TECNOLOGIA DA INFORMAÇÃO

Segurança da Informação – Parte III

Livro Eletrônico

GRAN CURSOS ONLINE

SUMÁRIO

Apresentação

Saudações caro (a) amigo(a),

Hoje veremos uma série de conceitos e questões **relacionados à Auditoria, à Conformidade e à Continuidade de negócio**, com foco nos aspectos da **Norma ABNT NBR ISO/IEC 15999: 2007** (cobrada ainda em algumas provas, mas já cancelada pela ABNT), que foi substituída pela **ABNT NBR ISO/IEC 22301**

Aos estudos com toda a garra e dedicação!

Em caso de dúvidas, acesse o fórum do curso ou entre em contato.

Um forte abraço!

Profª Patrícia Quintão
Instagram: @coachpatriciaquintao
WhatsApp: (31) 99442.0615

SEGURANÇA DA INFORMAÇÃO – PARTE III

Norma ABNT NBR ISO/IEC 15999:2007

A **norma NBR ISO/IEC 15999** estabelece o **processo**, os **princípios** e a **terminologia para a Gestão da Continuidade de Negócios (GCN).**

O propósito dessa norma é fornecer uma base para que se possa **entender, desenvolver e implementar a continuidade de negócios em uma empresa**, além de obter a confiança nos negócios desta com clientes e outras instituições. Ela **permite também que a organização possa avaliar a sua capacidade de GCN de uma maneira consistente e reconhecida**.

A **NBR ISO/IEC 15999** é baseada na norma britânica BSI 25999:2006 e é dividida em duas partes:

- **15999-1 – Código de prática, que apresenta recomendações para o estabelecimento da GCN** (**Cancelada** em 05/10/2015, substituída pela: ABNT NBR ISO 22313:2015).
- **15999-2 – Requisitos, que estabelece os requisitos para estabelecer e gerir um sistema de GCN (SGCN)** (**Cancelada** em 06/06/2013, substituída pela ABNT NBR ISO 22301:2013).

A figura seguinte destaca o **ciclo de vida da Gestão de Continuidade de Negócios**, composto por 6 elementos:

- **1.Gestão do programa de CGN;**
- **2.Entendendo a organização;**
- **3.Determinando a estratégia de continuidade de negócios;**
- **4.Desenvolvendo e implementando uma resposta de GCN;**
- **5.Testanto, mantendo e analisando criticamente os preparativos de GCN;**
- **6.Incluindo a GCN na cultura da organização.**

Figura. Ciclo de vida da Gestão de Continuidade de Negócios.
Fonte: (ABNT NBR ISO/IEC 15999-1:2007, p. 08)

A **continuidade do negócio** é disciplina fundamental para garantir a perenidade das empresas em momentos de crise, e, neste capítulo veremos o seu conceito e formas de implantação.

Direto do Concurso

001. (FCC/INFRAERO/ANALISTA DE REDES E COMUNICAÇÃO DE DADOS/2011) Um plano de contingência se situa no contexto dos resultados da criação de uma estrutura de gestão e numa estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação de negócios que detalhem os passos a serem tomados durante e após um incidente para manter ou restaurar as operações.
No ciclo de vida da Gestão de Continuidade de Negócio, tal afirmação está associada ao elemento:

a) Desenvolvendo e implementando uma resposta de GCN.
b) Entendendo a organização.
c) Determinando a estratégia de continuidade de negócios.
d) Testando, mantendo e analisando criticamente os preparativos de GCN.
e) Incluindo a GCN na cultura da organização.

O **ciclo de vida de GCN** é composto por 6 elementos, que podem ser visualizados na figura seguinte:

- **1.Gestão do programa de CGN;**
- **2.Entendendo a organização;**
- **3.Determinando a estratégia de continuidade de negócios;**
- **4.Desenvolvendo e implementando uma resposta de GCN;**
- **5.Testanto, mantendo e analisando criticamente os preparativos de GCN;**
- **6.Incluindo a GCN na cultura da organização**.

Figura. Ciclo de vida da Gestão de Continuidade de Negócios. Fonte: (ABNT NBR ISO/IEC 15999-1:2007, p. 08)

Na etapa 4, conforme destaca a **ABNT NBR 15999-1:2007**, é criada uma estrutura de gestão e uma estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação de negócios que detalham os passos a serem tomados durante e após um incidente, para manter ou restaurar as operações.

