ISO/IEC 27002
CÓDIGO DE PRÁTICAS PARA CONTROLES DE SEGURANÇA DA INFORMAÇÃO

PROF. LUIS CLAUDIO, M.SC., PMP®
WWW.PROVASDETI.COM.BR

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

De onde Vieram estas Normas?

Como vai a Família?

ISO/IEC 27000:2014

Information security management systems

Overview and vocabulary

*This International Standard provides the **overview** of information security management systems, and **terms and definitions** commonly used in the ISMS family of standards.*

*This International Standard is applicable to **all types and sizes of organization** (e.g. commercial enterprises, government agencies, not-for-profit organizations).*

Como vai a Família?

ISO/IEC 27001:2013

Information security management systems

Requirements

*This International Standard specifies the **requirements** for **establishing**, **implementing**, **maintaining** and **continually improving** an ISMS within the context of the organization.*

*This International Standard **also** includes **requirements** for the **assessment** and **treatment** of information security risks tailored to the needs of the organization.*

*Excluding any of the requirements specified in **Clauses 4 to 10** is not acceptable when an organization claims conformity to this International Standard.*

Como vai a Família?

ISO/IEC 27002:2013

Code of practice for information security controls

This International Standard gives **guidelines** for organizational information security standards and information security management practices including the **selection**, **implementation** and **management** of **controls** taking into consideration the organization's information security risk environment(s).

Como vai a Família?

ISO/IEC 27003:2010

Information security management system implementation guidance

This International Standard focuses on the **critical** aspects needed for **successful** design and implementation of an ISMS in accordance with ISO/IEC 27001:2005.

It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of **obtaining management approval** to implement an ISMS, defines a **project** to implement an ISMS, and provides guidance on how to plan the ISMS project, resulting in a final ISMS **project implementation plan**.

Como vai a Família?

ISO/IEC 27004:2009

Information security management

Measurement

This International Standard provides guidance on the development and use of **measures** and **measurement** in order to assess the **effectiveness** of an implemented ISMS and controls or groups of controls, as specified in ISO/IEC 27001.

Como vai a Família?

ISO/IEC 27005:2011

Information security risk management

This International Standard provides guidelines for information security **risk** management.

Knowledge of the concepts, models, processes and terminologies described in **ISO/IEC 27001** and **ISO/IEC 27002** is important for a complete understanding of this International Standard.

Seção 0 – Introdução

0.1 Contexto e histórico

Esta Norma é projetada para as organizações usarem como uma referência na **seleção de controles** dentro do processo de implementação de um SGSI, baseado na ISO/IEC 27001 **OU** ... como um documento de orientação para as organizações implementarem controles de SI comumente aceitos.

Seção 0 – Introdução

0.1 Contexto e histórico

A segurança da informação é alcançada pela implementação de um conjunto adequado de **controles** (políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*).

Um SGSI considera uma visão **holística** e coordenada dos riscos de SI da organização, para implementar um conjunto de controles detalhado, com base na estrutura global de um sistema de gestão coerente.

Seção 0 – Introdução

0.1 Contexto e histórico

Um sistema de gestão da segurança da informação bem sucedido requer apoio de todos os funcionários da organização.

Isto pode também exigir a participação de **acionistas**, **fornecedores** ou **outras partes externas**. Orientações de **especialistas externos** podem também ser necessárias.

Seção 0 – Introdução

0.2 Requisitos

Existem três fontes principais de requisitos de SI:

- Gerados pela avaliação de riscos.
- Legislação, estatutos, regulamentação e contratos.
- Princípios, objetivos e requisitos do negócio.

Os recursos empregados na implementação dos controles precisam ser **balanceados** com base na probabilidade de danos ao negócio... A ABNT NBR ISO/IEC 27005 fornece diretrizes...

Seção 0 – Introdução

0.3 Seleção de controle

Controles podem ser selecionados da norma ou de **outros** conjuntos de controles, ou **novos** controles podem ser projetados, conforme apropriado.

Alguns dos controles podem ser considerados como **princípios básicos** para a gestão da segurança da informação e podem ser aplicados na **maioria das organizações**.

Seção 0 – Introdução

0.4 Desenvolvendo suas próprias diretrizes

A Norma é considerada como um **ponto de partida**. Nem todos os controles e diretrizes contidos neste código de prática **podem ser aplicados**.

Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma **referência cruzada** com as seções desta Norma, onde aplicável, para **facilitar a verificação da conformidade por auditores e parceiros de negócio**.

Seção 0 – Introdução

0.5 Considerações sobre o ciclo de vida

A informação tem um **ciclo de vida** natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até sua eventual destruição/obsolescência.

O **valor** e os **riscos** aos ativos podem **variar** durante o tempo de vida da informação... [], porém a SI permanece importante... em de todos os estágios.

Seção 0 – Introdução

0.5 Considerações sobre o ciclo de vida

Sistemas de informação têm ciclos nos quais eles são **concebidos**, **especificados**, **projetados**, **desenvolvidos**, **testados**, **implementados**, **usados**, **mantidos** e, eventualmente, **retirados do serviço** e **descartados**.

Convém que a segurança da informação seja considerada em cada estágio.

Seção 1 – Escopo

Fornece diretrizes para práticas de gestão de SI e normas de SI para as organizações selecionarem, implementarem e gerenciarem controles, levando em consideração os ambientes de risco da organização.

- Selecionar controles no processo de implementação de um SGSI baseado na ABNT NBR ISO/IEC 27001.
- Implementar controles de SI comumente aceitos.
- Desenvolver seus próprios princípios de gestão da SI.

Seção 2 – Referências normativas

O documento referenciado a seguir é indispensável à aplicação desta norma. Para referências datadas, aplicam-se somente as edições citadas.

Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas). ISO/IEC 27000*, Information technology – Security techniques – Information security management systems - Overview and vocabulary*

Seção 3 – Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO IEC 27000:

Seção 4 – Estrutura desta Norma

A Norma contém:

- 14 Seções (seções 5 a 18 da norma).
- 35 Objetivos de Controle.
- 114 Controles.

Obs.: A norma foi melhor organizada. Além disso, no aspecto quantitativo, no passado eram **11 seções**, **133 controle** e **39 objetivos de controle.**

Seção 4 – Estrutura desta Norma

Seção	Objetivo	Controle
5 - Políticas de segurança da informação	1	2
6 - Organização da segurança da informação	2	7
7 - Segurança de recursos humanos	3	6
8 - Gestão de ativos	3	10
9 - Controle de acesso	4	14
10 - Criptografia	1	2
11 - Segurança física e do ambiente	2	15
12 - Segurança nas operações	7	14
13 - Segurança nas comunicações	2	7
14 - Aquisição, dev. e manutenção de sistemas	3	13
15 - Relacionamento na cadeia de suprimento	2	5
16 - Gestão de incidentes de SI	1	7
17 - Aspectos da SI na gestão da continuidade	2	4
18 - Conformidade	2	8

Seção 4 – Estrutura desta Norma

4.1 Seções

Cada seção definindo os controles de SI contém um ou mais objetivos de controle. A **ordem** em que se encontram as seções **não implica** nem significa o seu grau de importância.

Convém que cada organização implemente esta Norma identificando quais controles são aplicáveis, quão importantes eles são e qual a aplicação para os processos individuais do negócio. Os controles não estão em ordem de prioridade.

Seção 4 – Estrutura desta Norma

4.2 Categorias de controles

Cada seção principal contém:

a) um objetivo de controle declarando o que se espera ser alcançado;

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

Seção 4 – Estrutura desta Norma

4.2 Categorias de controles

As descrições do controle são assim:

Controle

O texto do controle para atender ao objetivo de controle.

Diretrizes para implementação

Informações para apoiar a implementação do controle e alcançar o objetivo do controle. As diretrizes podem não ser totalmente adequada ou suficiente em todas as situações...

Informações adicionais

Dados que podem ser considerados, como por exemplo, questões legais e referências normativas. Nem sempre existem.

QUESTÕES

FGV/2015 - TCE-SE - Analista de TI - Segurança da Informação

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.

QUESTÕES

CS-UF/2015 - AL-GO - Analista Legislativo - Analista de Sistemas

A norma ISO/IEC 27002:2005 fornece um conjunto de diretrizes e princípios gerais para

a) avaliação da qualidade de pacotes de software em uma organização.

b) implementação da governança de TI em uma organização.

c) gestão de segurança da informação em uma organização.

d) certificação da maturidade.

QUESTÕES

ITNERANTE/2015

Com base na família de normas ISO/IEC 27000, julgue o item abaixo:

Alguns dos controles podem são considerados princípios básicos para a gestão da segurança da informação e, por isso, a norma ISO/IEC sugere que eles podem ser aplicados na maioria das organizações.

QUESTÕES

CESPE/2015 - MPOG - Analista em Tecnologia da Informação

Julgue o seguinte item, relativo à segurança da informação, com base no que dispõem as normas ISO/IEC 27002 e ISO/IEC 27001.

Quanto à abrangência, a norma ISO 27002 estabelece diretrizes e princípios gerais para gestão de segurança da informação incluindo a sua implantação, manutenção e melhoria.

QUESTÕES

FCC/2015 - TCE-CE - Técnico de Controle Externo-Auditoria de TI

A Norma NBR ISO/IEC 27002:2013 possui 14 sessões 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.

QUESTÕES - Gabarito

FGV/2015 - TCE-SE: Alternativa B
CS-UF/2015 - AL-GO: Alternativa C
ITNERANTE/2015: CORRETO
CESPE/2015 – MPOG: CORRETO
FCC/2015 - TCE-CE: Alternativa D

Seção 5 – Políticas

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Seção 5 – Políticas

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

- Definição e aprovação em alto nível.
- Requisitos vêm do negócio; de leis etc.; e do ambiente.
- Há diversas políticas: a “principal” e outras “específicas” de apoio (controle de acesso, classificação da informação, segurança física, uso de ativos, backup, transferência de informação etc.).
- A necessidade varia dependendo do nível de segregação de funções.
- Cuidados com as políticas divulgadas fora da organização.

