sistemas, cópias de segurança, procedimentos em caso de falha do sistema, e outros)

· **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**

Assegurar a disponibilidade dos recursos de processamento da informação (redundâncias)

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

Conformidade

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

· **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**

· **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 software proprietários (não à PIRATARIA!)**

· **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**

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

· **Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes** (restrições à importação e/ou exportação de hardware e software de computador para execução de funções criptográficas, com funções criptográficas embutidas ou mesmo no uso da criptografia)

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

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

· **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**

· **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**

Análise final

Pois bem, acabamos de ver, de forma resumida, **todos** os controles da ISO 27002. A norma completa possui 99 páginas, detalhando esses e outros procedimentos importantes.

Entretanto, acredito que você conseguiu capturar o "espírito" da norma. Logo, ao deparar-se com os exercícios, você será capaz de enxergar, nas alternativas, sentenças que fazem (ou não fazem) sentido estar na norma, o que fará que você consiga acertar questões sobre o assunto. De qualquer forma, recomendo a visualização da mesma pelo menos uma vez, para melhor entendimento.

No resumo direcionado colocarei em uma tabela as seções, objetivos e controle e controle. Se servir de ajuda para os seus estudos... ficarei feliz em ter colaborado.

Victor Dalton

Questões para fixar

(CESPE – CGE/CE – Auditor de Controle Interno – Tecnologia da Informação – 2019)

Em uma organização em que se processam dados pessoais sensíveis, existe a preocupação com o manuseio dos dados pelos empregados, para que não aconteçam vazamentos de dados e exposição indevida de pessoas. Segundo a NBR ISO/IEC 27002, para assegurar que as referidas informações pessoais recebam o nível adequado de proteção, deve-se utilizar como controle

A) o descarte de mídias.

B) o uso aceitável de ativos.

C) o gerenciamento de chaves.

D) o provisionamento para acesso de usuário.

E) a classificação da informação.

_____

Comentários: Perceba que a preocupação é proteger a informação de forma adequada. A ISO 27002, na Gestão de Ativos, prevê que as informações devem receber um nível adequado de proteção. E, para que tal nível de proteção seja implementado, convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e

criticidade. Quando olhamos pras alternativas, vemos muitos itens que não fazem sentido. Uma pitada de bom senso sempre ajuda em questões de Normas ISO.

Resposta certa, alternativa e).

(AOCP – PC/ES – Perito Oficial Criminal – Área 2 – 2019)

De acordo com a Norma NBR ISO/IEC nº 27.002, evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação é um dos objetivos de controle associado à categoria de

A) controle de acesso.

B) organização da segurança da informação.

C) conformidade.

D) gestão de incidentes de segurança da informação.

E) segurança física e do ambiente.

_____

Comentários: Se o objetivo é não violar a legalidade da informação, certamente estamos falando da categoria da Conformidade. Nela, veremos controles focados em cumprimento de requisitos legais, proteção à propriedade intelectual, aderência à legislação vigente, dentre outros.

Resposta certa, alternativa c).

(CESGRANRIO – LIQUIGÁS – Analista de Sistemas – 2018)

Para a segurança da informação, é importante formular uma política com relação ao uso de redes e serviços de rede.

De acordo com a NBR ISO/IEC 27002, os usuários devem receber acesso

A) irrestrito às redes e restrito aos serviços de rede que tenham sido especificamente autorizados a usar.

B) irrestrito aos serviços de rede e restrito às redes que tenham sido especificamente autorizados a usar.

C) restrito às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

D) irrestrito às redes e aos serviços de rede de toda a empresa, e restrito às redes e aos serviços de rede externos.

E) irrestrito às redes e aos serviços de rede de toda a empresa, e às redes e aos serviços de rede externos.

_____

Comentários: Na categoria Controle de Acesso, temos um controle que prevê que os usuários somente devem receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar. E veja que faz sentido, né? Em uma política de segurança da informação, cada um tem acesso somente ao que lhe é permitido.

Resposta certa, alternativa c).

(CESPE – TRE/BA – Analista Judiciário – Análise de Sistemas – 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: Pela análise das alternativas, percebe-se, com bom senso, que o primeiro objetivo de resposta ao incidente será restaurar o nível de segurança normal, para depois apurar fatos, aprender lições e outras atividades relacionadas.

Resposta certa, alternativa d).

(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.

_____

Comentários: Esses controles têm por objetivo **prevenir o acesso não autorizado aos sistemas e aplicações**. O controle é **acesso ao sistema e à aplicação**.

Resposta certa, alternativa b).

(FCC – TRT/23ª Região - Analista de Tecnologia da Informação – 2016)

De acordo com a norma ABNT NBR ISO/IEC 27002:2013 a política de controle de acesso deve considerar

(A) a disponibilidade de referências de caráter satisfatórias do usuário, por exemplo, uma profissional e uma pessoal.

(B) verificações financeiras e verificações de registros criminais do usuário.

(C) ações a serem tomadas no caso de o funcionário desrespeitar os requisitos de segurança da informação da organização.

(D) a legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços.

(E) a confirmação e documentação das qualificações acadêmicas e profissionais do usuário.

_____

Comentários: A política de controle de acesso diz respeito a estabelecer, documentar e analisar criticamente uma política baseada nos requisitos de segurança da informação e dos negócios.

Tal política deverá considerar:

a) Requisitos de segurança de aplicações de negócios individuais;

b) política para disseminação e autorização da informação, por exemplo, o princípio "necessidade de conhecer" e níveis de segurança e a classificação das informações;

c) consistência entre os direitos de acesso e as políticas de classificação da informação de sistemas e redes;

d) Legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços;

e) gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;

f) segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;

g) requisitos para autorização formal de pedidos de acesso;

h) requisitos para análise crítica periódica de direitos de acesso;

i) remoção de direitos de acesso;

j) arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta;

k) regras para o acesso privilegiado.

Resposta certa, alternativa d).

(FCC – Prefeitura de Teresina – Analista de Sistemas – 2016)

De acordo com a Norma NBR ISO/IEC 27002:2013, no estabelecimento da política de segurança da informação deve-se contemplar requisitos provenientes de

(A) ambiente de ameaça da segurança futuro, estratégia de negócios e plataforma de processamento.

(B) contratos, política da presidência da organização e custos.

(C) legislação interna, recursos disponíveis e estratégia de negócios.

(D) recursos disponíveis, ambiente de ameaça da segurança atual e contratos.

(E) regulamentações, estratégia de negócio e ambiente de ameaça da segurança.

_____

Comentários: Que decoreba terrível!

Para a norma ISO 27002, a política de segurança da informação deve contemplar requisitos provenientes da **estratégia do negócio**, **regulamentações**, legislações e contratos, e **ambiente de ameaça da segurança da informação**, atual e futuro.

Resposta certa, alternativa e).

(FCC – Prefeitura de Teresina – Analista de Sistemas – 2016)

Com relação aos aspectos de responsabilidades pela segurança da informação no processo de organização da segurança da informação, de acordo com a Norma NBR ISO/IEC 27002:2013,

(A) a responsabilidade de pesquisar todos os controles é do gerente de TI.

(B) a responsabilidade pode ser terceirizada.

(C) o dirigente de mais alto nível é responsável pelos ativos da organização.

(D) tarefas podem ser delegadas para outros.

(E) o dirigente de mais alto nível deve prover todos os recursos necessários para a segurança.

_____

Comentários: Indivíduos que receberam responsabilidades de segurança de segurança da informação **podem delegar tarefas** de segurança da informação para outros. Todavia, convém que eles permaneçam responsáveis e determinem se quaisquer tarefas delegadas tenham sido corretamente executadas.

Muitas organizações atribuem a um gestor de segurança da informação a responsabilidade global pelo desenvolvimento e implementação da segurança da informação, e para apoiar a identificação de controles.

Entretanto, a responsabilidade por pesquisar e implementar os controles frequentemente permanecerá com os gestores individuais. Uma prática comum é a nomeação de um proprietário para cada ativo que, então, se torna responsável por sua proteção no dia a dia.

Resposta certa, alternativa d).

(FCC – TRT/20ª Região – Técnico de Tecnologia da Informação – 2016)

Com relação à segurança nas comunicações, a norma ABNT NBR ISO/IEC 27002:2013 possui uma seção que fornece diretrizes, controles e objetivos de controle para assegurar a proteção das informações em redes. Um desses controles recomenda que

(A) a conexão de sistemas às redes deve ser restrita, porém, nessas conexões, não é necessário autenticação.

(B) mecanismos de segurança e níveis de serviço sejam identificados e incluídos somente em acordos de serviços de redes providos internamente, excluindo-se terceirizados.