Letra a.

A seguir, disponibilizamos um quadro resumo sobre **tipos** e **métodos** **de teste de estratégias de Gestão de Continuidade de Negócios (GCN),** conforme destacado na ABNT NBR 15999-1:2007, p. 35.

Complexidade	Teste	Processo	Variações	Freqüência recomendada [a]
Simples	Testes-de-mesa	Análise crítica/correção Questionar conteúdo do PCN	Atualização/Validação Auditoria/Verificação	Ao menos anualmente Anualmente
	"Walk-through" (repassar os passos) do plano	Questionar o conteúdo do PCN	Incluir interação e validar papéis dos participantes	Anualmente
Médio	Simulação	Usar situação "artificial" para validar se os PCN possuem as informações necessárias e suficientes, de forma a permitir uma recuperação com sucesso	Incorporar planos associados	Anualmente ou duas vezes ao ano
	Testar atividades críticas	Execução em ambiente controlado que não prejudique o andamento normal dos negócios	Executar algumas operações a partir de um local alternativo por um tempo determinado	Anualmente ou menos
Complexo	Testar todo o PCN, incluindo o gerenciamento de incidentes	Teste que envolve todo o prédio/campus/zona de exclusão		Anualmente

[a] Convém que a freqüência dos testes dependa das necessidades da organização, do ambiente no qual ela opera e das necessidades das partes interessadas. Porém, convém que o programa de testes seja flexível, levando em conta a freqüência de ocorrência de mudanças na organização e o resultado dos testes anteriores. Os métodos de teste acima podem ser empregados para cada componente de um plano ou para um ou mais planos.

Segundo a NBR 15999-1:2007, p. 34, os **testes** devem ser realistas, planejados cuidadosamente e acordados com as partes interessadas, de modo que haja um risco mínimo de interrupção dos processos de negócio, e de forma a minimizar a chance de que ocorra um incidente como resultado direto do teste.

Todo teste deve ter objetivos claramente definidos.

Direto do Concurso

002. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO/TI/ARQUITETURA DE SOLUÇÕES/2009) Testes de mesa, testes de recuperação em local alternativo e ensaio geral são técnicas que podem ser empregadas na gestão da continuidade de negócios, conforme prescrição na norma ABNT NBR ISO/IEC 17799:2005.

Conforme prescrito na norma ABNT NBR ISO/IEC 17799:2005 (renomeada para 27002) os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Nesse contexto diversas técnicas devem ser usadas para fornecer garantia de que os planos funcionarão na vida real, como as listadas a seguir:

a) **testes de mesa** (faz-se a leitura em conjunto dos procedimentos de um grupo/equipe discutindo os arranjos para recuperação);

b) **simulações** (particularmente para treinar pessoas em seus papéis de gerenciamento pós-incidente/crise);

c) **testes da recuperação técnica** (garantindo que os sistemas de informação podem ser restaurados eficientemente);

d) **testar recuperação em um site alternativo** (executando processos do negócio em paralelo com operações de recuperação longe do site principal);

e) **testes das facilidades e serviços de fornecimento** (garantindo que serviços e produtos providos externamente satisfarão o compromisso contratado);

f) **ensaios completos** (testando se a organização, pessoal, equipamento, facilidades e processos conseguem lidar com interrupções).

Segundo a ISO/IEC 17799:2005, as técnicas podem ser usadas por qualquer organização e devem refletir a natureza do plano de recuperação específico.

A seguir, disponibilizamos um quadro resumo sobre **tipos e métodos de teste de estratégias de Gestão de Continuidade de Negócios (GCN), conforme destacado na ABNT NBR 15999-1:2007, p. 35.**

Complexidade	Teste	Processo	Variações	Freqüência recomendada [a]
Simples	Testes-de-mesa	Análise crítica/correção Questionar conteúdo do PCN	Atualização/Validação Auditoria/Verificação	Ao menos anualmente Anualmente
	"Walk-through" (repassar os passos) do plano	Questionar o conteúdo do PCN	Incluir interação e validar papéis dos participantes	Anualmente
Médio	Simulação	Usar situação "artificial" para validar se os PCN possuem as informações necessárias e suficientes, de forma a permitir uma recuperação com sucesso	Incorporar planos associados	Anualmente ou duas vezes ao ano
	Testar atividades críticas	Execução em ambiente controlado que não prejudique o andamento normal dos negócios	Executar algumas operações a partir de um local alternativo por um tempo determinado	Anualmente ou menos
Complexo	Testar todo o PCN, incluindo o gerenciamento de incidentes	Teste que envolve todo o prédio/campus/zona de exclusão		Anualmente