Seção 5 – Políticas

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

- Cada política deve ter um gestor individual.
- Ela muda em resposta ao negócio, economia, legislação etc.
- Todas “devem” ser aprovadas pela alta direção após revisão.

Seção 6 – Organização da Segurança

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

A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.

Seção 6 – Organização da Segurança

6.1.1 - Responsabilidades e papéis pela segurança da informação - Convém que todas as responsabilidades pela SI sejam definidas e atribuídas.

- Responsabilidades pelo gerenciamento de riscos e, em particular, pela aceitação dos riscos residuais.
- Delegação da execução, mas não da responsabilidade.
- Competência e capacidade das pessoas com responsabilidades.
- Gestor global *versus* gestores individuais.

Seção 6 – Organização da Segurança

6.1.2 - Segregação de funções - 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.

- Dificuldade de segregar funções em pequenas organizações, mas o princípio deve ser aplicável, tão logo seja possível e praticável.
- Se não der, pelo menos, implementar monitoração de atividades, trilhas de auditoria e gerenciamento da supervisão.

Seção 6 – Organização da Segurança

6.1.3 - Contato com autoridades - Convém que contatos apropriados com autoridades relevantes sejam mantidos.

- A norma fala de corpo de bombeiros, autoridades fiscalizadoras, entidades regulatórias etc. que “devem” ser contatadas.
- Autoridades que tomem providências contra a origem dos ataques.
- A norma fala também de fornecedores de telecomunicações (rotas de linha e disponibilidade) e fornecedores de água (instalação de refrigeração para os equipamentos).

Seção 6 – Organização da Segurança

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

- Ampliação do conhecimento sobre as melhores práticas.
- Recebimento de alertas de vulnerabiliddes, aconselhamentos etc.
- Trocar informações sobre novas tecnologias.

Seção 6 – Organização da Segurança

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

- Aplica-se a qualquer projeto independentemente do seu propósito.
- Objetivo de “avaliar riscos” em todos os projetos.

Seção 6 – Organização da Segurança

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

A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
A.6.2.2	Teleworking	*Control* A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Seção 6 – Organização da Segurança

6.2.1 - Política para o uso de dispositivo móvel - Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.

- Dispositivos móveis em locais públicos, salas de reuniões etc.
- Dispositivos deixados em carros, outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião.
- Dispositivos móveis que contêm informações importantes, sensíveis e/ou críticas não podem ser deixados sem observação.
- Política de uso de dispositivos móveis.
- Separação do uso para fins de negócio e para fins pessoais.

Seção 6 – Organização da Segurança

6.2.2 - Trabalho remoto - Convém que uma política e medidas que apoiam a SI sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

- Política que defina as condições e restrições para o trabalho remoto.
- Segurança física existente no local do trabalho remoto.
- A segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização.
- Prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular.
- Cuidado com familiares e amigos.
- Evitar disputas relativas a propriedade intelectual.
- Revogação de autoridade e direitos de acesso ao final das atividades.

Seção 7 – Segurança de RH

Objetivo: Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados.

A.7.1.1	Screening	*Control* Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2	Terms and conditions of employment	*Control* The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

Seção 7 – Segurança de RH

7.1.1 - Seleção - 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.

- Referências, pelo menos, uma profissional e uma pessoal.
- Verificação independente da identidade (passaporte ou documento similar) e mais detalhadas (de crédito ou de registros criminais).
- Confirmação das qualificações (do currículo etc.).
- Processo de seleção também para fornecedores e partes externas.

Seção 7 – Segurança de RH

7.1.2 - Termos e condições de contratação - Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.

- Consolidar em um termo de confidencialidade e não divulgação.
- Responsabilidade com relação às leis de direitos autorais.
- Responsabilidades pelo tratamento da informação recebida de outras companhias ou partes interessadas.

Obs.: Tais responsabilidades podem continuar após o término da contratação, onde apropriado.

Seção 7 – Segurança de RH

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

A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
A.7.2.3	Disciplinary process	*Control* There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Seção 7 – Segurança de RH

7.2.1 - Responsabilidades da direção - 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.

- Assegurar que todos estão instruídos sobre as responsabilidades e papéis antes de obter acesso às informações sensíveis.
- Assegurar que todos estão motivados e que atinjam um nível de conscientização para cumprir os termos e condições e a política.
- Assegurar que haja um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de SI.
- A direção deve agir de forma exemplar.

Seção 7 – Segurança de RH

7.2.2 - Conscientização, educação e treinamento em segurança da informação - Convém que todos os funcionários da organização e, onde pertinente, partes externas “devem” receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

- Considerar atividades de conscientização como campanhas (dia da segurança da informação) e publicação de boletins, folhetos etc.
- Usar diferentes formas de treinamento (presencial, a distância, baseado em web, autodidata e outros).
- Focar não só no “o que” e no “como”, mas também no “porquê”.

Seção 7 – Segurança de RH

Neste controle há uma menção indireta ao que se pode considerar procedimento ou controle “básico” (seção 7.2.2-d):

> Convém que o treinamento e educação em segurança da informação também contemple aspectos gerais, como:
>
> ...
>
> d- procedimentos de segurança da informação básicos (tais como, notificação de incidente de segurança da informação) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa).
>
> ...

Seção 7 – Segurança de RH

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

- Verificação prévia de que a violação realmente ocorreu.
- A resposta deve ser feita de forma gradual.
- Incentivar e recompensar o comportamento desejável.

Seção 7 – Segurança de RH

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

A.7.3.1	Termination or change of employment responsibilities	*Control* Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

Seção 7 – Segurança de RH

7.3.1 - Responsabilidades pelo encerramento ou mudança 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 sejam cumpridas.

- Incluir na comunicação de encerramento de atividades requisitos de segurança da informação e responsabilidades legais apropriados.
- A função de RH é geralmente responsável pelo processo demissional e trabalha junto com o gestor da pessoa ao longo do desligamento.
- No caso de parte externa, este processo é feito pela parte externa de acordo com o contrato entre a organização e a parte externa.

Seção 8 – Ativos

Objetivo: Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos.

A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4	Return of assets	*Control* All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Seção 8 – Ativos

8.1.1 - Inventário dos ativos - Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.

- Considerar todo o ciclo de vida (criação, o processamento, o armazenamento, a transmissão, a exclusão e destruição).
- Todo ativo em inventário de SI deve ter um responsável.

Seção 8 – Ativos

8.1.2 - Proprietário dos ativos - Convém que os ativos mantidos no inventário tenham um proprietário.

- O proprietário identificado não é dono do ativo.
- Para sistemas complexos, pode ser útil definir grupos de ativos que atuem juntos para fornecer um serviço particular. Neste caso, o proprietário deste serviço é responsável pela entrega do serviço, incluindo a operação adequada de todos os ativos.

Seção 8 – Ativos

8.1.3 - Uso aceitável dos ativos - 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.

- Funcionários e partes externas “devem” estar conscientes dos requisitos de segurança da informação dos ativos da organização.
- Funcionários e partes externas “devem” ser responsáveis pelo uso de qualquer recurso de processamento da informação e tal uso seja realizado sob sua responsabilidade.

Seção 8 – Ativos

8.1.4 - Devolução de ativos - 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.

- O encerramento de atividades deve contemplar a devolução de equipamentos físicos e eletrônicos de propriedade da organização.
- No caso de compra de equipamento da organização ou uso de equipamento pessoal, procedimentos “devem” ser adotados para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento.

Seção 8 – Ativos

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

A.8.2.1	Classification of information	*Control* Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Seção 8 – Ativos

8.2.1 - Classificação da informação - 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 outros ativos além dos ativos de informação também sejam classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.
- A classificação deve considerar a análise ao longo do tempo.
- Classificação superestimada pode levar à implementação de controles desnecessários (e vice versa).

Seção 8 – Ativos

Na seção 8.2.1, a Norma sugere um exemplo de um esquema de classificação de confidencialidade da informação que poderia ser baseado em quatro níveis, quando sua divulgação:

a) não causa nenhum dano;

b) causa menor constrangimento ou inconveniência operacional;

c) tem pequeno impacto nas operações ou objetivos táticos;

d) tem sério impacto sobre os objetivos estratégicos, ou coloca a sobrevivência da organização em risco.

Seção 8 – Ativos

8.2.2 - Rótulos e tratamento da informação - 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.

- Definir a situação onde a rotulação é omitida, por exemplo, de informação não confidencial (cuja divulgação não causa dano).

Seção 8 – Ativos

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

- Restrições de acesso conforme cada nível de classificação.
- Manutenção de um registro formal dos destinatários de ativos.
- Identificação eficaz de todas as cópias das mídias, para chamar a atenção dos destinatários autorizados.

Seção 8 – Ativos

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

A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

Seção 8 – Ativos

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

- Destruição, quando não for mais necessário, do conteúdo de qualquer meio magnético reutilizável.
- Autorização para remoção de qualquer mídia da organização e manutenção do registro da remoção para fins de auditoria.
- Uso de criptografia para proteger os dados na mídia removível.
- Habilitação das unidades de mídia removível somente se necessário.

Seção 8 – Ativos

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

- Por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização.
- Destruição física de certos itens, se apropriado, ao invés de serem enviados para conserto ou descartados.

Seção 8 – Ativos

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

- Proteção contra fatores ambientais como exposição ao calor, umidade ou campos eletromagnéticos etc.
- Durante a transferência, registrar (logs) o conteúdo da mídia, a proteção aplicada e os tempos de trânsito.
- Vale para envio de mídia através do serviço postal ou correio.
- Neste controle, incluem-se mídias de documentos em papel.

QUESTÕES

FCC/2015 - TRT - 3ª Região (MG) - Analista Judiciário - TI

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.

QUESTÕES

FCC/2015 - TRT - 3ª Região (MG) - Analista Judiciário - TI

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

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.