(C) a responsabilidade operacional pelas redes nunca seja separada das operações dos demais recursos computacionais.

(D) o controle de perímetro de domínio de rede seja feito por terceiros especializados.

(E) grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes de computadores.

_____

Comentários: Analisando os itens:

a) sistemas sobre redes devem ser autenticados;

b) não há motivos para excluir os terceirizados dos mecanismos de segurança das redes.

c) a responsabilidade operacional pelas redes deve ser separada das operações dos demais recursos computacionais, quando apropriado;

d) Esse controle deve ser feito por um *gateway.*

e) Essa segregação pode ser tanto em redes físicas como em redes lógicas (ex: VPN), e cada domínio deve ter perímetro bem definido.

Resposta certa, alternativa e).

(FGV – TCE/SE - Analista de Tecnologia da Informação – 2015)

Com relação à norma ISO/IEC 27002:2013, está correto afirmar que:

a) ela indica a necessidade do uso do ciclo PDCA nos processos da organização;

b) a revisão de 2013 criou uma seção específica para controles criptográficos;

c) não é mais necessário o gerenciamento de ativos, cuja cláusula foi suprimida na revisão de 2013;

d) organizações agora podem ser certificadas na última revisão (2013) da ISO 27002;

e) ela tem foco no gerenciamento de risco na segurança da informação.

_____

Comentários: Todas as assertivas acima estão incorretas, à exceção da alternativa b). Afinal, (agora) a norma possui uma seção exclusiva sobre **Criptografia**.

(FCC – TCE/CE - Técnico de Tecnologia da Informação – 2015)

A Norma NBR ISO/IEC 27002:2013 possui 14 seções de controles de segurança da informação, dentre elas,

a) Gestão de Riscos de Segurança da Informação.

b) Métricas de Sistemas de Gestão de Segurança da Informação.

c) Gestão da Segurança da Informação em Organizações da Administração Pública.

d) Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio.

e) Técnicas para Governança da Segurança da Informação.

_____

Comentários: Percebe-se que os nomes de seções supracitados inexistem na norma, à exceção da **Gestão da Continuidade do Negócio**.

Resposta certa, alternativa d).

(FCC – TCE/SP – Agente da Fiscalização Financeira – Infraestrutura de TI – 2015)

Uma empresa verificou que a norma NBR ISO/IEC 27002:2013 define como se deve proceder na questão da segurança ligada a recursos humanos. A norma estabelece, em um de seus capítulos, que os recursos humanos devem ter um acompanhamento

a) apenas antes e após o término do vínculo contratual.

b) apenas antes e durante o vínculo contratual.

c) apenas durante a vigência do período contratual.

d) apenas durante e após o término do vínculo contratual.

e) antes, durante e após o término do vínculo contratual.

_____

Comentários: A segurança em RH preconiza o acompanhamento em três "tempos": antes, durante e após a contratação.

Resposta certa, alternativa e).

(FCC – TRT/MG – Analista Judiciário – Tecnologia da Informação – 2015)

Baseado nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, um analista de TI está definindo uma política de controle de acesso às informações e aos recursos de processamento de uma organização. Nesse contexto, estas normas recomendam que

(A) os direitos de acesso dos funcionários às informações e aos recursos de processamento devem ser retirados quando o funcionário for desligado, mas não precisam ser ajustados se o funcionário mudar de cargo.

(B) os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários em intervalos regulares.

(C) um processo de registro e cancelamento de usuário, mesmo que informal, deve ser implementado para permitir atribuição de direitos de acesso.

(D) os usuários recebam acesso às redes e aos serviços de redes que necessitarem e/ou quiserem utilizar.

(E) uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada apenas nos requisitos de segurança da informação.

_____

Comentários: Todas as políticas, via de regra, devem ser revisadas quando ocorrem mudanças significativas, ou em **intervalos regulares** ou em intervalos planejados. Já sabemos que a norma costuma se expressar nestes termos.

Resposta certa, alternativa b).

(FCC – TRT/MG – Analista Judiciário – Tecnologia da Informação – 2015)

Para assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade das informações de uma organização, um analista de TI está desenvolvendo uma política para criptografia, utilizando as recomendações da seção "Criptografia" da norma ABNT NBR ISO/IEC 27002:2013. Para verificar a autenticidade ou a integridade de informações sensíveis ou críticas armazenadas ou transmitidas, esta seção da norma recomenda o uso de

(A) certificados digitais ou assinaturas digitais.

(B) códigos de autenticação de mensagens (MAC) ou criptografia de chaves públicas.

(C) criptografia de chaves assimétricas e função de hash.

(D) assinaturas digitais ou códigos de autenticação de mensagens (MAC).

(E) criptografia de chaves públicas ou certificados digitais.

_____

Comentários: Questão profunda!

Para verificação da autenticidade ou integridade, a norma recomenda a utilização de assinaturas digitais ou códigos de autenticação de mensagens (MAC).

Resposta certa, alternativa d).

(CESPE – TCU – Auditor – Tecnologia da Informação – 2015)

Entre os serviços proativos a serem prestados por um grupo de respostas a incidentes de segurança incluem-se a realização de tarefas de auditoria, a avaliação de vulnerabilidades e outras avaliações que visem identificar fraquezas ou vulnerabilidades nos sistemas antes que elas sejam exploradas.

Correto.

(CESPE – STJ – Analista Judiciário – Suporte de Tecnologia da Informação – 2015)

Conforme disposto na norma ISO 27002, as senhas de acesso devem, necessariamente, ser de uso pessoal e individual bem como devem ser mantidas sob sigilo.

_____

Comentários: A norma ISO 27002 permite o uso de IDs compartilhados, por necessidades operacionais ou de negócio, de modo que tais senhas também serão compartilhadas. Errado!

(FCC – ELETROSUL – Informática – 2016)

Considere que na Eletrosul o acesso à informação, recursos de processamento das informações e processos de negócios devem ser controlados com base nos requisitos de negócio e segurança da informação. Assim, convém

(A) que os procedimentos de controle de acesso para registro e cancelamento de usuários incluam fornecer aos usuários uma declaração por escrito dos seus direitos de acesso.

(B) considerar os controles de acesso lógico e físico separadamente, já que os controles lógicos são mais importantes e devem ter prioridade sobre os demais controles, pois estão descritos na política de segurança da informação.

(C) que questões de legislação pertinentes e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços estejam em um documento próprio, separado da política de controle de acesso.

(D) estabelecer regras baseadas na premissa "tudo é permitido, a menos que expressamente proibido" em lugar da regra mais fraca "tudo é proibido, a menos que seja expressamente permitido".

(E) fornecer senhas aos usuários de maneira segura, através de mensagens de e-mail, SMS ou arquivo de senha.

_____

Comentários: Analisando os itens, percebemos que:

a) O Gerenciamento de Acesso recomenda que um processo formal seja estabelecido para o registro e cancelamento de usuários, e tal processo envolve a assinatura de uma declaração de confidencialidade, além dos direitos de acesso. Correta.

b) acesso físico e lógico são igualmente importantes no sentido de prevenir incidentes de segurança da informação;

c) a legislação pertinente sempre deve ser levada em consideração, para qualquer regramento de segurança da informação. Não se pode infringir leis no estabelecimento da política de segurança da informação.

d) as regras devem ser estabelecidas na política do "tudo é proibido, exceto o expressamente permitido";

e) a norma não especifica as melhores mídias para envio de senha, mas enfatiza que as senhas distribuídas inicialmente devem ser temporárias, para que o usuário a modifique no primeiro acesso.

Resposta certa, alternativa a).

(FGV – TCE/SE - Analista de Tecnologia da Informação – 2015)

Com relação à norma ISO/IEC 27002:2013, está correto afirmar que:

a) ela indica a necessidade do uso do ciclo PDCA nos processos da organização;

b) a revisão de 2013 criou uma seção específica para controles criptográficos;

c) não é mais necessário o gerenciamento de ativos, cuja cláusula foi suprimida na revisão de 2013;

d) organizações agora podem ser certificadas na última revisão (2013) da ISO 27002;

e) ela tem foco no gerenciamento de risco na segurança da informação.

_____

Comentários: Como nós vimos, a ISSO 27002 de 2013 criou um controle novo chamado **Criptografia**.

Resposta certa, alternativa b).

Questões Comentadas

1.(CESPE – DPE/RO – Analista da Defensoria Pública– 2022)

De acordo com a Norma NBR ISO/IEC n.º 27002, no gerenciamento da segurança em redes, tecnologias aplicadas como autenticação, encriptação e controles de conexões de rede são

a) serviços voltados à confidencialidade do tráfego de rede.

b) controles de segurança essenciais para a segregação de redes.

c) características típicas de um ambiente seguro de rede.

d) diretrizes para implementação de segurança de serviços de rede.

e) funcionalidades de segurança de serviços de rede.