[a] Convém que a freqüência dos testes dependa das necessidades da organização, do ambiente no qual ela opera e das necessidades das partes interessadas. Porém, convém que o programa de testes seja flexível, levando em conta a freqüência de ocorrência de mudanças na organização e o resultado dos testes anteriores. Os métodos de teste acima podem ser empregados para cada componente de um plano ou para um ou mais planos.

Segundo a NBR 15999-1:2007, p. 34, **os testes devem ser realistas, planejados cuidadosamente e acordados com as partes interessadas, de modo que haja um risco mínimo de interrupção dos processos de negócio**, e **de forma a minimizar a chance de que ocorra um incidente como resultado direto do teste**.

Todo teste deve ter objetivos claramente definidos. Relatórios e análises que demonstrem se os objetivos do teste foram alcançados devem ser elaborados após o teste. Além disso, é importante que seja elaborado um relatório pós-teste, que contenha recomendações juntamente de uma previsão de tempo para a implementação destas.

A escala e a complexidade dos testes devem ser apropriadas aos objetivos de recuperação da organização. O programa de testes deve considerar o papel de todas as partes envolvidas, inclusive principais fornecedores, parceiros terceirizados e outros que poderiam participar das atividades de recuperação. A organização deve incluí-los nos testes.

Certo.

ASPECTOS DA ABNT NBR ISO/IEC 22301: 2013 (SUBSTITUTA DA ABNT NBR ISO/IEC 15999-2)

A norma ABNT NBR ISO/IEC 22301:2013, intitulada: "Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios – Requisitos" especifica requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um eficaz Sistema de Gestão de Continuidade de Negócios (SGCN).

Os **requisitos** especificados nessa norma são **genéricos** e planejados para serem aplicados a **todos os tipos e tamanhos de organizações ou parte delas**.

Essa norma adota o modelo "Plan-Do-Check-Act" (PDCA) para **planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente** a eficácia do **SGCN** de uma **organização**.