QUESTÕES

CESPE/2015 - MPOG - Analista em TI - Cargo 12

Julgue o seguinte item, relativo à segurança da informação, com base no que dispõem as normas ISO/IEC 27002 e ISO/IEC 27001.

A norma ISO 27002 estabelece que seja designado um proprietário para todas as informações e os ativos associados com os recursos de processamento da informação.

QUESTÕES

CESPE/2014 - TJ-SE - Analista Judiciário - Suporte Técnico

Com base no disposto nas normas NBR ISO/IEC 27001 e 27002 e na ITIL (versão 3), julgue os itens seguintes.

O inventário de ativos refere-se a um controle incluído na interação com as partes externas à organização.

QUESTÕES

CESPE/2014 - TJ-SE - Analista Judiciário - Suporte Técnico

Com base no disposto nas normas NBR ISO/IEC 27001 e 27002 e na ITIL (versão 3), julgue os itens seguintes.

A política de segurança da informação, os objetivos e as atividades que refletem os objetivos do negócio são fatores críticos de sucesso na implementação da segurança da informação em uma organização.

QUESTÕES

MSGas/2015 – MSGás - Analista de Tecnologia da Informação

A norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização é a:

a) ABNT NBR ISO/IEC 27004:2010.

b) ABNT NBR ISO/IEC 27001:2013.

c) ABNT NBR ISO/IEC 27003:2011.

d) ABNT NBR ISO/IEC 27002:2013.

QUESTÕES

VUNESP/2014 - TJ-PA - Análise de Sistema - Desenvolvimento

Há uma seção da norma ISO 27002 que contém recomendações para que sejam cumpridas obrigações legais, estatutárias ou contratuais. A seção referida é

a) Gestão de Ativos

b) Gestão de Continuidade do Negócio

c) Conformidade.

d) Gestão de Incidentes de Segurança da Informação.

e) Segurança em Recursos Humanos

QUESTÕES

VUNESP/2014 - TJ-PA - Análise de Sistema - Suporte

As categorias da norma ISO 27002 que tratam de procedimentos importantes sobre a contratação e seleção de funcionários, fornecedores e terceiros fazem parte da seção

a) Controle de Acesso.

b) Conformidade

c) Gestão de Ativos.

d) Segurança em Recursos Humanos.

e) Segurança Física e do Ambiente.

QUESTÕES

QUADRIX/2014 – SERPRO - Administração de Serviços de TI

Segundo a norma ABNT NBR ISO/IEC 27002, trata-se de um controle considerado essencial:

a) documento da política de segurança.

b) atribuição de responsabilidades para a segurança.

c) direitos de propriedade intelectual.

d) gestão de vulnerabilidades técnicas.

e) gestão de incidentes de segurança.

QUESTÕES

TIMASTERS/2015

Com relação à ISO/IEC 27002, é incorreto:

a) O controle para seleção de RH deve ser aplicado tanto para funcionários, quanto para fornecedores e outras partes externas.

b) A norma sugere que o termo de confidencialidade trate até de obrigações que possam durar após o encerramento da contratação.

c) Convém que existam canais para relatar possíveis violações da política, preferencialmente, com identificação do autor da denúncia.

d) Para aumentar o nível de conscientização, o treinamento deve ter foco não somente no “o quê” e no “como”, mas também no “porquê”.

e) Convém que exista um processo disciplinar formal para tomar ações contra funcionários que cometam violações da política.

QUESTÕES - Gabarito

FCC/2015 - TRT: Alternativa B
CESPE/2015 – MPOG: ERRADO
CESPE/2014 - TJ-SE: ERRADO
CESPE/2014 - TJ-SE: CERTO
MSGas/2015 – MSGás: Alternativa B
VUNESP/2014 - TJ-PA: Alternativa C
VUNESP/2014 - TJ-PA: Alternativa D
QUADRIX/2014 – SERPRO: Alternativa C
TIMASTERS/2015: Alternativa C

Seção 9 – Acesso

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

A.9.1.1	Access control policy	*Control* An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

Seção 9 – Acesso

9.1.1 - Política de controle de acesso - Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de SI e dos negócios.

- Considerar legislação pertinente e qualquer obrigação contratual.
- Definir requisitos para autorização formal de pedidos de acesso, análise crítica periódica de direitos e remoção de direitos.
- Definir regras para o acesso privilegiado.

Obs.: “Tudo é proibido a menos que expressamente permitido.“

Obs.: Abordagem da necessidade “de conhecer” e “de usar”.

Seção 9 – Acesso

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

- Procedimentos para autorizar acesso a redes e a serviços de redes.
- Controles para proteger o acesso a conexões e a serviços de redes.
- Requisitos de autenticação do usuário para acessar serviços de rede e monitoramento do uso dos serviços de rede.

Seção 9 – Acesso

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

A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provision-ing	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privi-leged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication infor-mation of users	*Control* The allocation of secret authentication information shall be con-trolled through a formal management process.

Seção 9 – Acesso

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

A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Seção 9 – Acesso

9.2.1 - Registro e cancelamento de usuário - Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição de direitos de acesso.

- Uso de ID de usuário único para permitir responsabilização.

ATENÇÃO: O uso compartilhado de ID de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e convém que seja aprovado e documentado.

- Envolve atribuir, permitir ou revogar um ID de um usuário e fornecer ou revogar os direitos de acesso para este usuário de ID.

Seção 9 – Acesso

9.2.2 - Provisionamento para acesso de usuário - 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.

- Verificação de que o nível de acesso é apropriado às políticas de acesso e é consistente com outros requisitos.
- Garantia de que os direitos de acesso não estão ativados (por provedores de serviço) antes que o procedimento esteja completo.
- Convém que consideração seja dada para incluir cláusulas nos contratos (de pessoas e de serviços), que especifiquem sanções no caso de tentativa de acesso não autorizado.

Seção 9 – Acesso

9.2.3 - Gerenciamento de direitos de acesso privilegiados - Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.

- Direitos de acesso privilegiados sejam atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio.
- As atividades normais do negócio não sejam desempenhadas usando contas privilegiadas.
- Para o ID de usuário de administrador genérico, a confidencialidade da informação de autenticação secreta seja mantida quando for compartilhada.

Seção 9 – Acesso

9.2.4 - Gerenciamento da informação de autenticação secreta de usuários - Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

- Assinatura de uma declaração, para manter a confidencialidade da informação de autenticação secreta e manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo.
- Fornecer informação de autenticação secreta temporárias aos usuários de maneira segura (evitar e-mail desprotegido).
- Usar informação de autenticação secreta temporária única.

Obs.: Senhas são usadas como um tipo de informação de autenticação secreta (além disso, há chaves criptográficas, tokens etc.)

Seção 9 – Acesso

9.2.5 - Análise crítica dos direitos de acesso de usuário - Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

- Revisar os direitos de acesso de usuários em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou encerramento do contrato.
- Revisar autorizações para direitos de acesso privilegiado especial em intervalos mais frequentes.

Seção 9 – Acesso

9.2.6 - Retirada ou ajuste de direitos de acesso - 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.

- Alterar senhas de contas que permanecem ativas e que sejam do conhecimento do funcionário ou parte externa que está saindo.
- Avisar aos outros funcionários, fornecedores e terceiros envolvidos para não mais compartilhar informações com a pessoa.

Obs.: Pessoas descontentes podem deliberadamente corromper a informação, sabotar os recursos de processamento da informação ou tentar coletar informações para uso futuro.

Seção 9 – Acesso

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

A.9.3.1	Use of secret authentication information	*Control* Users shall be required to follow the organization's practices in the use of secret authentication information.

Seção 9 – Acesso

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

- Evitar manter anotadas a informação de autenticação secreta, a menos que elas possam ser armazenadas de forma segura.
- Usar tamanho mínimo de senha e evitar senhas baseadas em nomes, números de telefone e datas de aniversário, palavras inclusas no dicionário, caracteres consecutivos etc.
- Evitar utilizar a mesma informação de autenticação secreta para uso com finalidades profissionais e pessoais.

Seção 9 – Acesso

Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.

A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5	Access control to program source code	*Control* Access to program source code shall be restricted.

Seção 9 – Acesso

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

- Usar menus para controlar o acesso às funções dos sistemas.
- Controlar quais dados podem ser acessados por um usuário e os direitos de acesso, como ler, escrever, excluir e executar.
- Prover controles de acesso lógico ou fisico para o isolamento de aplicações sensíveis, dados de aplicação ou sistemas.

Seção 9 – Acesso

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

- Procedimento para entrada no sistema operacional seja configurado para minimizar a oportunidade de acessos não autorizados.
- Procedimento de entrada (log-on) revele o mínimo de informações.
- Mostre aviso geral informando que o computador seja acessado somente por usuários autorizados.
- Valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos.
- Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correto ou incorreto.

Seção 9 – Acesso

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

- Proteja contra tentativas forçadas de entrada no sistema (log-on) e registre todas as tentativas de acesso.
- Registre data e hora da última entrada (log-on) ou detalhes de qualquer tentativa sem sucesso de entrada (log-on).
- Não transmita senhas em texto claro pela rede.
- Encerre sessões inativas após um período, especialmente em locais de alto risco (locais públicos, àreas externas ou dispositivos móveis).
- Restrinja os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e reduzir a janela de oportunidade.

Seção 9 – Acesso

9.4.3 - Sistema de gerenciamento de senha - Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

- Permita que os usuários modifiquem suas próprias senhas, mas obrigue a escolha de senhas de qualidade.
- Obrigue a mudarem senhas temporárias no primeiro acesso e force as mudanças de senha a intervalos regulares.
- Mantenha registro das senhas anteriores e impeça a reutilização.
- Armazene e transmita as senhas de forma protegida.

Seção 9 – Acesso

9.4.4 - Uso de programas utilitários privilegiados - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.

- Segregação de programas utilitários dos softwares de aplicação.
- Limitação do uso de programas utilitários a um número mínimo de usuários confiáveis e autorizados.
- Remoção ou desabilitação dos programas utilitários desnecessários.