Comentários:

Segundo a ISO 27002 Funcionalidades de segurança de serviço de rede podem ser:

a) tecnologias aplicadas para segurança de serviços de redes como autenticação, encriptação e controles de conexões de rede;

b) parâmetros técnicos requeridos para uma conexão segura com os serviços de rede de acordo com as regras de conexão de redes e segurança;

c) procedimentos para o uso de serviços de rede para restringir o acesso a serviços de rede ou aplicações, onde for necessário.

Desta forma autenticação, encriptação e controles de conexões de rede são FUNCIONALIDADES de segurança, ou seja, características desejáveis em uma rede.

Resposta correta, alternativa e).

2. (FCC – TJ/SC – Analista de Sistemas– 2021)

Considere:

Manter a confidencialidade da informação de autenticação secreta, garantindo que ela não seja divulgada para quaisquer outras partes, incluindo autoridades e lideranças.

De acordo com a Norma ABNT NBR ISO/IEC 27002:2013, essa recomendação é do âmbito de

a) gerenciamento de acesso do usuário.

b) responsabilidades dos usuários.

c) controle de acesso ao sistema e à aplicação.

d) controles criptográficos.

e) responsabilidades e procedimentos operacionais.

Comentários:

No item 9.3.1 da norma ISO 27002 temos que...

"Convém que todos os usuários sejam informados para:

a) manter a confidencialidade da informação de autenticação secreta, garantido que ela não seja divulgada para quaisquer outras partes, incluindo autoridade e lideranças"

É responsabilidade dos usuários manter a confidencialidade de autenticação secreta, não podendo ser divulgada nem para autoridades e nem lideranças. Veja que é algo que faz sentido, pois tais procedimentos não podem ser impedidos por sistemas ou controles, somente pelos próprios usuários.

Resposta correta, alternativa b).

3. (FCC – TJ/SC – Analista de Sistemas– 2021)

De acordo com a Norma ABNT NBR ISO/IEC 27002:2013, no âmbito do Gerenciamento da segurança em redes, um método de controlar a segurança da informação em grandes redes é

a) definir que os administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

b) definir 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.

c) estabelecer e implementar regras definindo critérios para a instalação de software pelos usuários.

d) definir que as atualizações do software operacional, aplicativos e bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada.

e) dividir em diferentes domínios de redes que podem, por exemplo, ser escolhidos com base no nível de confiança.

Comentários:

Quando analisada a NBR ISO 27002, em relação à segurança nas comunicações:

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

Desta forma a implementação pode ser feita dividindo os domínios de redes.

Resposta correta, alternativa e).

4.(CESPE – SEFAZ/AL – Auditor Fiscal de Finanças e Controle– 2021)

Considere que, em uma organização, tenha sido realizada uma inspeção aleatória para detectar e coibir a retirada não autorizada de equipamentos e ativos, sem aviso prévio aos colaboradores. Nesse caso, de acordo com a NBR ISO/IEC 27002, é dispensável autorização prévia ou aviso aos colaboradores somente se os ativos armazenarem ou processarem informações sensíveis aos negócios da organização.

Comentários:

Quanto à segurança física e do ambiente na perspectiva da NBR ISO 17002 "Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia"

Resposta incorreta.

5. (CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

De acordo com a NBR ISO/IEC 27002, uma política para transferência de informações tem como objetivo a proteção da transferência de informações por meio de todos os tipos de recursos de comunicação.

Comentários:

À luz da ISO 27002 "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."

Resposta correta.

6. (CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

Controles criptográficos como assinaturas digitais e códigos de autenticação de mensagens são aplicáveis para verificar a integridade de informações sensíveis ou críticas, armazenadas ou transmitidas.

Comentários:

Tanto assinatura digital quanto códigos de autenticação são responsáveis por verificar a integridade das mensagens

Resposta correta.

7.(CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

No que se refere à NBR ISO/IEC 27002:2013 e a confiabilidade, integridade e disponibilidade, julgue o item a seguir. No contexto de política de segurança da informação no relacionamento com fornecedores, convém que sejam estabelecidos, quando necessário, acordos de contingência e recuperação para assegurar a disponibilidade da informação.

Comentários:

Quando necessário deve-se fazer acordos de contingência e recuperação. Faz todo o sentido, pois backups precisam ter metas claras de periodicidade e prazo de recuperação.

Resposta correta.

8. (CESPE – BANESE – Desenvolvimento– 2021)

Cabe ao provedor de serviço em nuvem disponibilizar informações sobre os países e a localização geográfica onde os dados serão armazenados, para que as entidades regulatórias e as jurisdições possam ser mapeadas pelo cliente.

Comentários:

É necessário que a equipe de TI tenha essa informação, visto que estes precisam se adequar às leis locais onde estão os provedores da nuvem.

Resposta correta.

9. (CESPE – BANESE – Desenvolvimento– 2021)

Implementando-se um conjunto adequado de controles, de forma coordenada e coerente com os riscos associados a uma visão holística da organização, alcança-se a segurança da informação.

Comentários:

A segurança da informação só pode ser alcançada pela implementação de um conjunto adequado de controles, tais qual políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware.

Para além deste ponto, para que sejam implementados esse conjunto de controles é necessário ter uma visão global da empresa, visão holística.

Resposta correta.

10.(CESPE – BANESE – Desenvolvimento– 2021)

Soluciona-se a vulnerabilidade de um sistema de criptografia simétrica por meio da utilização de chaves diferentes para cifrar e decifrar mensagens.

Comentários:

A própria ISO 27002 traz como informação adicional "Técnicas criptográficas podem ser também utilizadas para proteger chaves criptográficas."

Pode-se utilizar as duas formas de criptografia, sendo a criptografia simétrica como um sistema de criptografia de dados e a chave assimétrica para autenticação e troca de chaves.

Resposta correta.

11. (CESPE – PG/DF – Analista de Sistema– 2021)

O fornecimento de evidências formais da aplicação de testes suficientes por empresa de desenvolvimento de sistemas terceirizado contra a presença de vulnerabilidades conhecidas em sistemas novos ou em processo de manutenção é uma diretriz para implementação do controle relacionado à supervisão e ao monitoramento de atividades de desenvolvimento terceirizado pela organização.

Comentários:

É necessário que antes da implementação de um controle terceirizado sejam feitos testes suficientes, oferecendo evidências de que o sistema não seja frágil.

Resposta correta.

12.(CESPE – MPE/AP – Tecnologia da Informação– 2021)

De acordo com a NBR ISO/IEC 27002, quando do desenvolvimento de uma política sobre o uso de controles criptográficos, convém considerar

a) a identificação do nível requerido de proteção com base na avaliação de risco, considerando-se o tipo, a força e a qualidade do algoritmo de criptografia.

b) a realização de cópias de segurança ou arquivamento das chaves criptográficas.

c) a manutenção de registro e auditoria das atividades relacionadas ao gerenciamento de chaves.

d) a implementação de um firewall com vistas à melhora do algoritmo de criptografia.

e) a manutenção de um registro de auditoria de todos os acessos a código-fonte de programas.

Comentários:

"Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação" (identificar o nível requerido de proteção dos dados, papéis e responsáveis).

Resposta correta, alternativa a).

13. (SELECON – EMGEPRON – Analista Técnico – 2021)

Entre as Normas da ISO/IEC 27000, a ISO 27002 trata da adoção das práticas, imprescindíveis para blindar a empresa contra ataques cibernéticos e demais ameaças. Duas dessas práticas são descritas a seguir.

I. É indispensável realizar a definição dos procedimentos e das responsabilidades da gestão e a operação de todos os recursos ligados ao processamento das informações. Para isso, é preciso gerenciar os serviços terceirizados, o planejamento dos recursos dos sistemas para reduzir riscos de falhas, a criação de processos para gerar cópias de segurança, a recuperação e a administração segura das redes de comunicação.

II. Antes de contratar funcionários ou fornecedores, é preciso fazer uma análise cuidadosa, principalmente se forem ter acesso a informações sigilosas. O objetivo dessa atitude é eliminar o risco de roubo, mau uso ou fraude dos recursos. Uma vez atuando na organização, o funcionário deve ser conscientizado sobre as ameaças que expõem a segurança da informação, bem como sobre as suas obrigações e responsabilidades.