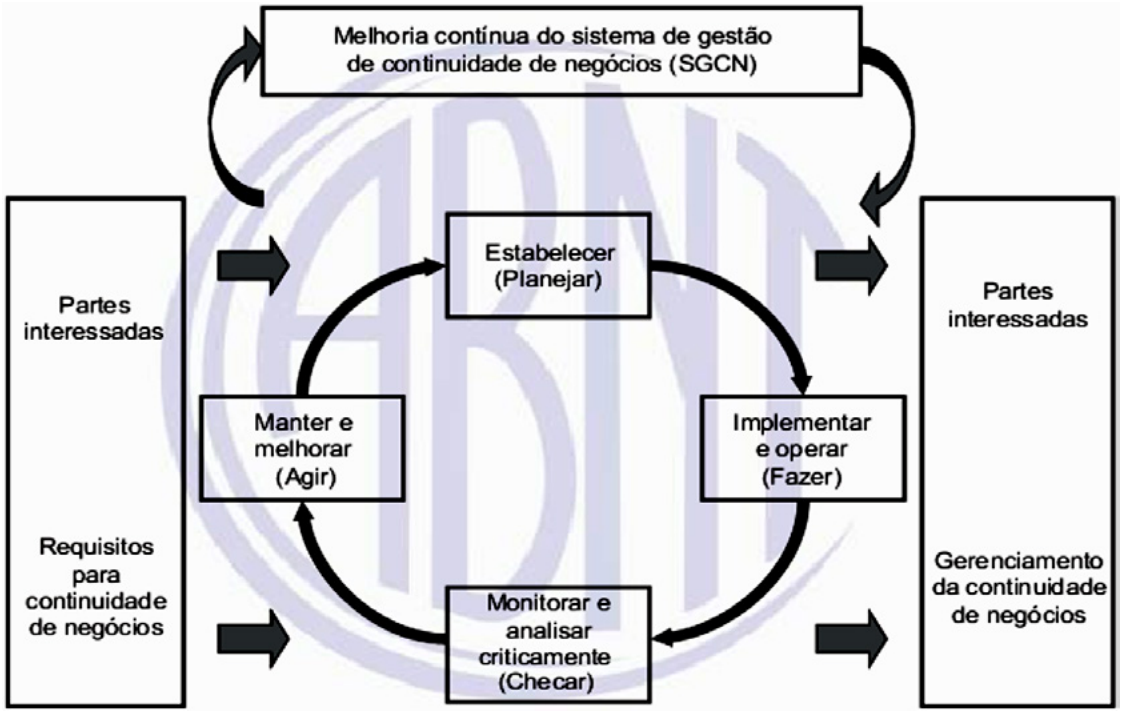


Figura – Modelo PDCA Aplicado aos Processos do SGCN (ABNT NBR ISO 22301:2013)

A figura anterior destaca que **um SGCN considera como entradas as partes interessadas e os requisitos de continuidade de negócios e, por meio de ações necessárias e processos, produz resultados de continuidade (por exemplo, continuidade de negócios gerenciada) que atendem àqueles requisitos.**

Plan (Estabelecer)	Estabelecer uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos e políticas gerais da organização.
Do (Implementar e operar)	Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.
Check (Monitorar e analisar criticamente)	Monitorar e analisar criticamente o desempenho em relação aos objetivos e à política de continuidade de negócios, reportar os resultados à direção para análise crítica e definir e autorizar ações de melhorias e correções.
Act (Manter e melhorar)	Manter e melhorar o SGCN, tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica pela Direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

Figura – Explicação do Modelo PDCA, conforme (ABNT NBR ISO 22301:2013)

A organização deve estabelecer **procedimentos documentados** **para responder a incidentes de interrupção**, **e como irá continuar ou recuperar suas atividades dentro de um prazo predefinido**. Tais procedimentos devem atender aos requisitos de quem irá usá-lo.

Principais Termos e Definições Referenciados na Norma ABNT NBR ISO/IEC 22301:2013

Atividade

- **Processo ou conjunto de processos executados por uma organização (ou em seu nome) que produzem ou suportem um ou mais produtos ou serviços.**

Continuidade de Negócios

- **Capacidade da organização em continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidentes de interrupção.**

Gestão de Continuidade de Negócios

- **Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem.**
- **Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado.**

Sistema de Gestão de Continuidade de Negócios – SGCN

- **Parte do sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantem e melhora a continuidade de negócios.**

Plano de Continuidade de Negócios

- **Procedimentos documentados que orientam as organizações a responder, recuperar, retomar e restaurar a um nível predefinido de operação após interrupção.**

Direto do Concurso

003. (FCC/2016/PREFEITURA DE TERESINA-PI/ANALISTA TECNOLÓGICO/ANALISTA DE NEGÓCIOS) Um dos objetivos principais da Gestão de Continuidade de Negócios é

a) promover avaliação de desempenho dos responsáveis pela organização.

b) identificar as ameaças à organização e seus impactos, bem como prover resiliência a tais ameaças.

c) realizar um estudo para contenção dos gastos da organização.

d) promover um ambiente harmonioso entre os funcionários da organização.

e) substituir o parque computacional da organização a cada 2 anos.

Conforme destaca ABNT NBR ISO/IEC 22301:2013, a Gestão de continuidade de negócios é o **processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem.**

Esse processo fornece uma estrutura para que se desenvolva uma **resiliência organizacional** que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

Letra b.

Planos de Continuidade de Negócios (PCN)

Os **planos de continuidade de negócios devem** coletivamente **conter**:

- **Papéis e responsabilidades** definidos para pessoas e equipes com autoridade durante e após um incidente;
- Um **processo** para ativar a estrutura de **resposta a incidentes**;
- Detalhes para **gerenciar os impactos imediatos** de um incidente de interrupção, dando a devida atenção a:
  - bem-estar dos colaboradores;

  - alternativas estratégicas, táticas e operacionais para responder à interrupção; e
  - prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
- Detalhes sobre **como e em que circunstâncias a organização irá se comunicar com os funcionários e seus familiares**, os principais interessados e contatos de emergência;
- **Como** a organização vai **continuar ou recuperar suas atividades prioritárias dentro de prazos predefinidos**;
- Detalhes de resposta após incidente da organização **à mídia**, incluindo:
  - a estratégia de comunicação;
  - meio de comunicação preferido;
  - diretriz ou modelo para a elaboração de uma declaração para a mídia; e
  - porta-voz apropriado;
- Um processo para **retorno à normalidade** quando o incidente terminar.