Seção 9 – Acesso

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

- Convém que seja evitado manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais.
- Convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte.
- Convém que seja mantido um registro de auditoria de todos os acessos a código-fonte de programas.

Obs.: Se o código do programa-fonte pretende ser publicado, controles adicionais para ajudar a garantir a sua integridade (por exemplo, assinatura digital) “devem” ser considerados.

Seção 10 – Criptografia

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

A.10.1.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	*Control* A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

Seção 10 – Criptografia

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

- Nível requerido de proteção com base em avaliação de risco, considerando tipo, força e a qualidade do algoritmo requerido.
- Proteção de informações sensíveis transportadas em dispositivos móveis, mídias removiveis ou através de linhas de comunicação.
- Considerar as leis ou regulamentações e restrições aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo.

Seção 10 – Criptografia

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

- Gerar chaves e certificados para diferentes sistemas e aplicações, distribuir para usuários, armazenar, mudar ou atualizar chaves etc.
- Lidar com chaves comprometidas, revogar chaves, recuperar chaves perdidas ou corrompidas, realizar cópias de segurança, guardar as chaves, destruir chaves etc.
- Manter registro e auditoria das atividades relacionadas com o gerenciamento de chaves.

Obs.: ISO/IEC 11770 para informação adicional sobre o tema.

Seção 11 – Segurança Física

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

A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.

Seção 11 – Segurança Física

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

A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5	Working in secure areas	*Control* Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Seção 11 – Segurança Física

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

- Instalações de processamento da informação fisicamente sólidas.
- Existência de área de recepção e sistemas de detecção de intrusos.
- Instalações de processamento gerenciadas pela organização fisicamente separadas das gerenciadas por partes externas.

Seção 11 – Segurança Física

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

- Registrar data e hora da entrada e saída de visitantes.
- Armazenar de forma segura em meio eletrônico ou livro de registro físico dados de acesso para fins de auditoria.
- Exigir de todos os funcionários, fornecedores e partes externas, e de todos os visitantes, alguma forma visível de identificação.

Seção 11 – Segurança Física

11.1.3 - Segurança em escritórios, salas e instalações - Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

- Edifícios discretos com a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício.
- Projetos que evitem que as informações confidenciais ou as atividades sejam visíveis e possam ser ouvidas da parte externa, inclusive, com proteção eletromagnética conforme apropriado.
- Listas de funcionários e guias telefônicos internos, que identifiquem a localização das instalações que processam informações sensíveis, não fiquem facilmente acessíveis a qualquer pessoal não autorizado.

Seção 11 – Segurança Física

11.1.4 - Proteção contra ameaças externas e do meio-ambiente - Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.

- Convém que orientações de especialistas sejam obtidas sobre como evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.

Seção 11 – Segurança Física

11.1.5 - Trabalhando em áreas seguras - Convém que seja projetado e aplicado procedimentos para o trabalho em áreas seguras.

- Divulgar a existência de áreas seguras ou as atividades nelas realizadas, apenas se for necessário.
- Supervisionar o trabalho em áreas seguras.
- Trancar áreas seguras, não ocupadas, e verificar periodicamente.
- Proibir uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

Obs.: As normas para o trabalho em áreas seguras “devem” incluir o controle dos funcionários, fornecedores e partes externas que trabalham em tais áreas, em todas as suas atividades.

Seção 11 – Segurança Física

11.1.6 - Áreas de entrega e de carregamento - Convém que pontos de acesso, tais 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.

- Áreas de entrega e carregamento sejam projetadas para permitir carregar e descarregar sem que se tenha acesso a outras áreas.
- Inspecionar a presença de explosivos, materiais químicos ou outros materiais perigosos, antes de serem transportados da área de entrega e carregamento para o local de utilização.
- Registrar ativos antes do carregamento para o local de utilização.
- Segregar remessas que entram das remessas que saem da empresa.

Seção 11 – Segurança Física

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

A.11.2.1	Equipment siting and protection	*Control* Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.

Seção 11 – Segurança Física

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

A.11.2.5	Removal of assets	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.7	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Seção 11 – Segurança Física

11.2.1 - Escolha do local e proteção do equipamento - Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.

- Hospedar equipamentos sensíveis em “data centers”.
- Minimizar o risco de ameaças como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferência elétrica e nas comunicações, radiação eletromagnética e vandalismo.
- Proibir comer, beber e fumar nas proximidades das instalações.

Seção 11 – Segurança Física

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

- Conformidade com as especificações do fabricante.
- Capacidade para atender ao crescimento do negócio.
- Alarmes para detectar mau funcionamento.
- Múltiplas alimentações com rotas físicas diferentes.
- Iluminação e comunicação de emergência.

Obs: As chaves de emergência (switches) e válvulas para o corte de energia, água, gás ou outras utilidades, sejam localizadas próximo das saídas de emergência ou salas de equipamentos.

Seção 11 – Segurança Física

11.2.3 - Segurança do cabeamento - 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.

- Usar linhas de energia e de telecomunicações subterrâneas (ou abaixo do piso) sempre que possível.
- Cabos de energia segregados dos cabos de comunicações.
- Para cabeamento sensível ou crítico, instalar conduítes blindados e salas ou caixas trancadas, utilizar blindagem eletromagnética, realizar varreduras técnicas e inspeções físicas.

Seção 11 – Segurança Física

11.2.4 - Manutenção dos equipamentos - Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.

- Manutenção dos equipamentos de acordo com as especificações.
- Registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas.
- Na época da manutenção, dependendo da manutenção ser realizada pelo pessoal local ou por pessoal externo à organização, informações sensíveis sejam eliminadas do equipamento.
- Exigências de manutenção estabelecidas nas apólices de seguro.

Seção 11 – Segurança Física

11.2.5 - Remoção de ativos - Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

- Identificar funcionários, fornecedores e partes externas que tenham autoridade para permitir a remoção de ativos para fora do local.
- Estabelecer limites de tempo para a retirada do local.
- Registrar a retirada e a devolução de ativos.
- Ducumentar a identidade, atribuição e função de qualquer pessoa que manuseia ou utiliza os ativos.

Obs.: Podem ser feitas inspeções aleatórias para detectar a retirada não autorizada de ativos e a existência de equipamentos de gravação não autorizados etc., e impedir sua entrada e saída do local.

Seção 11 – Segurança Física

11.2.6 - Segurança de equipamentos e ativos fora das dependências da organização - 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.

- Estabelecer controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, determinados por uma avaliação de riscos.
- Inclui todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, cartões inteligentes, papéis e outros, utilizados no trabalho em casa, ou fora do local normal de trabalho.

Obs.: Recomenda-se evitar o risco, desencorajando o trabalho fora da organização, ou restringindo o uso de dispositivos móveis.

Seção 11 – Segurança Física

11.2.7 - Reutilização e alienação segura de equipamentos - Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança, antes do descarte ou do seu uso.

- Destruir fisicamente mídias de armazenamento que contém informações confidenciais ou de direitos autorais.
- Ou destruir as informações, apagar ou sobregravar por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.
- Determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo.
- Adicionalmente, pode-se usar a encriptação completa do disco.

Seção 11 – Segurança Física

11.2.8 - Equipamento de usuário sem monitoração - Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

- Encerrar as sessões ativas ou bloquear tela com proteção de senha.
- Efetuar a desconexão de serviços de rede ou aplicações.

Seção 11 – Segurança Física

11.2.9 - Política de mesa limpa e tela limpa - Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

- Estabelecer uma política de mesa limpa e tela protegida levando em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da organização.
- Guardar as informações do negócio sensíveis ou críticas em lugar seguro, idealmente em um cofre, armário ou outras formas de mobília de segurança, quando não em uso, especialmente quando o escritório está desocupado.
- Evitar uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (scanners, máquinas fotográficas digitais etc.).

Seção 12 – Segurança nas Operações

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

A.12.1.1	Documented operating procedures	*Control* Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	Change management	*Control* Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
A.12.1.3	Capacity management	*Control* The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

Seção 12 – Segurança nas Operações

12.1.1 - Documentação dos procedimentos de operação - Convém que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.

- Instruções para tratamento de erros ou condições excepcionais.
- Contatos para suporte e escalação, incluindo contatos externos.
- Instruções quanto ao manuseio de mídias, incluindo procedimentos para o descarte seguro destas mídias.
- Procedimento para o reinício e recuperação em caso de falha.
- Gerenciamento de trilhas de auditoria e registros (logs) de sistemas.

Obs.: Convém que os procedimentos operacionais e os procedimentos documentados para atividades de sistemas sejam tratados como documentos formais e as mudanças sejam autorizadas pela direção.

Seção 12 – Segurança nas Operações

12.1.2 - Gestão de mudanças - 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.

- Identificação e registro das mudanças significativas.
- Planejamento, testes das mudanças, avaliação de impactos potenciais, incluindo impactos de segurança da informação.
- Procedimento formal de aprovação das mudanças propostas e comunicação dos detalhes para todas as pessoas relevantes.
- Procedimentos de recuperação, incluindo procedimentos e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

Seção 12 – Segurança nas Operações

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

- Identificar requisitos de capacidade levando-se em conta a criticidade do negócio e implantar controles detectivos para prever problemas em tempo hábil e projetar a capacidade futura.
- Exemplos para aumentar ou manter a capacidade incluem: exclusão de dados obsoletos, desativação de aplicações, sistemas, ou ambientes, otimização das programações, da lógica de aplicação ou das consultas à base, negar ou restringir a largura da banda para recursos não críticos ao negócio.

Obs.: Este controle também considera a capacidade dos recursos humanos, bem como dos escritórios e instalações.