As práticas descritas em I / II são denominadas, respectivamente:

a) Gerenciamento de operações e comunicações/ Segurança física e do ambiente

b) Gerenciamento de operações e comunicações/ Segurança em Recursos Humanos

c) Gestão de incidentes de segurança da informação/ Segurança física e do ambiente

d) Gestão de incidentes de segurança da informação/ Segurança em Recursos Humanos

Comentários:

Analisando cada uma das afirmativas.

I - Este é um ponto que se relaciona ao gerenciamento de operações e comunicações.

II - Só pelo "Antes de contratar o funcionário..." fica evidente que esta afirmativa está relacionada aos Recursos Humanos.

Resposta correta, alternativa b).

14.(CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

De acordo com a NBR ISO/IEC 27002, a política de senhas da organização deve permitir o envio de senhas de acesso em texto claro, por correio eletrônico, quando se tratar de senhas temporárias com prazo de validade definido.

Comentários:

Perceba o grande erro desta questão, "... envio de senhas de acesso em texto claro.."

É pertinente lembrar que as senhas não podem ser visualizadas por ninguém além do usuário.

Além de toda a explicação acima, veja o que a ISO 27002 diz sobre.

9.4.2 Procedimentos seguros

Convém que o procedimento para entrada no sistema operacional seja configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada (log-on) revele o mínimo de informações sobre o sistema ou aplicação, deforma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado. Convém que um bom procedimento de entrada no sistema (log-on):

...

j) nao transmita senhas em texto claro pela rede;

....

Resposta incorreta.

15. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

Conforme prescreve a NBR ISO/IEC 27002 a respeito do controle de acesso ao código-fonte de programas, para que se reduza o risco de corrupção de programas de computador na organização, convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte.

Comentários:

Segundo a ISO 27002 no item 9.4.5 Controle de acesso ao código-fonte de programas "Convém que o acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) seja estritamente controlado...".

Resposta correta.

16. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

De acordo com a NBR ISO/IEC 27002, as ferramentas de gerenciamento de informações de autenticação aumentam a eficácia desse controle e reduzem o impacto de uma eventual revelação de informação de autenticação secreta.

Comentários:

Dentro das informações adicionais no item 9.3.1 Uso da informação de autenticação secreta diz-se:

"O fornecimento de um Simples Sign On (SSO) ou outras ferramentas de gerenciamento de informação de autenticação secreta reduz o número de informação de autenticação secreta que os usuários são solicitados a proteger, aumentando dessa forma a eficácia desse controle. Entretanto, estas ferramentas podem também aumentar o impacto da revelação da informação de autenticação secreta."

O grande problema nesta questão é dizer que o impacto é reduzido, quando na realidade eles aumentam o impacto em uma eventual revelação de informação de autenticação secreta.

Resposta incorreta.

17. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

A contratação de seguros contra sinistros digitais é uma medida de transferência de riscos relacionados a possíveis impactos potencialmente causados por vulnerabilidades e ameaças à segurança da informação organizacional.

Comentários:

A ISO 27002 provém a transferência de riscos para terceiros.

Resposta correta.

18.(CESPE– Ministério da Economia – Tecnologia da Informação – 2020)

No que diz respeito a controle de entrada física, a norma ISO/IEC 27002:2013 recomenda que o acesso às áreas onde são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado, mediante a implementação de controles de acesso apropriados, que podem ser, por exemplo, mecanismos de autenticação de dois fatores, tais como cartões de controle de acesso e PIN (personal identification number).

Comentários:

A questão foi totalmente transcrita da própria ISO 27002 no item 11.1.2 Controles de entrada física.

"Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes:

...

b) convém que o acesso às áreas em que são processadas ou armazenadas inforrnações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados, por exemplo, mecanismos de autenticação de dois fatores, como, cartões de controle de acesso e PIN (personal identification number);

...."

Resposta correta.

19.(AOCP– MJSP– Analista de Governança de Dados– 2020)

O valor de um Ativo pode ser considerado uma vulnerabilidade relacionada a qual tópico previsto na ISO 27002?

a) Contratação.

b) Perímetro de segurança.

c) Retirada de direito de acesso.

d) Segurança em escritórios, salas e instalações.

e) Segurança de equipamentos.

Comentários:

No item 9.2.5 Análise crítica dos direitos de acesso de usuário temos a seguinte informação adicional: "Este controle compensa possíveis vulnerabilidades na execução dos controles de 9.2.1, 9.2.2 e 9.2.6."

O item 9.2.1 corresponde ao Registro e cancelamento de usuário.

O item 9.2.2 corresponde ao Provisionamento para acesso de usuário

O item 9.2.6 corresponde à retirada ou ajuste dos direitos de acesso.

Veja que nas opções dadas, dos três itens, apenas o item 9.2.6 está entre as opções como Retirada de direito de acesso.

Resposta correta, alternativa c).

20. (AOCP– MJSP– Analista de Governança de Dados– 2020)

Em uma situação na qual é necessário o acesso externo a informações, assinale a alternativa que apresenta uma recomendação da ISO 27002.

a) Limitar o acesso às informações antes da implantação dos controles apropriados.

b) Garantir o acesso às informações para avaliação das vulnerabilidades posteriores.

c) Permitir o acesso às informações dentro de um ambiente de testes.

d) Bloquear totalmente o acesso às informações antes da implantação dos controles apropriados.

e) Impor normas de acesso independentemente das particularidades de cada agente externo.

Comentários:

O item 9.1.1 Política de controle de acesso em sua informações adicionais nos traz que "... a) 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".

Analisando cada uma das alternativas com esta ideia em mente.

A) Perceba que neste ponto há uma permissão mesmo que não tenha todos os controles apropriados, neste caso estamos permitindo algo que não está expressamente proibido, entrando na regra mais fraca. Alternativa incorreta.

B) Na alternativa b é proposto que as vulnerabilidades estejam expostas. Se não há controle em relação as vulnerabilidades, então não há como permitir este acesso. Alternativa incorreta.

C) Em um ambiente de teste há diversas vulnerabilidades a serem expostas. Alternativa incorreta.

D) Perceba que nesta alternativa já há uma proibição, e que esta proibição só será revogada quando todos os controles apropriados estiverem implantados. Alterativa correta.

E) Deve haver uma norma centralizada, não faz sentido dar a cada um o acesso como melhor lhe convém, isso possibilita o enfraquecimento de segurança do sistema.

Resposta correta, alternativa d).

21.(AOCP– MJSP– Analista de Governança de Dados– 2020)

Pedro está aplicando a norma ISO 27002 em sua organização. De acordo com essa norma, qual vulnerabilidade Pedro deve estar ciente que pode surgir durante a autorização para recursos de processamento de informação?

a) Uso de notebook pessoal.

b) Sites maliciosos.

c) Ferramentas antivírus.

d) Aplicativos móveis.

e) Sistemas on-line.

Comentários:

Quando se trata de processamento de informação, existem diretrizes cabíveis a equipamentos de usuários sem monitoração, neste caso, a alternativa que se aplica a este ponto é a questão de equipamentos pessoais como o notebook.

Resposta correta, alternativa a).

22.(FCC – AL/AP– Desenvolvedor de Sistemas– 2020)

No que diz respeito à gestão de incidentes de segurança da informação, é recomendável que a organização defina como identificar, coletar, adquirir e preservar evidências, além de que procedimentos internos sejam desenvolvidos e seguidos para os propósitos de ação legal ou disciplinar, quando necessário. Segundo a norma ABNT NBR ISO/IEC 27002:2013, é recomendável que os procedimentos para registro, guarda e divulgação de evidência de incidentes levem em conta

a) a ficha criminal dos colaboradores da organização.

b) a classificação da ação disciplinar ou legal pelos incidentes ocorridos na organização.

c) o número de incidentes ocorridos em cada mês.

d) papéis e responsabilidades das pessoas envolvidas.

e) os custos envolvidos e o impacto em cada setor da organização.

Comentários:

Quando analisado o item 16.1.7 Coleta da evidência da ISO 27002.

"... Convém que os procedimentos

levem em conta:

a) cadeia de custódia;

b) segurança da evidência;

c) segurança das pessoas;

d) papéis e responsabilidades das pessoas envolvidas;

e) competência do pessoal;

f) documentação;

g) resumo do incidente."

Resposta correta, alternativa d).

23.(FCC – TRT/RS– Tecnologia da Informação – 2020)

Texto 4A04-I

Um hacker invadiu o sistema computacional de determinada instituição e acessou indevidamente informações pessoais dos colaboradores e servidores. Durante a ação, foram alterados os registros de logs do sistema operacional e das aplicações, a fim de dificultar o trabalho de auditoria. Após o ocorrido, identificaram-se as seguintes ações do hacker.

I Exploração, a partir da Internet, de uma vulnerabilidade da página de notícias do portal da instituição localizada no servidor web, o que permitiu o acesso não autorizado à rede interna.