Cada plano deve definir:

- **propósito e escopo;**
- **objetivos;**
- **critérios e procedimentos para sua ativação;**
- **procedimentos de implementação;**
- **papéis, responsabilidades e autoridades;**
- **requisitos e procedimentos de comunicação;**
- **interdependências internas, externas e suas interações;**
- **recursos necessários; e**
- **fluxo de informações e processos documentados.**

O **Plano de Continuidade de Negócios (PCN)** estabelece critérios para prover a continuidade de negócios organizacionais **em momento de crise**.

Em suma, o PCN tem como **finalidade** central criar normas e padrões para que, em situações adversas, **as empresas possam recuperar, retomar e dar prosseguimento aos seus mais cruciais processos de negócio**, evitando que eles sofram danos mais profundos que provoquem perdas financeiras.

Três pilares são essenciais ao **elaborar o Plano de Continuidade de Negócios (PCN):**
1) Análise de risco: o que de ruim pode vir a acontecer? Ou seja, quais as principais ameaças;
2) Análise de impacto: de que forma eventuais ameaças podem impactar o negócio da organizacão? ; e
3)Planejamento Estratégico: Se uma ameaça se apresentar, quais atitudes e ações se fariam necessárias para a retomada das operações da empresa?

Sob o ponto de vista do PCN, o funcionamento de uma empresa **deve-se, fundamentalmente, a duas variáveis**:

- 1. **processos**: as **atividades** realizadas para operar os negócios da empresa;
- 2. **componentes**: todas as variáveis utilizadas para realização dos processos: **energia** (Operadoras fornecedoras de energia elétrica), **telecomunicações** (empresas que fornecem comunicação usando dados e voz), **infraestrutura** (localização, para-raios, instalações elétricas, segurança física etc.), **pessoas** (Contingência das atividades e atendimento através de Sites Remotos etc.); **informática** (Equipamentos, Sistemas, Conectividade etc.).

O PCN é estruturado em **quatro subplanos** menores ligados entre si, e cada qual para um estágio diferente. São eles:

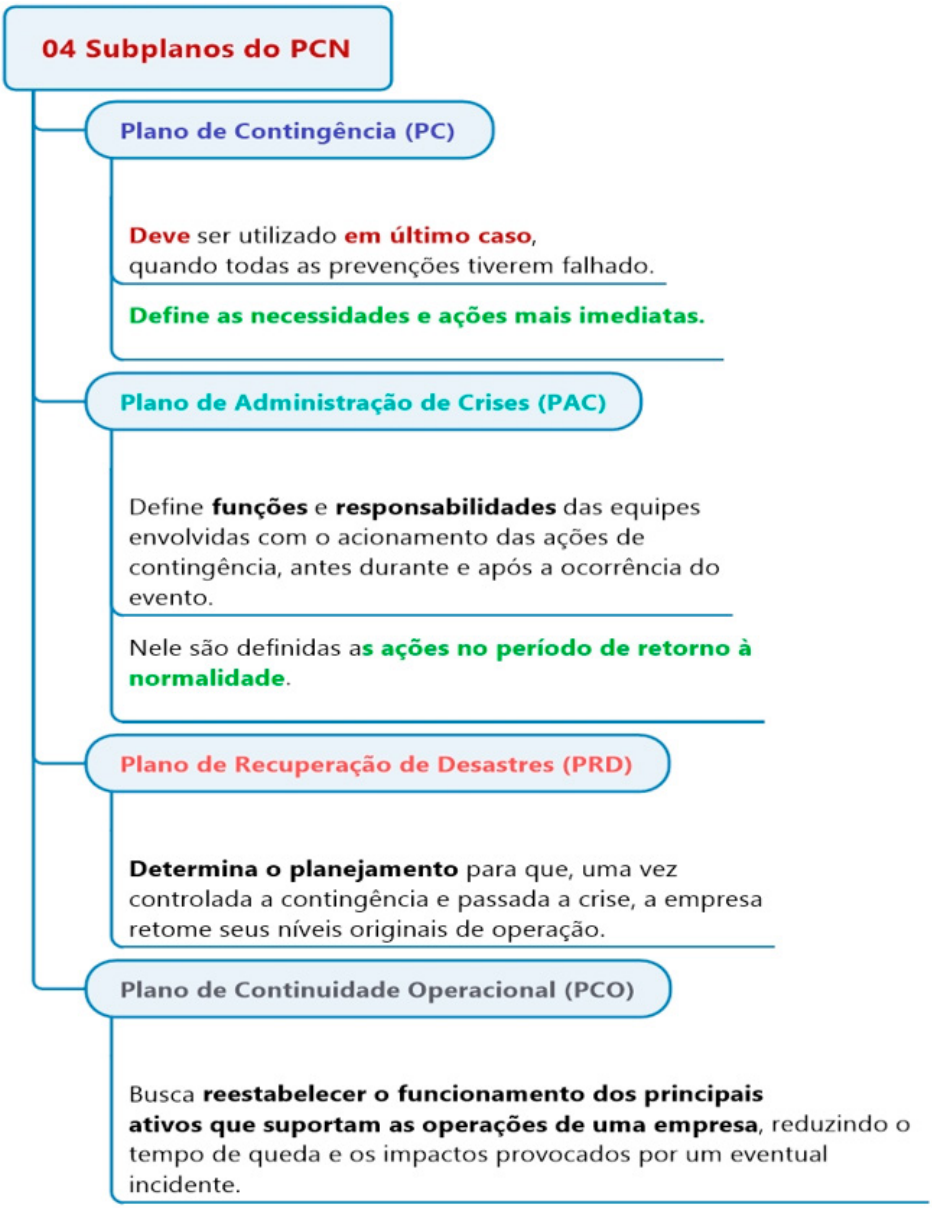


Figura – Subplanos do PCN. Fonte: QUINTÃO (2021)

Direto do Concurso

004. (FCC/2018/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA) Estabelecer um plano de continuidade de negócios é primordial para as empresas, sendo que o plano de continuidade é constituído de subplanos. O subplano estabelecido para ser utilizado em último caso quando todas as prevenções tiverem falhado é conhecido como Plano de

a) Gerenciamento de Crises.
b) Contingência.
c) Recuperação de Desastres.
d) Administração.
e) Continuidade Operacional.

Um **Plano de Continuidade de Negócios** pode ser estruturado em **quatro outros planos ligados entre si**, cada qual criado para cuidar de um estágio diferente**. São eles:**

- **1.Plano de Contingência ou Emergência (PC): deve ser utilizado em último caso,** quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas;
- **2.Plano de Administração ou Gerenciamento de Crises (PAC)**: define **funções** e **responsabilidades** das equipes envolvidas com o acionamento das ações de contingência, **antes durante e após a ocorrência;**
- **3.Plano de Continuidade Operacional (PCO)**: seu objetivo é **reestabelecer o funcionamento dos principais ativos** que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet;
- **4.Plano de Recuperação de Desastres (PRD)**: determina o **planejamento** para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.

Letra b.

O **planejamento de continuidade do negócio** deve ter como preocupação principal a **delimitação de escopo**. Algumas observações:

- É **errado** imaginar que teremos toda a organização protegida por um **plano de continuidade do negócio**, pois **existem processos em que a tolerância à falha é tão grande que implantar controles de redundância e recuperação poderiam ser maiores financeiramente do que simplesmente aceitar o serviço parado;**
- Mas, existem processos de negócio que quando paralisados podem colocar em risco a receita e a imagem da empresa, são estes os processos que requerem mais atenção.

Além da **definição do escopo**, existem uma **série de etapas que devem ser discutidas e determinadas**, de forma macro, para posterior detalhamento no decorrer dos trabalhos. Uma boa forma de implantar a **continuidade do negócio** consiste em seguir o **processo** descrito no livro *CISSP All-In-one,* conforme figura aqui destacada. Detalharemos os principais pontos que devem ser considerados no PCN: a **Análise de Impacto no negócio ou BIA (*Business Impact Analysis*)** e a **implantação e testes**.