Seção 12 – Segurança nas Operações

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

- Regras para a transferência de software do ambiente de desenvolvimento para o de produção.
- Separar software em desenvolvimento de software em produção.
- Testar mudanças nas aplicações e nos sistemas operacionais em um ambiente de teste ou projeto piloto.
- Desabilitar compiladores, editores e ferramentas de desenvolvimento ou utilitários de sistemas não necessários.
- Evitar copiar dados sensíveis para os ambientes de testes.

Seção 12 – Segurança nas Operações

Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

A.12.2.1	Controls against mal-ware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Seção 12 – Segurança nas Operações

12.2.1 - Controles contra códigos maliciosos - Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.

- Proibir e detectar o uso de softwares não autorizados.
- Prevenir e detectar o uso de websites maliciosos.
- Conduzir análises críticas regulares dos softwares e dados dos sistemas que suportam processos críticos de negócio.
- Instalar e atualizar regularmente softwares de detecção e remoção de códigos maliciosos para o exame de computadores e mídias.
- Coletar informações, através por exemplo, de assinaturas de listas de discussão e sites informativos sobre códigos maliciosos.

Seção 12 – Segurança nas Operações

12.2.1 - Controles contra códigos maliciosos - Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.

Obs.: A utilização de dois ou mais tipos de software de controle contra códigos maliciosos de diferentes fornecedores e tecnologias pode aumentar a eficácia na proteção contra códigos maliciosos.

Obs.: Atenção contra a introdução de códigos maliciosos durante procedimentos de emergência, os quais podem ultrapassar os controles comuns de proteção contra códigos maliciosos.

Obs.: O uso isolado de softwares de reparação e detecção não é usualmente adequado e geralmente necessita ser acompanhado de procedimentos operacionais adicionais.

Seção 12 – Segurança nas Operações

Objetivo: Proteger contra a perda de dados.

A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

Seção 12 – Segurança nas Operações

12.3.1 - Cópias de segurança das informações - Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

- A abrangência e freqüência “devem” refletir requisitos de negócio.
- Armazenar as cópias de segurança em uma localidade remota.
- Dar nível apropriado de proteção física e ambiental das informações das cópias de segurança, consistentes com as da instalação principal.
- Testar as mídias de backup regularmente combinado com um teste de restauração contra o tempo de restauração requerido.
- Proteger as cópias de segurança através de encriptação.

Seção 12 – Segurança nas Operações

Objetivo: Registrar eventos e gerar evidências.

A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronisation	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

Seção 12 – Segurança nas Operações

12.4.1 - Registros de eventos - 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.

- Incluir ID dos usuários, atividades, datas, horários e eventos-chave.
- Registros das tentativas de acesso ao sistema (aceitas e rejeitadas).
- Alterações na configuração do sistema, uso de privilégios, uso de aplicações e utilitários do sistema, arquivos acessados, endereços e protocolos de rede, alarmes provocados pelo sistema, ativação e desativação dos sistemas de proteção, registros de transações etc.

Obs.: Proteger os registros (log) contra a violação da privacidade.

Seção 12 – Segurança nas Operações

12.4.2 - Proteção das informações dos registros de eventos (logs) - Convém que as informações dos registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração.

- Proteger contra modificações não autorizadas às informações dos (logs) e problemas operacionais como: alterações dos tipos de mensagens que são gravadas, arquivos de registros (log) sendo editados ou excluídos, capacidade de armazenamento da mídia magnética do arquivo de registros (log) excedida, resultando em falhas no registro de eventos ou sobreposição do registro anterior.

Obs.: Registros (log) precisam ser protegidos, porque se os dados forem modificados ou excluídos, a sua existência pode gerar a falsa sensação de segurança. A cópia em tempo real para um sistema fora do controle do administrador ou operador pode ser ideal.

Seção 12 – Segurança nas Operações

12.4.3 - Registros de eventos (log) de administrador e operador - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

- As pessoas que possuem conta de usuário privilegiado podem ser capazes de manipular os registros (logs) nos recursos de processamento da informação que estão sob o seu controle direto, sendo portanto necessário proteger e analisar criticamente os registros (logs) para manter o controle dos usuários privilegiados.

Seção 12 – Segurança nas Operações

12.4.4 - Sincronização dos relógios - 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.

- Utilizar um tempo padrão de referência obtido de uma fonte externa para sincronizar, de forma confiável, os relógios internos.

Obs.: O ajuste correto dos relógios dos computadores é importante para garantir a exatidão dos registros (log) de auditoria, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares. O protocolo de hora da rede pode ser utilizado para sincronizar todos os relógios dos servidores.

Seção 12 – Segurança nas Operações

Objetivo: Assegurar a integridade dos sistemas operacionais.

A.12.5.1	Installation of software on operational systems	*Control* Procedures shall be implemented to control the installation of software on operational systems.

Seção 12 – Segurança nas Operações

12.5.1 - Instalação de software nos sistemas operacionais - Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

- Sistemas apenas com código executável e aprovado, e sem códigos em desenvolvimento ou compiladores.

Obs.: Qualquer decisão de atualização para uma nova versão precisa considerar os requisitos do negócio e de segurança associada, por exemplo, à introdução de uma nova funcionalidade e à gravidade dos problemas de segurança associados a esta nova versão.

Obs.: É recomendado que acessos físicos e lógicos sejam concedidos a fornecedores, somente quando necessário e com aprovação gerencial.

Seção 12 – Segurança nas Operações

Objetivo: Prevenir a exploração de vulnerabilidades técnicas.

A.12.6.1	Management of technical vulnerabilities	*Control* Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.

Seção 12 – Segurança nas Operações

12.6.1 - Gestão de vulnerabilidades técnicas - Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.

- Um inventário completo e atualizado dos ativos de informação é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica.
- Definir um prazo para a reação a notificações de vulnerabilidades.
- Dependendo da urgência, a ação a ser tomada pode estar relacionada à gestão de mudanças ou à resposta a incidentes.
- Avaliar os riscos associados à sua instalação de uma correção.

Obs.: A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças.

Seção 12 – Segurança nas Operações

12.6.2 - Restrições quanto à instalação de software - Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.

- Definir uma política mandatória e restrita, sobre quais os tipos de software os usuários podem instalar.
- Aplicar o princípio do privilégio mínimo nas máquinas de usuários.

Seção 12 – Segurança nas Operações

Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

A.12.7.1	Information systems audit controls	*Control* Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

Seção 12 – Segurança nas Operações

12.7.1 - Controles de auditoria de sistemas de informação - Convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

- Acordar requisitos de auditoria para acesso a sistemas e dados e o escopo dos testes técnicos da auditoria e gerar registros de forma a produzir uma trilha de referência.
- Limitar auditoria somente a leitura.
- Realizar testes que possam afetar a disponibilidade fora do horário normal de trabalho.

Seção 13 – Segurança nas Comunicações

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

Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	*Control* Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	*Control* Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3	Segregation in networks	*Control* Groups of information services, users and information systems shall be segregated on networks.

Seção 13 – Segurança nas Comunicações

13.1.1 - Controles de redes - Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

- Responsabilidades sobre o gerenciamento de equipamentos de rede.
- Controles especiais para proteção dos dados que trafegam sobre redes públicas ou sobre as redes sem fio (wireless).
- Restingir e autenticar a conexão de sistemas à rede.

Obs.: Informações adicionais sobre segurança em rede pode ser encontrada na ISO / IEC 27033.

Seção 13 – Segurança nas Comunicações

13.1.2 - Segurança dos serviços de rede - 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.

- Determinar, monitorar e auditar a capacidade do provedor dos serviços de rede de gerenciar os serviços de maneira segura.
- Identificar e assegurar a implementação das medidas de segurança necessárias para serviços específicos, como características de segurança, níveis de serviço e requisitos de gerenciamento.

Obs.: Serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como firewalls e sistemas de detecção de intrusos.

Seção 13 – Segurança nas Comunicações

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

- Dividir diferentes domínios de rede com base no nível de confiança (público, estações de trabalho, servidores etc.), em áreas da organização (por exemplo, RH, financeiro, marketing) etc.
- Permitir a acesso entre domínios somente através de um gateway (firewall etc.) considerando custos da incorporação da tecnologia.
- Tratar acessos wireless como conexão externa e segregar esse acesso das redes internas, até que o acesso tenha passado por um gateway, antes de conceder comunicação com sistemas internos.

Seção 13 – Segurança nas Comunicações

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

A.13.2.1	Information transfer policies and procedures	*Control* Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
A.13.2.2	Agreements on information transfer	*Control* Agreements shall address the secure transfer of business information between the organization and external parties.
A.13.2.3	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.
A.13.2.4	Confidentiality or non-disclosure agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

Seção 13 – Segurança nas Comunicações

13.2.1 - Políticas e procedimentos para transferência de informações - 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.

- Proteger contra interceptação, modificação, desvio e destruição.
- Proteger informações eletrônicas sensíveis transmitidas em anexos.
- Definir política que especifiquem o uso aceitável dos recursos eletrônicos de comunicação (responsabilidade de funcionários e partes externas que possam comprometer a organização através de, por exemplo, difamação, assédio, falsa identidade, retransmissão de "correntes", compras não autorizadas etc.).
- Restringir a retransmissão de e-mails para endereços externos.

Seção 13 – Segurança nas Comunicações

13.2.1 - Políticas e procedimentos para transferência de informações - 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.

- Alertar quanto ao uso de fax (acesso não autorizado a dispositivos; retransmissão de mensagens para números determinados; envio de documentos e mensagens para número errado, por falha na discagem ou uso de número errado etc.).
- Alertar quanto a manter conversas confidenciais em locais públicos, escritórios abertos, canais de comunicação inseguros etc.

Obs.: Atentar para os aspectos legais e de negócio pertinentes.

Seção 13 – Segurança nas Comunicações

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

- Assegurar a rastreabilidade dos eventos e o não-repúdio.
- Definir padrões técnicos para embalagem e transmissão, custódia, identificação de portadores, responsabilidades e obrigações na ocorrência de incidentes de segurança, como perda de dados.
- Identificar informações críticas e sensíveis, garantindo que os rótulos sejam entendidos e que a informação seja devidamente protegida.