II Utilização de um script para alteração dos registros dos logs, com a troca dos endereços IP reais por fictícios.

III Quebra das credenciais administrativas do servidor de banco de dados dos sistemas internos, a partir do servidor web e utilização da técnica de ataques de dicionário.

IV Acesso de forma não autorizada ao servidor de banco de dados dos sistemas internos, para efetuar a extração das informações pessoais de colaboradores e servidores.

A equipe incumbida de analisar o caso concluiu que o risco era conhecido e considerado alto, já tendo sido comunicado à alta gestão da instituição; a vulnerabilidade explorada e sua correção eram conhecidas havia mais de seis meses, bem como a inexistência de dependências e da troca de dados entre os servidores de web e banco de dados; o incidente poderia ter sido evitado com o uso eficaz dos controles de segurança da informação.

Com base na NBR ISO/IEC n.º 27002, é correto afirmar que, no cenário apresentado no texto 4A04-I, foram explorados os controles de

a) manutenção de equipamentos e de segurança física, pela ineficiência das manutenções preventivas recomendadas e da proteção física dos servidores web e de banco de dados.

b) manutenção de equipamentos e de segregação de rede, pela ineficiência das manutenções preventivas recomendadas e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

c) segurança física e de segregação de rede, pela ineficiência da proteção física e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

d) gestão de vulnerabilidades técnicas e de segurança física, pela ineficiência do monitoramento e das correções das vulnerabilidades e da proteção física dos servidores web e de banco de dados.

e) gestão de vulnerabilidades técnicas e de segregação de rede, pela ineficiência do monitoramento e das correções das vulnerabilidades e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

Comentários:

Em um primeiro momento foi utilizado a rede para acessar esta vulnerabilidade, sendo assim, são descartados as opções que envolvam a segurança física e nem houve problemas com manutenção de equipamentos, visto que o ataque foi feito via script, portanto só nos resta a alternativa e).

Resposta correta, alternativa e).

24.(FCC – TRT/RS– Tecnologia da Informação – 2022)

Para impedir perdas, danos, furtos ou roubos, ou comprometimento de ativos e interrupção das operações da organização, a norma ABNT NBR 27001:2013 recomenda que

a) os equipamentos sejam ligados diretamente em tomadas novas ou testadas por profissionais especializados e que a corrente elétrica seja 220 V.

b) os equipamentos devem ter uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.

c) equipamentos ou softwares podem ser retirados do local sem autorização prévia, desde que sob a vista de um funcionário da área de TI.

d) os equipamentos que contenham mídias de armazenamento de dados não precisam ser examinados antes da reutilização, uma vez que são ativos registrados da organização.

e) o cabeamento de energia e telecomunicações deve ser colocado no mesmo conduíte.

Comentários:

Analisando cada uma das alternativas:

A) Primeiramente temos um erro de física nessa alternativa, visto que Voltagem é usado para medida de diferença de potencial elétrico e não para corrente elétrica. O segundo ponto é que a ISO 27001 diz que os equipamentos devem ser devidamente instalados conforme especificação do fornecedor, podendo utilizar equipamentos de 110V ou 220V. Errado.

B) Segundo o controle 11.2.4 item 4 diz respeito a manutenção correta dos equipamentos para continuidade da integralidade e disponibilidade. Correto.

C) Segundo a NBR 27001:2013 "Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia". Errado

D) Ainda segundo a NBR 27001:2013 "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". Errado.

E) "Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos". Perceba que se colocados os cabos de energia e de telecomunicações em um mesmo conduíte este apresentará interferência, portanto a alternativa está incorreta.

Resposta correta, alternativa b).

25.(CESPE – APEX Brasil– Tecnologia da Informação e Comunicação – 2022)

Conforme a NBR ISO/IEC 27001, as organizações devem realizar avaliações de risco de segurança da informação a) em intervalos planejados ou quando mudanças significativas são propostas para ocorrer.

b) mensalmente.

c) semestralmente.

d) anualmente.

Comentários:

Segundo a NBR 27001, uma das medidas para assegurar que a segurança da informação esteja implementada e operando de acordo com as políticas e procedimentos da organização é: "Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas"

Resposta correta, alternativa a).

26.(CESPE – SEFAZ/AL– Auditor Fiscal– 2021)

Segundo a referida norma, um incidente de segurança da informação é uma ocorrência identificada de um estado de sistema, serviço ou rede, que indica uma possível falha no sistema de gestão da informação.

Comentários:

Segundo a referida norma um incidente é um evento ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Neste caso a questão está se referindo a um evento.

Resposta errada.

27.(CESPE – SEFAZ/AL– Auditor Fiscal– 2021)

A NBR ISO/IEC 27001 prescreve que, por medida de segurança, as informações documentadas como evidências de monitoramento, de auditoria e de análises críticas da segurança da informação sejam descartadas imediatamente após serem apresentadas aos gestores principais da organização.

Comentários:

Perceba que essa afirmação por si só é um absurdo, porém vamos ver o que a ISO 27001 diz sobre:

7.5.3 Controle da informação documentada.

A informação documentada requerida pelo sistema de gestão de segurança da informação e por esta Norma deve ser controlada para assegurar que:

a) esteja disponível e adequada para o uso, onde e quando necessário;

...

Para controle da informação documentada, a organização deve considerar as seguintes atividades, conforme aplicadas:

a) distribuição, acesso, recuperação e uso;

b) armazenagem e preservação, incluindo a preservação da legibilidade;

c) controle de mudanças (por exemplo, controle de versão);

d) retenção e disposição

Resposta errada.

28. (IBFC– Prefeitura de São Gonçalo do Amarante/ RN – Analista de Sistema – 2021)

De acordo com a norma ISO 27001, a classificação de uma informação possui um processo de quatro etapas. A este respeito, assinale a alternativa correta.

a) Inventário de Ativos, Classificação da Informação, Rotulagem da Informação e Manuseio da informação

b) Análise de Conteúdo da Informação, Varredura de Vírus, Rotulagem da informação e Manuseio da informação

c) Classificação da Informação, Eliminação de Riscos para os documentos alterados, Inventário de Ativos e Manuseio da informação

d) Classificação da Informação, Armazenamento da Informação, Varredura de Vírus e Análise de Conteúdo da Informação

Comentários:

Quando se trata da classificação da informação, existem 4 etapas a qual ela deve passar:

(1) Primeiramente a informação deve ser inserida em um Inventário de Ativos;

(2) estando as informações no inventário, estas devem ser classificadas (Confidencial, restrita, uso interno, pública);

(3) com as informações já classificadas, estas devem ser rotuladas;

(4) e por fim, fazer o manuseio dos ativos.

De forma resumida as etapas são Inventário de ativos>Classificação da Informação> Rotulagem da informação> Manuseio da informação.

Resposta correta, alternativa a).

29.(FGV – IMBEL– Supervisor TI– 2021)

A Associação Brasileira de Normas Técnicas, ABNT, é responsável pela elaboração das Normas Brasileiras como, por exemplo, a ABNT NBR ISO/IEC 27001:2013, sobre aspectos da Segurança da Informação.

Dado que a sigla ISO deriva de International Organization for Standardization, assinale a correta natureza das normas NBR ISO.

a) São normas brasileiras que passam a ser adotadas pela ISO.

b) São normas definidas em conjunto com a ISO.

c) São traduções de normas da ISO que passam a ser adotadas pela ABNT.

d) São normas da ISO adaptadas pela ABNT às práticas brasileiras.

e) São normas brasileiras compiladas a partir da combinação de outras normas da ISO.

Comentários:

Sempre quando houver uma norma do tipo NBR ISO, significa que uma norma internacional ISO foi traduzida para o português pela ABNT.

Resposta correta, alternativa c).

30.(CESPE – PG/DF– Analista de Sistemas– 2021)

Conscientização, educação e treinamento em segurança da informação são previstos na norma como segurança em recursos humanos durante a contratação.

Comentários:

Durante a contratação - Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação

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

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 suas funções

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

Resposta correta.

31. (CESPE – PG/DF– Analista de Sistemas– 2021)

A manutenção de contatos apropriados com autoridades relevantes relaciona-se com a organização da segurança da informação na medida em que reduz o uso indevido de ativos da entidade.

Comentários:

No item 6.1.3 Contato com autoridades nos diz que:

Convém que contatos apropriados com autoridades relevantes sejam mantidos.

Para além disso, nas informações adicionais temos o seguinte texto:

"Manter tais contatos pode ser um requisito para apoiar a gestão de incidentes de segurança da informação..."

Resposta errada.

32.(CESPE – PG/DF– Analista de Sistemas– 2021)

Ao analisar criticamente o sistema de gestão de segurança da informação (SGSI) da organização, a alta direção deve incluir oportunidades de melhoria nesse sistema.

Comentários:

No item 5.1 Liderança e comprometimento, nos é dado o seguinte texto

"A alta Direção deve demonstra sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

()... g) promovendo a melhoria contínua;"

Resposta correta.

33. (CESPE – PG/DF– Analista de Sistemas– 2021)

A referida norma determina que, durante o planejamento do sistema de gestão de segurança da informação, sejam tomadas as medidas de prevenção e redução de efeitos indesejados dos riscos relacionados ao escopo de gestão dos serviços de tecnologia da informação.

Comentários:

Segundo a norma ISO 27001 no item 6. Planejamento

"A organização deve planejar:

a) ações para considerar estes riscos e oportunidades; e

b) como

1) integrar e implementar estas ações dentro dos processos do seu sistema de gestão da segurança da informação; e

2) avaliar a eficácia destas ações."

Perceba que apenas existe o planejamento de como fazer a implementação destas medidas, mas não há a implementação destas.

Resposta errada.

34.(CESPE – PG/DF– Analista de Sistemas– 2021)

Uma organização deve prever auditorias internas sobre o seu sistema de gestão de segurança da informação, em intervalos planejados, para verificar a conformidade com os requisitos da norma.

Comentários:

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

Resposta correta.

35. (VUNESP – EBSERH– Analista de Tecnologia da Informação– 2020)

A norma ISO 27001 estabelece a seguinte definição: uso sistemático de informações para identificar fontes e estimar o risco. Essa definição corresponde à

a) gestão dos riscos.

b) análise de riscos.

c) criptografia dos riscos.

d) diminuição de riscos.

e) interação com os riscos.

Comentários:

Segundo a Norma ISO 27001 a Análise de risco é o uso sistemático de informações para identificar fontes e estimar o risco.

Resposta correta, alternativa b).

36.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Na implementação do plano de tratamento de riscos, a inclusão de atribuição de papéis e responsabilidades deve ser evitada, pois aquele é um documento sucinto e confidencial.

Comentários:

No plano de tratamento de riscos é necessário que haja a inclusão de atribuição de papéis e responsabilidades.

Veja o que diz o controle A.6.1.1

"Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas."

Resposta errado.

37. (CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Para estabelecer o SGSI, no tocante à análise e à avaliação dos riscos, uma das ações que devem ser executadas consiste em avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando-se

em consideração as consequências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos.

Comentários:

A ISO 27001 tem como tríade da segurança a confidencialidade, integridade e disponibilidade; ao se analisar os riscos envolvidos deve-se ter em mente esses três requisitos, além de trazer luz as consequências relacionadas as falhas de segurança.

Resposta correta.

38.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

A política do SGSI, para os efeitos da norma em questão, não é considerada um documento importante da política de segurança da informação, pois estabelece apenas diretrizes.

Comentários:

A política do SGSI é um documento de extrema importância na ISO 27001.

Resposta errada.

39.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

A organização deve comunicar as ações e melhorias do SGSI a todas as partes interessadas, com um nível de detalhamento apropriado às circunstâncias, bem como deve assegurar-se de que as melhorias atinjam os objetivos pretendidos.

Comentários:

"A organização deve regularmente comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhamento apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder."

Resposta correta.

40.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Ao estabelecer o SGSI, a organização deve identificar os riscos e as ameaças; para isso, ela deverá identificar e registrar em documento os proprietários dos ativos dentro do escopo do SGSI, ou seja, as pessoas que têm o direito de propriedade sobre o ativo.

Comentários:

Nas informações adicionais do item 8.1.2 Proprietário do ativo temos:

"O proprietário identificado pode ser um indivíduo ou urna entidade que aprovou a responsabilidade pela gestão, para controlar todo o ciclo de vida de um ativo. O proprietário identificado não tem necessariamente quaisquer direitos de propriedade sobre o ativo."

Resposta errada.

Lista de Questões

1.(CESPE – DPE/RO – Analista da Defensoria Pública– 2022)

De acordo com a Norma NBR ISO/IEC n.º 27002, no gerenciamento da segurança em redes, tecnologias aplicadas como autenticação, encriptação e controles de conexões de rede são

a) serviços voltados à confidencialidade do tráfego de rede.

b) controles de segurança essenciais para a segregação de redes.

c) características típicas de um ambiente seguro de rede.

d) diretrizes para implementação de segurança de serviços de rede.

e) funcionalidades de segurança de serviços de rede.

2. (FCC – TJ/SC – Analista de Sistemas– 2021)

Considere:

Manter a confidencialidade da informação de autenticação secreta, garantindo que ela não seja divulgada para quaisquer outras partes, incluindo autoridades e lideranças.

De acordo com a Norma ABNT NBR ISO/IEC 27002:2013, essa recomendação é do âmbito de

a) gerenciamento de acesso do usuário.

b) responsabilidades dos usuários.

c) controle de acesso ao sistema e à aplicação.

d) controles criptográficos.

e) responsabilidades e procedimentos operacionais.

3. (FCC – TJ/SC – Analista de Sistemas– 2021)

De acordo com a Norma ABNT NBR ISO/IEC 27002:2013, no âmbito do Gerenciamento da segurança em redes, um método de controlar a segurança da informação em grandes redes é

a) definir que os administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

b) definir 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.

c) estabelecer e implementar regras definindo critérios para a instalação de software pelos usuários.

d) definir que as atualizações do software operacional, aplicativos e bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada.

e) dividir em diferentes domínios de redes que podem, por exemplo, ser escolhidos com base no nível de confiança.

4.(CESPE – SEFAZ/AL – Auditor Fiscal de Finanças e Controle– 2021)

Considere que, em uma organização, tenha sido realizada uma inspeção aleatória para detectar e coibir a retirada não autorizada de equipamentos e ativos, sem aviso prévio aos colaboradores. Nesse caso, de acordo com a NBR ISO/IEC 27002, é dispensável autorização prévia ou aviso aos colaboradores somente se os ativos armazenarem ou processarem informações sensíveis aos negócios da organização.

5. (CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

De acordo com a NBR ISO/IEC 27002, uma política para transferência de informações tem como objetivo a proteção da transferência de informações por meio de todos os tipos de recursos de comunicação.

6. (CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

Controles criptográficos como assinaturas digitais e códigos de autenticação de mensagens são aplicáveis para verificar a integridade de informações sensíveis ou críticas, armazenadas ou transmitidas.

7.(CESPE – SEFAZ/CE – Auditor Fiscal de Tecnologia da Informação da Receita Estadual– 2021)

No que se refere à NBR ISO/IEC 27002:2013 e a confiabilidade, integridade e disponibilidade, julgue o item a seguir. No contexto de política de segurança da informação no relacionamento com fornecedores, convém que sejam estabelecidos, quando necessário, acordos de contingência e recuperação para assegurar a disponibilidade da informação.

8. (CESPE – BANESE – Desenvolvimento– 2021)

Cabe ao provedor de serviço em nuvem disponibilizar informações sobre os países e a localização geográfica onde os dados serão armazenados, para que as entidades regulatórias e as jurisdições possam ser mapeadas pelo cliente.

9. (CESPE – BANESE – Desenvolvimento– 2021)

Implementando-se um conjunto adequado de controles, de forma coordenada e coerente com os riscos associados a uma visão holística da organização, alcança-se a segurança da informação.

10.(CESPE – BANESE – Desenvolvimento– 2021)

Soluciona-se a vulnerabilidade de um sistema de criptografia simétrica por meio da utilização de chaves diferentes para cifrar e decifrar mensagens.

11. (CESPE – PG/DF – Analista de Sistema– 2021)

O fornecimento de evidências formais da aplicação de testes suficientes por empresa de desenvolvimento de sistemas terceirizado contra a presença de vulnerabilidades conhecidas em sistemas novos ou em processo de manutenção é uma diretriz para implementação do controle relacionado à supervisão e ao monitoramento de atividades de desenvolvimento terceirizado pela organização.

12.(CESPE – MPE/AP – Tecnologia da Informação– 2021)

De acordo com a NBR ISO/IEC 27002, quando do desenvolvimento de uma política sobre o uso de controles criptográficos, convém considerar

a) a identificação do nível requerido de proteção com base na avaliação de risco, considerando-se o tipo, a força e a qualidade do algoritmo de criptografia.

b) a realização de cópias de segurança ou arquivamento das chaves criptográficas.

c) a manutenção de registro e auditoria das atividades relacionadas ao gerenciamento de chaves.

d) a implementação de um firewall com vistas à melhora do algoritmo de criptografia.

e) a manutenção de um registro de auditoria de todos os acessos a código-fonte de programas.