Seção 13 – Segurança nas Comunicações

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

- Proteger contra acesso não autorizado, modificação ou negação de serviço e assegurar endereçamento e transporte estejam corretos.
- Aprovar uso de serviços públicos tais como sistemas de mensagens instantâneas, redes sociais e compartilhamento de arquivos.

Obs.: Existem muitos tipos de mensagem eletrônica, como, e-mails, Eletronic Data Interchange (EDI), e redes sociais que cumprem um papel importante nas comunicações do negócio

Seção 13 – Segurança nas Comunicações

13.2.4 - Acordos de confidencialidade e não divulgação - 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.

- Definir o tempo de duração esperado do acordo.
- Definir o proprietário da informação, que tipo de uso é permitido, e os direitos do signatário para usar a informação.
- Determinar termos para a informação ser retornada ou destruída quando do término do acordo e as ações esperadas a serem tomadas no caso de uma violação do acordo.

Obs.: Atentar para a conformidade com as leis e regulamentações aplicáveis na jurisdição para a qual eles se aplicam.

QUESTÕES

CESPE/2015 - STJ - Analista Judiciário - Suporte em TI

Com base nas normas ISO 27001, ISO 27002, ISO 27003, ISO 27004 e ISO 27005, relativas à segurança de ativos de informação das organizações, julgue o item a seguir.

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.

QUESTÕES

CESPE/2015 - MPOG - Analista em Tecnologia da Informação

Julgue o seguinte item, relativo à segurança da informação, com base no que dispõem as normas ISO/IEC 27002 e ISO/IEC 27001.

De acordo com a norma ISO 27002, convém que os acordos com terceiros que envolvam, por exemplo, processamento ou gerenciamento dos recursos de processamento da informação cubram todos os requisitos de segurança da informação relevantes, incluindo a possibilidade de indenização a terceiros.

QUESTÕES

CESPE/2015 - MPOG - Analista em Tecnologia da Informação

Julgue o seguinte item, relativo à segurança da informação, com base no que dispõem as normas ISO/IEC 27002 e ISO/IEC 27001.

A norma ISO 27002 estabelece que seja designado um proprietário para todas as informações e os ativos associados com os recursos de processamento da informação.

QUESTÕES

CESPE/2014 - ANATEL - Analista Administrativo - Suporte

Julgue os itens de 86 a 90 a respeito das normas ISO/IEC 27001 e ISO/IEC 27002 e do sistema de gestão de segurança da informação (SGSI).

A norma ISO 27002 recomenda que as chaves criptográficas usadas para as assinaturas digitais de documentos eletrônicos sejam idênticas àquelas usadas para a criptografia desses documentos: a padronização das chaves garante maior segurança aos documentos.

QUESTÕES

CESPE/2014 - TJ-SE - Analista Judiciário - Análise de Sistemas

Com base nas normas ABNT NBR ISO/IEC n.º 27001:2006 e n.º 27002:2005, julgue os itens a seguir, relativos à gestão de segurança da informação.

De acordo com a norma ISO/IEC n.º 27002:2005, é permitido que o administrador de sistemas suprima ou desative o registro (log) de suas próprias atividades em caso de falta de espaço em disco.

QUESTÕES

CESPE/2015 - MEC - Administrador de Dados

Considerando as normas ISO/IEC 27001, ISO/IEC 27002 e IN MPOG n.º 04/2014, julgue o item subsequente.

Durante o processo de correção das provas do ENEM, deve-se implementar a separação dos recursos de desenvolvimento, mas não os de teste e de produção.

QUESTÕES - Gabarito

CESPE/2015 - STJ: ERRADO
CESPE/2015 - MPOG: CERTO (mas com base na 27002:2005)
CESPE/2015 - MPOG: ERRADO
CESPE/2014 - ANATEL: ERRADO
CESPE/2014 - TJ-SE: ERRADO
CESPE/2015 - MEC: ERRADO

Seção 14 – Aquisição, Dev. e Manutenção

Objetivo: Garantir que a segurança da informação é 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.

A.14.1.1	Information security requirements analysis and specification	*Control* The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	*Control* Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	*Control* Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Seção 14 – Aquisição, Dev. e Manutenção

14.1.1 - Análise e especificação dos requisitos de segurança da informação - Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

- Definir requisitos nos estágios iniciais dos projetos de sistemas.
- Seguir um processo de aquisição e testes para produtos adquiridos.
- Para aquisições de software, contemplar segurança nos contratos com fornecedores, risco e controles associados antes da compra.
- Avaliar funcionalidades adicionais criticamente para assegurar que ela não introduz riscos adicionais inaceitáveis.

Seção 14 – Aquisição, Dev. e Manutenção

14.1.2 - Serviços de aplicação seguros em 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.

- Informar parceiros sobre as diretrizes de fornecimento e uso.
- Garantir confidencialidade e integridade de transações de pedidos, pagamentos, informações de transação etc.

Obs.: Aplicações acessadas através de redes públicas são suscetíveis a uma variedade de ameaças de rede, como: atividades fraudulentas, disputas contratuais ou divulgação de informação para o público.

Obs.: Os controles requeridos sempre incluem métodos de criptografia para autenticação e segurança na transferência dos dados.

Seção 14 – Aquisição, Dev. e Manutenção

14.1.3 - Protegendo as transações nos aplicativos de serviços - 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.

- Usar assinaturas eletrônicas para cada uma das partes.
- Criptografar o caminho de comunicação entre todas as partes usando protocolos de comunicação seguros.
- Armazenar detalhes da transação fora de locais públicos, como a Intranet da organização; evitar um meio acessível pela Internet.
- Onde for usada uma CA a segurança é integrada ao longo de todo o processo de gestão dos certificados/assinaturas.

Seção 14 – Aquisição, Dev. e Manutenção

Objetivo: Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.

A.14.2.1	Secure development policy	*Control* Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.2	System change control procedures	*Control* Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3	Technical review of applications after operating platform changes	*Control* When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	Restrictions on changes to software packages	*Control* Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Seção 14 – Aquisição, Dev. e Manutenção

Objetivo: Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.

A.14.2.5	Secure system engineering principles	*Control* Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
A.14.2.6	Secure development environment	*Control* Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.7	Outsourced development	*Control* The organization shall supervise and monitor the activity of outsourced system development.
A.14.2.8	System security testing	*Control* Testing of security functionality shall be carried out during development.
A.14.2.9	System acceptance testing	*Control* Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Seção 14 – Aquisição, Dev. e Manutenção

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

- Considerar a segurança do desenvolvimento em todo o projeto.
- Adotar práticas de programação seguras tanto para novos desenvolvimentos como para cenários de reuso dos códigos.
- Obter garantia de que a parte externa adota as mesmas regras para o desenvolvimento seguro no caso de software terceirizado.

Seção 14 – Aquisição, Dev. e Manutenção

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

- Controlar mudança de novos sistemas ou mudanças maiores em sistemas existentes, seguindo um processo formal para documentar, especificar, testar, controlar qualidade e gerir a implementação.
- Obter aprovação para mudanças antes do início dos trabalhos, e garantir que usuários aceitam as mudanças antes da implementação.
- Garantir o controle de versão para todas as atualizações de software e de uma trilha de auditoria de todas as mudanças solicitadas.

Obs.: Não é recomendada a utilização de atualizações automáticas em sistemas críticos visto que algumas atualizações podem causar falhas.

Seção 14 – Aquisição, Dev. e Manutenção

14.2.3 - Análise crítica técnica das aplicações após mudanças nas plataformas operacionais - Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.

- Garantir que as mudanças previstas na plataforma operacional sejam comunicadas em tempo hábil para permitir os testes e análises críticas antes da implementação.
- Garantir que as mudanças necessárias sejam incluídas nos planos de continuidade de negócios.

Obs.: Plataformas operacionais incluem sistemas operacionais, banco de dados e plataformas intermediárias.

Seção 14 – Aquisição, Dev. e Manutenção

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

- Utilizar pacotes providos por fornecedores sem modificações.

Se for modificar,

- Considerar o risco de que controles e processos de integridade embutidos no software sejam comprometidos.
- Obter consentimento do fornecedor.
- Considerar o impacto resultante quando a organização passa a ser responsável pela manutenção futura do software.

Seção 14 – Aquisição, Dev. e Manutenção

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

- Projetar segurança em todas as camadas da arquitetura (negócios, dados, aplicações e tecnologia), realizando o balanceamento entre a necessidade da segurança da informação com a acessibilidade.
- Analisar novas tecnologias quanto aos riscos de segurança.
- Analisar os princípios criticamente, a intervalos regulares, para garantir que eles permanecem atualizados.
- Aplicar os princípios de engenharia de segurança onde pertinente, para sistemas terceirizados, por meio de contratos e outros acordos.

Seção 14 – Aquisição, Dev. e Manutenção

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

- O ambiente de desenvolvimento seguro inclui pessoas, processos e tecnologia, associados com a integração e o desenvolvimento.
- Considerar a confiabilidade das pessoas que trabalham no ambiente.
- Considerar o grau de terceirização associado aos sistemas.
- Segregar os diferentes ambientes de desenvolvimento, controlar acesso ao ambiente de desenvolvimento, monitorar mudanças ao ambiente e do código armazenado no ambiente.
- Armazenar backups em locais seguros externos à organização.

Seção 14 – Aquisição, Dev. e Manutenção

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

- Considerar segurança ao longo de toda a cadeia de suprimento.
- Considerar acordos de licença, propriedade do código e direitos de propriedade intelectual relacionados com o conteúdo terceirizado.
- Executar testes de aceitação relativos à qualidade dos itens.
- Executar testes para proteger contra vulnerabilidades conhecidas e código malicioso, intencional e não intencional, antes da entrega.
- Considerar cláusulas para auditar processos de desenvolvimento.

Obs.: A organização ainda é sempre responsável pela conformidade.

Obs.: Informações sobre relação com fornecedores em ISO/IEC 27036.