13. (SELECON – EMGEPRON – Analista Técnico – 2021)

Entre as Normas da ISO/IEC 27000, a ISO 27002 trata da adoção das práticas, imprescindíveis para blindar a empresa contra ataques cibernéticos e demais ameaças. Duas dessas práticas são descritas a seguir.

I. É indispensável realizar a definição dos procedimentos e das responsabilidades da gestão e a operação de todos os recursos ligados ao processamento das informações. Para isso, é preciso gerenciar os serviços terceirizados, o planejamento dos recursos dos sistemas para reduzir riscos de falhas, a criação de processos para gerar cópias de segurança, a recuperação e a administração segura das redes de comunicação.

II. Antes de contratar funcionários ou fornecedores, é preciso fazer uma análise cuidadosa, principalmente se forem ter acesso a informações sigilosas. O objetivo dessa atitude é eliminar o risco de roubo, mau uso ou fraude dos recursos. Uma vez atuando na organização, o funcionário deve ser conscientizado sobre as ameaças que expõem a segurança da informação, bem como sobre as suas obrigações e responsabilidades.

As práticas descritas em I / II são denominadas, respectivamente:

a) Gerenciamento de operações e comunicações/ Segurança física e do ambiente

b) Gerenciamento de operações e comunicações/ Segurança em Recursos Humanos

c) Gestão de incidentes de segurança da informação/ Segurança física e do ambiente

d) Gestão de incidentes de segurança da informação/ Segurança em Recursos Humanos

14.(CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

De acordo com a NBR ISO/IEC 27002, a política de senhas da organização deve permitir o envio de senhas de acesso em texto claro, por correio eletrônico, quando se tratar de senhas temporárias com prazo de validade definido.

15. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

Conforme prescreve a NBR ISO/IEC 27002 a respeito do controle de acesso ao código-fonte de programas, para que se reduza o risco de corrupção de programas de computador na organização, convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte.

16. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

De acordo com a NBR ISO/IEC 27002, as ferramentas de gerenciamento de informações de autenticação aumentam a eficácia desse controle e reduzem o impacto de uma eventual revelação de informação de autenticação secreta.

17. (CESPE– SERPRO – Desenvolvimento de Sistemas– 2021)

A contratação de seguros contra sinistros digitais é uma medida de transferência de riscos relacionados a possíveis impactos potencialmente causados por vulnerabilidades e ameaças à segurança da informação organizacional.

18.(CESPE– Ministério da Economia – Tecnologia da Informação – 2020)

No que diz respeito a controle de entrada física, a norma ISO/IEC 27002:2013 recomenda que o acesso às áreas onde são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado, mediante a implementação de controles de acesso apropriados, que podem ser, por exemplo, mecanismos de autenticação de dois fatores, tais como cartões de controle de acesso e PIN (personal identification number).

19.(AOCP– MJSP– Analista de Governança de Dados– 2020)

O valor de um Ativo pode ser considerado uma vulnerabilidade relacionada a qual tópico previsto na ISO 27002?

a) Contratação.

b) Perímetro de segurança.

c) Retirada de direito de acesso.

d) Segurança em escritórios, salas e instalações.

e) Segurança de equipamentos.

20. (AOCP– MJSP– Analista de Governança de Dados– 2020)

Em uma situação na qual é necessário o acesso externo a informações, assinale a alternativa que apresenta uma recomendação da ISO 27002.

a) Limitar o acesso às informações antes da implantação dos controles apropriados.

b) Garantir o acesso às informações para avaliação das vulnerabilidades posteriores.

c) Permitir o acesso às informações dentro de um ambiente de testes.

d) Bloquear totalmente o acesso às informações antes da implantação dos controles apropriados.

e) Impor normas de acesso independentemente das particularidades de cada agente externo.

21.(AOCP– MJSP– Analista de Governança de Dados– 2020)

Pedro está aplicando a norma ISO 27002 em sua organização. De acordo com essa norma, qual vulnerabilidade Pedro deve estar ciente que pode surgir durante a autorização para recursos de processamento de informação?

a) Uso de notebook pessoal.

b) Sites maliciosos.

c) Ferramentas antivírus.

d) Aplicativos móveis.

e) Sistemas on-line.

22.(FCC – AL/AP– Desenvolvedor de Sistemas– 2020)

No que diz respeito à gestão de incidentes de segurança da informação, é recomendável que a organização defina como identificar, coletar, adquirir e preservar evidências, além de que procedimentos internos sejam desenvolvidos e seguidos para os propósitos de ação legal ou disciplinar, quando necessário. Segundo a norma ABNT NBR ISO/IEC 27002:2013, é recomendável que os procedimentos para registro, guarda e divulgação de evidência de incidentes levem em conta

a) a ficha criminal dos colaboradores da organização.

b) a classificação da ação disciplinar ou legal pelos incidentes ocorridos na organização.

c) o número de incidentes ocorridos em cada mês.

d) papéis e responsabilidades das pessoas envolvidas.

e) os custos envolvidos e o impacto em cada setor da organização.

23.(FCC – TRT/RS– Tecnologia da Informação – 2020)

Texto 4A04-I

Um hacker invadiu o sistema computacional de determinada instituição e acessou indevidamente informações pessoais dos colaboradores e servidores. Durante a ação, foram alterados os registros de logs do sistema operacional e das aplicações, a fim de dificultar o trabalho de auditoria. Após o ocorrido, identificaram-se as seguintes ações do hacker.

I Exploração, a partir da Internet, de uma vulnerabilidade da página de notícias do portal da instituição localizada no servidor web, o que permitiu o acesso não autorizado à rede interna.

II Utilização de um script para alteração dos registros dos logs, com a troca dos endereços IP reais por fictícios.

III Quebra das credenciais administrativas do servidor de banco de dados dos sistemas internos, a partir do servidor web e utilização da técnica de ataques de dicionário.

IV Acesso de forma não autorizada ao servidor de banco de dados dos sistemas internos, para efetuar a extração das informações pessoais de colaboradores e servidores.

A equipe incumbida de analisar o caso concluiu que o risco era conhecido e considerado alto, já tendo sido comunicado à alta gestão da instituição; a vulnerabilidade explorada e sua correção eram conhecidas havia mais de seis meses, bem como a inexistência de dependências e da troca de dados entre os servidores de web e banco de dados; o incidente poderia ter sido evitado com o uso eficaz dos controles de segurança da informação.

Com base na NBR ISO/IEC n.º 27002, é correto afirmar que, no cenário apresentado no texto 4A04-I, foram explorados os controles de

a) manutenção de equipamentos e de segurança física, pela ineficiência das manutenções preventivas recomendadas e da proteção física dos servidores web e de banco de dados.

b) manutenção de equipamentos e de segregação de rede, pela ineficiência das manutenções preventivas recomendadas e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

c) segurança física e de segregação de rede, pela ineficiência da proteção física e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

d) gestão de vulnerabilidades técnicas e de segurança física, pela ineficiência do monitoramento e das correções das vulnerabilidades e da proteção física dos servidores web e de banco de dados.

e) gestão de vulnerabilidades técnicas e de segregação de rede, pela ineficiência do monitoramento e das correções das vulnerabilidades e da segmentação da rede em domínio filtrados por firewalls entre os servidores web e de banco de dados.

24.(FCC – TRT/RS– Tecnologia da Informação – 2022)

Para impedir perdas, danos, furtos ou roubos, ou comprometimento de ativos e interrupção das operações da organização, a norma ABNT NBR 27001:2013 recomenda que

a) os equipamentos sejam ligados diretamente em tomadas novas ou testadas por profissionais especializados e que a corrente elétrica seja 220 V.

b) os equipamentos devem ter uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.

c) equipamentos ou softwares podem ser retirados do local sem autorização prévia, desde que sob a vista de um funcionário da área de TI.

d) os equipamentos que contenham mídias de armazenamento de dados não precisam ser examinados antes da reutilização, uma vez que são ativos registrados da organização.

e) o cabeamento de energia e telecomunicações deve ser colocado no mesmo conduíte.

25.(CESPE – APEX Brasil– Tecnologia da Informação e Comunicação – 2022)

Conforme a NBR ISO/IEC 27001, as organizações devem realizar avaliações de risco de segurança da informação a) em intervalos planejados ou quando mudanças significativas são propostas para ocorrer.

b) mensalmente.

c) semestralmente.

d) anualmente.

26.(CESPE – SEFAZ/AL– Auditor Fiscal– 2021)

Segundo a referida norma, um incidente de segurança da informação é uma ocorrência identificada de um estado de sistema, serviço ou rede, que indica uma possível falha no sistema de gestão da informação.