Seção 14 – Aquisição, Dev. e Manutenção

14.2.8 - Teste de segurança do sistema - Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.

- Testar sistemas durante o processo de desenvolvimento, incluindo a preparação de uma programação de atividades detalhada, com testes de entrada e saída sob determinadas condições.
- Para o desenvolvimento interno, convém que tais testes sejam inicialmente realizados pela equipe de desenvolvimento.
- Realizar testes de aceitação independente (tanto para desenvolvimento interno como para desenvolvimento terceirizado).

Seção 14 – Aquisição, Dev. e Manutenção

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

- Incluir testes de aceitação para validar requisitos de segurança da informação e aderência às práticas de desenvolvimento seguro.
- Utilizar ferramentas automatizadas, como ferramentas de análise de códigos ou scanners de vulnerabilidade, para verificar a correção dos defeitos relacionados à segurança.
- Construir um ambiente de teste realístico para assegurar que o sistema não introduzirá vulnerabilidades ao ambiente da organização e que os testes são confiáveis.

Seção 14 – Aquisição, Dev. e Manutenção

Objetivo: Assegurar a proteção dos dados usados para teste.

A.14.3.1	Protection of test data	*Control* Test data shall be selected carefully, protected and controlled.

Seção 14 – Aquisição, Dev. e Manutenção

14.3.1 - Proteção dos dados para teste - Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

- Selecionar, proteger e controlar os dados de teste.
- Evitar usar bancos operacionais que contenham informação de identificação pessoal ou qualquer outra informação confidencial.
- Aplicar procedimentos de controle de acesso semelhates aos aplicados aos sistemas de aplicações em operação.
- Apagar a informação operacional logo após a realização dos testes.

Obs.: Os testes de aceitação geralmente requerem um volume substancial de dados, o mais próximo possível do operacional.

Seção 15 – Cadeia de Suprimento

Objetivo: Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.

A.15.1.1	Information security policy for supplier relationships	*Control* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	*Control* All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
A.15.1.3	Information and communication technology supply chain	*Control* Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Seção 15 – Cadeia de Suprimento

15.1.1 - Política de segurança da informação no relacionamento com os 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.

- Criar uma política de acesso às informações da organização.
- Considerar os procedimentos para a organização e fornecedor.
- Conscientizar o pessoal da organização quanto aos procedimentos.

Obs.: Se existir uma necessidade especial de confidencialidade da informação, acordos de não divulgação podem ser utilizados.

Obs.: As responsabilidades contratuais e legais para proteger a informação permanecem com a organização.

Seção 15 – Cadeia de Suprimento

15.1.2 - Identificando segurança da informação nos acordos com fornecedores - 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.

- Assegurar clareza entre a organização e o fornecedor, com relação à obrigação de ambas as partes com o cumprimento dos requisitos.
- Classificar a informação de acordo com o esquema da organização.
- Controlar a subcontratação, incluindo os controles necessários.
- Estipular direito de auditar os processos do fornecedor.

Obs.: Convém que sejam considerados nos acordos procedimentos para continuidade nos casos em que o fornecedor se torne incapaz.

Seção 15 – Cadeia de Suprimento

15.1.3 - Cadeia de suprimento na tecnologia da comunicação e informação - Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.

- Exigir que os fornecedores divulguem os requisitos de segurança da informação da organização em toda a cadeia de suprimentos.
- Garantir que os componentes críticos e as suas origens podem ser rastreadas ao longo de toda a cadeia de suprimento.
- Incluir os serviços de computação na nuvem neste contexto.

Seção 15 – Cadeia de Suprimento

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

A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	*Control* Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Seção 15 – Cadeia de Suprimento

15.2.1 - Monitoramento e análise crítica de serviços com fornecedores - Convém que a organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

- Garantir que os termos e condições dos acordos sejam cumpridos.
- Realizar auditorias nos fornecedores, em conjunto com a análise crítica dos relatórios de auditoria independente, quando disponíveis.
- Analisar criticamente os aspectos de segurança da informação na relação dos fornecedores com seus próprios fornecedores.
- Garantir que o fornecedor mantém capacidade de serviço suficiente e que os níveis de continuidade do serviço acordados são mantidos.

Seção 15 – Cadeia de Suprimento

15.2.2 - Gerenciamento de mudanças para serviços com 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.

- Mudanças feitas pela organização: melhorias dos serviços, desenvolvimento novas aplicações e sistemas, atualizações das políticas e procedimentos, controles novos ou modificados para resolver os incidentes e para melhorar a segurança da informação.
- Mudanças nos serviços de fornecedores: mudanças e melhorias em redes, novas tecnologias, novos produtos ou versões, novas ferramentas e ambientes de desenvolvimento, localização física dos recursos ou subcontratação com outro fornecedor.

Seção 16 – Incidentes de Segurança

Objetivo: 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.

A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

Seção 16 – Incidentes de Segurança

Objetivo: 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.

A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Seção 16 – Incidentes de Segurança

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

- Estabelecer responsabilidades por gerenciar incidentes (planejar, monitorar, detectar, analisar, tratar evidências forenses etc.).
- Manter um ponto de contato para notificação de incidentes.
- Manter contatos apropriados com autoridades, grupos, fóruns etc.
- Treinar e conscientizar as pessoas quanto ao procedimento.
- Referenciar um processo interno disciplinar formal.

Obs.: Incidentes podem transcender os limites nacionais.

Obs.: Diretrizes sobre a gestão de incidentes em ISO/IEC 27035.

Seção 16 – Incidentes de Segurança

16.1.2 - Notificação de eventos de segurança da informação - Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

- Convém que todos os funcionários e partes externas notifiquem evento de segurança o mais rapidamente possível.
- Notificar um evento de segurança como: violação da disponibilidade, confidencialidade e integridade da informação, erros humanos, não-conformidade com políticas ou diretrizes, procedimentos de segurança física, mudanças descontroladas de sistemas, mau funcionamento de software ou hardware, violação de acesso etc.

Obs.: Mau funcionamento ou comportamento anômalo pode indicar ataques ou violação na segurança e, portanto, convém que sejam reportados como um evento de segurança da informação.

Seção 16 – Incidentes de Segurança

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

- Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido possível, de forma a prevenir incidentes de segurança da informação.
- O mecanismo de notificação deve ser fácil, acessível e disponível.

Obs.: Evitar tentar provar fraquezas de segurança. Testar fraquezas pode ser interpretado como potencial mau uso do sistema e pode também causar danos ao serviço ou sistema de informação e resultar em responsabilidade legal para o indivíduo que executou o teste.

Seção 16 – Incidentes de Segurança

16.1.4 - Avaliação e decisão dos eventos de segurança da informação - 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 se avalie cada evento usando uma escala de classificação de incidentes e eventos, para decidir se o evento seja classificado como um incidente de segurança da informação.
- Em casos onde a organização tenha uma equipe de resposta a incidentes de segurança da informação, a avaliação e decisão seja encaminhada para a equipe, para confirmação ou reavaliação.
- Convém que os resultados da avaliação e decisão sejam registrados em detalhes, para o propósito de verificação e referência futura.

Seção 16 – Incidentes de Segurança

16.1.5 - Resposta aos incidentes de segurança da informação - Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

- Convém que incidentes sejam reportados para um ponto de contato definido e outras pessoas relevantes, ou ainda, partes externas.
- Coletar evidências logo após a ocorrência e realizar análise forense.
- Tratar as fragilidades encontradas que causem ou contribuam para o incidente, uma vez que o incidente foi tratado.
- Convém que análises pós-incidente sejam realizadas, se necessário, para identificar a fonte do incidente.

Obs.: O primeiro objetivo de resposta a incidente é “voltar ao nível de segurança normal” e então iniciar a recuperação necessária.

Seção 16 – Incidentes de Segurança

16.1.6 - Aprendendo com os incidentes de segurança da informação - 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.

- Monitorar e quantificar os tipos, volumes e custos de incidentes.
- Convém que a informação resultante da análise de incidentes seja usada para identificar incidentes recorrentes ou de alto impacto.

Obs.: A avaliação pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de incidentes.

Obs.: Estórias de incidentes podem ser usadas em treinamentos de conscientizações de usuários como exemplos do que pode acontecer, como responder a tais incidentes e como evitá-los no futuro.

Seção 16 – Incidentes de Segurança

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

- Adotar procedimentos para obter evidências para os propósitos de ações legais ou disciplinares (identificação, coleta, preservação de evidências, de acordo com diferentes tipos de mídia etc.).
- Convém que os procedimentos levem em conta: a cadeia de custódia, a segurança da evidência, a segurança das pessoas, papéis e responsabilidades das pessoas envolvidas, competência do pessoal, documentação e resumo do incidente.
- Usar certificações ou outros meios de qualificação de pessoal (e ferramentas), para aumentar o valor da evidência preservada.

Seção 16 – Incidentes de Segurança

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

Obs.: Evidência forense pode ir além dos limites da organização ou da jurisdição e, em tais casos, convém que seja assegurado que a organização tem direito de coletar as informações.

Obs.: Os requisitos de diferentes jurisdições podem ser considerados para maximizar as chances de admissão.

Obs.: Logo quando um evento de segurança é detectado pode não ser óbvio se o evento resultará em uma ação judicial ou não. É aconselhável envolver um advogado ou a polícia o quanto antes.

Obs.: A ISO/IEC 27037 fornece diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.

Seção 17 – Continuidade

Objetivo: É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização.

A.17.1.1	Planning information security continuity	*Control* The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	*Control* The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3	Verify, review and evaluate information security continuity	*Control* The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Seção 17 – Continuidade

17.1.1 - Planejando a continuidade da segurança da informação - 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.

- Assegurar que a continuidade da segurança está dentro do processo de gestão da continuidade do negócio, quando este existir.
- Assegurar que requisitos de continuidade da segurança da informação estão contemplados na continuidade do negócio ou nos processos de gerenciamento da recuperação de desastre.

Obs.: Informações adicionais: ISO/IEC 27031, ISO 22313 e ISO 22301.

Seção 17 – Continuidade

17.1.2 - Implementando a continuidade da segurança da informação - 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.

- Implementrar estrutura de gerenciamento adequada.
- Designar pessoal de resposta a incidente com a necessária responsabilidade, autoridade e competência.
- Desenvolver e aprovar planos e procedimentos de resposta.
- Esabelecer e manter controles para os processos de recuperação de desastre ou de continuidade do negócio.

Obs.: Os controles devem operar durante uma condição de situação adversa ou outros controles devem ser estabelecidos.

Seção 17 – Continuidade

17.1.3 - Verificação, análise crítica e avaliação da continuidade da segurança da informação - Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

- Mudanças organizacionais podem conduzir a mudanças nos requisitos de continuidade da segurança da informação.
- Testar e verificar a funcionalidade dos processos, procedimentos e controles da continuidade para garantir que eles são consistentes com os objetivos da continuidade da organização.

Obs.: A verificação dos controles da continuidade da segurança da informação é diferente das verificações e testes da segurança.

Seção 17 – Continuidade

Objetivo: 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.

A.17.2.1	Availability of information processing facilities	*Control* Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Seção 17 – Continuidade

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

- Identificar requisitos do negócio quanto à disponibilidade.
- Considerar componentes redundantes.
- Testar sistemas de informação redundantes para assegurar a transferência de um componente para outro componente.

Obs.: A implementação de redundâncias pode introduzir riscos a integridade ou confidencialidade da informação e dos sistemas.

Seção 18 – Conformidade

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

A.18.1.1	Identification of applicable legislation and contractual requirements	*Control* All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2	Intellectual property rights	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3	Protection of records	*Control* Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

Seção 18 – Conformidade

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

A.18.1.4	Privacy and protection of personally identifiable information	*Control* Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

Seção 18 – Conformidade

18.1.1 - Identificação da legislação aplicável e de requisitos contratuais - 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 os controles específicos e as responsabilidades para atender a estes requisitos sejam definidos e documentados.
- Convém que os gestores identifiquem toda a legislação aplicável à sua organização, para atender aos requisitos relativos ao seu tipo de negócio. Caso a organização realize negócios em outros países convém considerar a conformidade em todos esses países.

Seção 18 – Conformidade

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

- Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal da informação.
- Aquirir software somente por meio de fontes conhecidas.
- Tomar ações disciplinares contra pessoas que violarem políticas.
- Manter provas e evidências da propriedade de licenças.
- Conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados.

Seção 18 – Conformidade

18.1.3 - Proteção de registros - 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.

- Classificar registros com base no esquema da organização.
- Categorizar os registros em tipos (contábeis, transações, auditoria e procedimentos operacionais).
- Tomar cuidados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros.

Obs.: Registros podem ser retidos por causa de requisitos estatutários, regulamentos ou contratos como prova de que uma organização opera dentro de normas, ou para confirmar a situação financeira perante os acionistas, partes externas e auditores.

Seção 18 – Conformidade

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

- Desenvolver a política de privacidade da identificação pessoal.
- Indicar uma pessoa responsável (privacy officer), que tem a função de fornecer orientações aos gestores, usuários e provedores.

Obs.: Alguns países têm introduzido legislação que estabelecem controles na coleta e processamento de informação pessoal.

Obs.: A ISO/IEC 29100 fornece uma estrutura de alto nível para a proteção da informação de identificação pessoal, no âmbito da TI.

Seção 18 – Conformidade

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

- Considerar restrições à importação e/ou exportação de hardware e software de computador para execução de funções criptográficas.
- Considerar restrições quanto ao uso de criptografia.
- Considerar métodos mandatórios ou discricionários de acesso pelas autoridades dos países à informação cifrada.

Obs.: Convém que a assessoria jurídica garanta a conformidade com as legislações e regulamentações vigentes. Convém que seja obtida assessoria jurídica antes de se transferir informações cifradas ou controles de criptografia para outros países.

Seção 18 – Conformidade

Objetivo: Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

A.18.2.1	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
A.18.2.2	Compliance with security policies and standards	*Control* Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	Technical compliance review	*Control* Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Seção 18 – Conformidade

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

- Iniciar a análise crítica independente pela direção a fim de assegurar a contínua pertinência, adequação e eficácia do enfoque.
- Avaliar oportunidades para melhoria e necessidade de mudanças.
- Realizar auditorias internas (ou externas).

Obs.: A ISO/IEC 27007, "Diretrizes para auditoria de sistemas" e a ISO/IEC TR 27008 , "Diretrizes para auditores sobre controles" também fornecem orientações para a realização de análise crítica.

Seção 18 – Conformidade

18.2.2 - Conformidade com as políticas e procedimentos de segurança da informação - 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.

- Identifiquem como analisar criticamente se os requisitos estabelecidos nas políticas, procedimentos, normas e outras regulamentações aplicáveis, estão sendo atendidos.
- No caso de não conformidade: identificar as causas, avaliar a necessidade de ações, implementar ação corretiva, analisar criticamente ação corretiva tomada.
- Registar e manter os resultados das análises críticas e das ações corretivas realizadas pelos gestores.

Seção 18 – Conformidade

18.2.3 - Análise crítica da conformidade técnica - 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.

- Verificar a conformidade com o apoio de ferramenta automática ou, alternativamente, por um engenheiro de sistemas experiente.
- Tomar precauções se forem usados teste de invasão.
- Analisar sistemas operacionais para garantir que controles de hardare e softare foram corretamente implementados.
- Os testes de invasão e avaliação de vulnerabilidades fornecem um snapshot em um estado específico para um tempo específico.

Obs.: A ISO/IEC TR 27008 fornece orientações específicas sobre as análises criticas de conformidade técnica.

QUESTÕES

FCC/2015 - TCM-GO - Auditor de Controle Externo - Informática

A seção Gestão de Incidentes de Segurança da Informação da Norma ABNT NBR ISO/IEC 27002:2005 tem como objetivo apresentar recomendações para

a) resolver de forma definitiva os problemas causados por incidentes de segurança da informação estabelecendo e executando as ações necessárias para minimizar efeitos causados aos dados dos sistemas de informação e comunicação.

b) não permitir a interrupção das atividades do negócio, proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.

QUESTÕES

FCC/2015 - TCM-GO - Auditor de Controle Externo - Informática

A seção Gestão de Incidentes de Segurança da Informação da Norma ABNT NBR ISO/IEC 27002:2005 tem como objetivo apresentar recomendações para

c) garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação e detectar e resolver incidentes de segurança da informação em tempo hábil.

d) evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

e) assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

QUESTÕES

ITNERANTE/2015

Julgue o item a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.

A fim de assegurar que os sistemas estejam sempre atualizados com relação às vulnerabilidades mais conhecidas de mercado, a norma recomenda que sejam feitas atualizações automáticas de sistemas sempre que possível.

QUESTÕES

TIMASTERS/2015

O principal objetivo da resposta aos incidentes de segurança da informação é:

a) Reportar o incidente para um ponto de contato definido e outras pessoas ou partes externas relevantes.

b) Coletar evidências logo após a ocorrência o incidente para possibilitar a relização de análise forense e auditoria.

c) Tratar as fragilidades encontradas que causem ou contribuam para o incidente, uma vez que o incidente foi tratado.

d) Aumentar a cultura de segurança da informação na empresa e criar processos formais para lidar com incidentes.

e) Garantir o restabelecimento operacional voltando ao nível de segurança considerado normal antes do incidente.

QUESTÕES

CESPE/2015 - MPOG - Analista em TI

Julgue o seguinte item, relativo à segurança da informação, com base no que dispõem as normas ISO/IEC 27002 e ISO/IEC 27001.

Segundo a ISO/IEC 27001, os controles são classificados em três categorias: obrigatórios, como os documentos da política de segurança da informação; os mandatórios, como os perímetros de segurança física; e os desejáveis, entre os quais se incluem os acordos de confidencialidade.

QUESTÕES

CESPE/2015 - MEC - Administrador de Rede

Julgue o seguinte item, de acordo com o que estabelecem as normas ISO/IEC 27001 e ISO/IEC 27002.

De acordo com a norma ISO/IEC 27002, os controles implementados para a proteção das informações de log devem levar em consideração a capacidade de armazenamento da mídia utilizada para esse fim.

QUESTÕES

CESPE/2015 - MEC - Administrador de Dados

Considerando as normas ISO/IEC 27001, ISO/IEC 27002 e IN MPOG n.º 04/2014, julgue o item subsequente.

De acordo com a norma ISO/IEC 27001, as informações publicamente disponíveis no sítio do MEC requerem mecanismos de proteção para sua visualização e modificação.

QUESTÕES

ITNERANTE/2015

Considerando as normas ISO/IEC 27001 e ISO/IEC 27002, julgue o item subsequente.

A seção 18, que trada da Conformidade, possui controles que dizem respeito à conformidade com leis e regulamentos. Se encaixa neste contexto, inclusive, a conformidade dos controles com as políticas de segurança da informação e com outras políticas subsidiárias da organização, mas não questões mais técnicas, uma vez que isso é tratado em outros controles.

QUESTÕES

CESPE/2015 - TCE-RN - Assessor Técnico de Informática - Cargo 1

Julgue o item a seguir, acerca de gestão de segurança da informação à luz das normas ISO/IEC 27001 e 27002.

Um dos objetivos das auditorias internas do SGSI é determinar se seus controles são executados conforme esperado.

QUESTÕES - Gabarito

FCC/2015 - TCM-GO – Alternativa E
ITNERANTE/2015 – ERRADO
TIMASTERS/2015 – Alternativa E
CESPE/2015 – MPOG – CORRETO (**p/ mim, ERRADO**)
CESPE/2015 – MEC – CORRETO
CESPE/2015 – MEC – CORRETO
ITNERANTE/2015 – ERRADO
CESPE/2015 - TCE-RN – CORRETO