27.(CESPE – SEFAZ/AL– Auditor Fiscal– 2021)

A NBR ISO/IEC 27001 prescreve que, por medida de segurança, as informações documentadas como evidências de monitoramento, de auditoria e de análises críticas da segurança da informação sejam descartadas imediatamente após serem apresentadas aos gestores principais da organização.

28. (IBFC– Prefeitura de São Gonçalo do Amarante/ RN – Analista de Sistema – 2021)

De acordo com a norma ISO 27001, a classificação de uma informação possui um processo de quatro etapas. A este respeito, assinale a alternativa correta.

a) Inventário de Ativos, Classificação da Informação, Rotulagem da Informação e Manuseio da informação

b) Análise de Conteúdo da Informação, Varredura de Vírus, Rotulagem da informação e Manuseio da informação

c) Classificação da Informação, Eliminação de Riscos para os documentos alterados, Inventário de Ativos e Manuseio da informação

d) Classificação da Informação, Armazenamento da Informação, Varredura de Vírus e Análise de Conteúdo da Informação

29.(FGV – IMBEL– Supervisor TI– 2021)

A Associação Brasileira de Normas Técnicas, ABNT, é responsável pela elaboração das Normas Brasileiras como, por exemplo, a ABNT NBR ISO/IEC 27001:2013, sobre aspectos da Segurança da Informação.

Dado que a sigla ISO deriva de International Organization for Standardization, assinale a correta natureza das normas NBR ISO.

a) São normas brasileiras que passam a ser adotadas pela ISO.

b) São normas definidas em conjunto com a ISO.

c) São traduções de normas da ISO que passam a ser adotadas pela ABNT.

d) São normas da ISO adaptadas pela ABNT às práticas brasileiras.

e) São normas brasileiras compiladas a partir da combinação de outras normas da ISO.

30.(CESPE – PG/DF– Analista de Sistemas– 2021)

Conscientização, educação e treinamento em segurança da informação são previstos na norma como segurança em recursos humanos durante a contratação.

31. (CESPE – PG/DF– Analista de Sistemas– 2021)

A manutenção de contatos apropriados com autoridades relevantes relaciona-se com a organização da segurança da informação na medida em que reduz o uso indevido de ativos da entidade.

32.(CESPE – PG/DF– Analista de Sistemas– 2021)

Ao analisar criticamente o sistema de gestão de segurança da informação (SGSI) da organização, a alta direção deve incluir oportunidades de melhoria nesse sistema.

33. (CESPE – PG/DF– Analista de Sistemas– 2021)

A referida norma determina que, durante o planejamento do sistema de gestão de segurança da informação, sejam tomadas as medidas de prevenção e redução de efeitos indesejados dos riscos relacionados ao escopo de gestão dos serviços de tecnologia da informação.

34.(CESPE – PG/DF– Analista de Sistemas– 2021)

Uma organização deve prever auditorias internas sobre o seu sistema de gestão de segurança da informação, em intervalos planejados, para verificar a conformidade com os requisitos da norma.

35. (VUNESP – EBSERH– Analista de Tecnologia da Informação– 2020)

A norma ISO 27001 estabelece a seguinte definição: uso sistemático de informações para identificar fontes e estimar o risco. Essa definição corresponde à

a) gestão dos riscos.

b) análise de riscos.

c) criptografia dos riscos.

d) diminuição de riscos.

e) interação com os riscos.

36.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Na implementação do plano de tratamento de riscos, a inclusão de atribuição de papéis e responsabilidades deve ser evitada, pois aquele é um documento sucinto e confidencial.

37. (CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Para estabelecer o SGSI, no tocante à análise e à avaliação dos riscos, uma das ações que devem ser executadas consiste em avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando-se em consideração as consequências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos.

38.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

A política do SGSI, para os efeitos da norma em questão, não é considerada um documento importante da política de segurança da informação, pois estabelece apenas diretrizes.

39.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

A organização deve comunicar as ações e melhorias do SGSI a todas as partes interessadas, com um nível de detalhamento apropriado às circunstâncias, bem como deve assegurar-se de que as melhorias atinjam os objetivos pretendidos.

40.(CESPE – Ministério da Economia– Gestão de Projetos – 2020)

Ao estabelecer o SGSI, a organização deve identificar os riscos e as ameaças; para isso, ela deverá identificar e registrar em documento os proprietários dos ativos dentro do escopo do SGSI, ou seja, as pessoas que têm o direito de propriedade sobre o ativo.

Resumo direcionado

ISO 27002

SEÇÃO	OBJETIVOS DE CONTROLE	CONTROLES
Políticas de Segurança da Informação	Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes	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 envolvidas
		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

Orientação da Direção para Segurança da Informação	Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização	Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas
		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
		Convém que contatos apropriados com as autoridades relevantes sejam mantidos
		Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos
		Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto
	Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis	Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis
		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

Segurança em Recursos Humanos	Antes da contratação - Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papeis para os quais eles foram selecionados	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

		Convém que as obrigações contratuais com funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando, dentre outros: Termo de confidencialidade ou de não divulgação, para funcionários, fornecedores e partes externas;e Responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização;
	Durante a contratação - Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação	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
		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 suas funções
		Convém que exista um processo disciplinar formal, implantado e comunicado, para tornar ações contra funcionários que tenham cometido uma violação de segurança da informação
	Encerramento e mudança da contratação – Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação	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

Gestão de ativos		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

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

		Convém que os ativos mantidos no inventário tenham um proprietário
		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
		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
	Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização	Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada
		Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização
		Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização

	Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias	Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização
		Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais
		Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte

Controle de acesso	Limitar o acesso à informação e aos recursos de processamento da informação	Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios

	Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar
Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços	Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição dos direitos de acesso
	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 tipos de sistemas e serviços
	Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados
	Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal
	Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares
	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 ou acordos, ou ajustados após a mudança destas atividades
Tornar os usuários responsáveis pela proteção das suas informações de autenticação	Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta

	Prevenir o acesso não autorizado aos sistemas e aplicações	Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso
		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)
		Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade
		Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado
		Convém que o acesso ao código-fonte de programa seja restrito
Criptografia	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação	Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação
		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

Segurança Física e do Ambiente		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

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

		Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido
		Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações
		Convém que seja projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes
		Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras
		Convém que pontos de acesso, como áreas de entrega 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

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

		Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades
		Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos
		Convém que os equipamentos tenham uma manutenção correta para assegurar a sua contínua integridade e disponibilidade
		Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia
		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
		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
		Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada
		Convém que sejam adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de

		tela limpa para os recursos de processamento da informação

Segurança nas Operações		Convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles
	Garantir a operação segura e correta dos recursos de processamento da informação	

	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
	Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema
	Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção
Assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware	Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra *malware*, combinados com um adequado programa de conscientização do usuário
Proteger contra a perda de dados	Convém que cópias de segurança das informações, dos software e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida

Registrar eventos e gerar evidências	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
	Convém que as informações dos registros de eventos (log) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração
	Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares
	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
Assegurar a integridade dos sistemas operacionais	Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados
Prevenir a exploração de vulnerabilidades técnicas	Convém que 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 lidar com os riscos associados
	Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários

	Minimizar o impacto das atividades de auditoria nos sistemas operacionais	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

Segurança nas Comunicações	Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam	Convém que as redes sejam gerenciadas e controladas para proteger as ¡informações nos sistemas e aplicações
		Convém que mecanismos de segurança, níveis de serviço 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
		Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes
	Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas	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
		Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e as partes externas
		Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas
		Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados

Aquisição, Desenvolvimento e Manutenção de Sistemas		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
	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 serviços sobre as redes públicas	

		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
		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

	Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação	Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização

		Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças
		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
		Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas
		Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação
		Convém que as organizações estabeleçam e protejam adequadamente ambientes seguras de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema
		Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado
		Convém que os testes das funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas

		Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões
	Assegurar a proteção dos dados usados para teste	Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados

Relacionamento na Cadeia de Suprimento	Garantir a proteção dos ativos da organização que são acessados pelos fornecedores	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 e documentados
		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
		Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados à cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação
	Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com os fornecedores	Convém que as organizações monitorem, analisem criticamente e auditem, a intervalos regulares, a entrega dos serviços executados pelos fornecedores
		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 de riscos

Gestão de Incidentes de segurança da informação	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação	Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação
		Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível
		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
		Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação
		Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados
		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
		Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências

Aspectos da segurança da informação na Gestão da continuidade do Negócio	Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização	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
		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
		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
		Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade

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

		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 software proprietários
		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
		Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável
		Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes

	Assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização	Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas
		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
		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