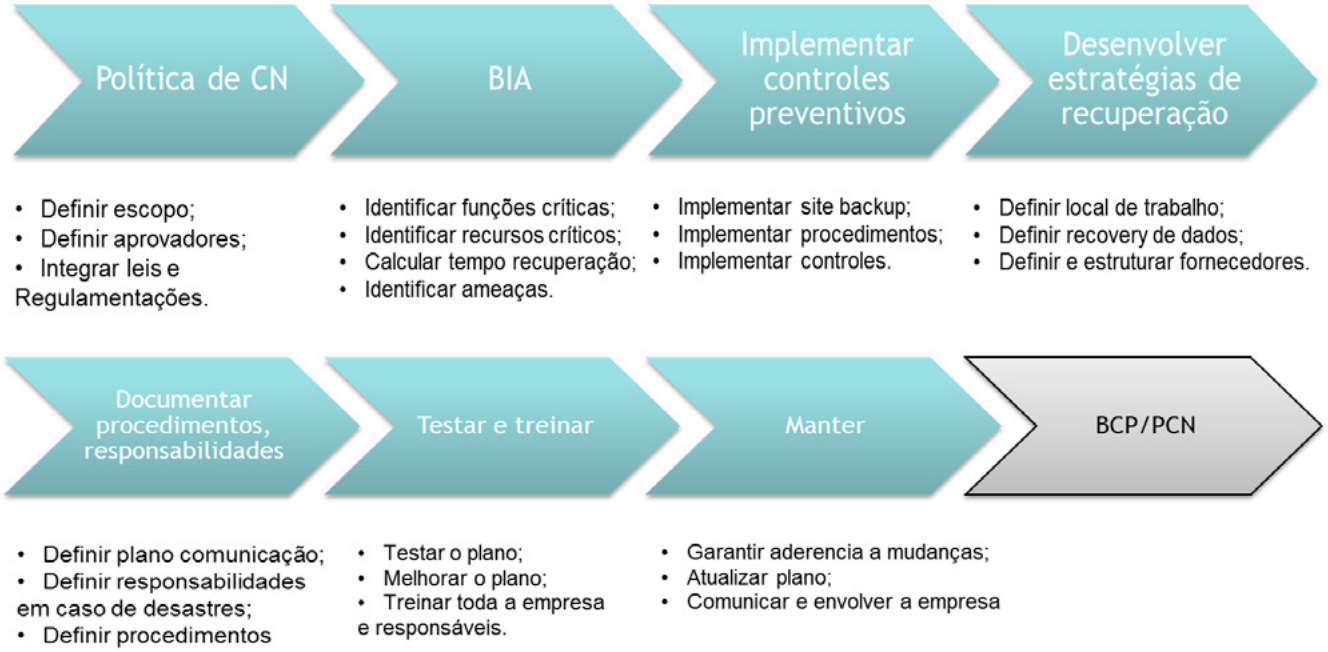


Figura – Processo de Continuidade do Negócio

Análise de Análise de Impacto de Negócio – BIA

A **Análise de Impacto no Negócio ou BIA (*Business Impact Analysis*)** é o processo no qual se identifica e prioriza os incidentes que podem ter potencial de perda financeira, de imagem ou regulatório em uma empresa.

O BIA, usualmente tem uma **abordagem *top-down***, em que uma reunião é feita com o *board,* e esse sinaliza quais são **os processos mais críticos dentro da empresa**, do ponto de vista de paralisação, seja por uma falha humana, tecnológica ou natural.

Tendo sido realizada esta identificação, o processo se desdobra com **entrevistas** realizadas com os donos de cada processo na empresa.

Os **resultados** esperados com a aplicação do **BIA**:

- **compreensão dos processos negócio e atividades**, contemplando os clientes (internos e externos), saídas e entregas, entradas (que permitem que o processo funcione, incluindo recursos e outras dependências de terceiros);
- compreender uma **estimativa do impacto do tempo de inatividade**, o que serve como justificativa de negócios para estabelecer objetivos de recuperação;

- **identificação dos objetivos de recuperação e de prioridades de recuperação** para os processos e recursos de negócios;
- **coleta de informações** que podem ajudar a identificar estratégias apropriadas de recuperação e documentar planos para o futuro.

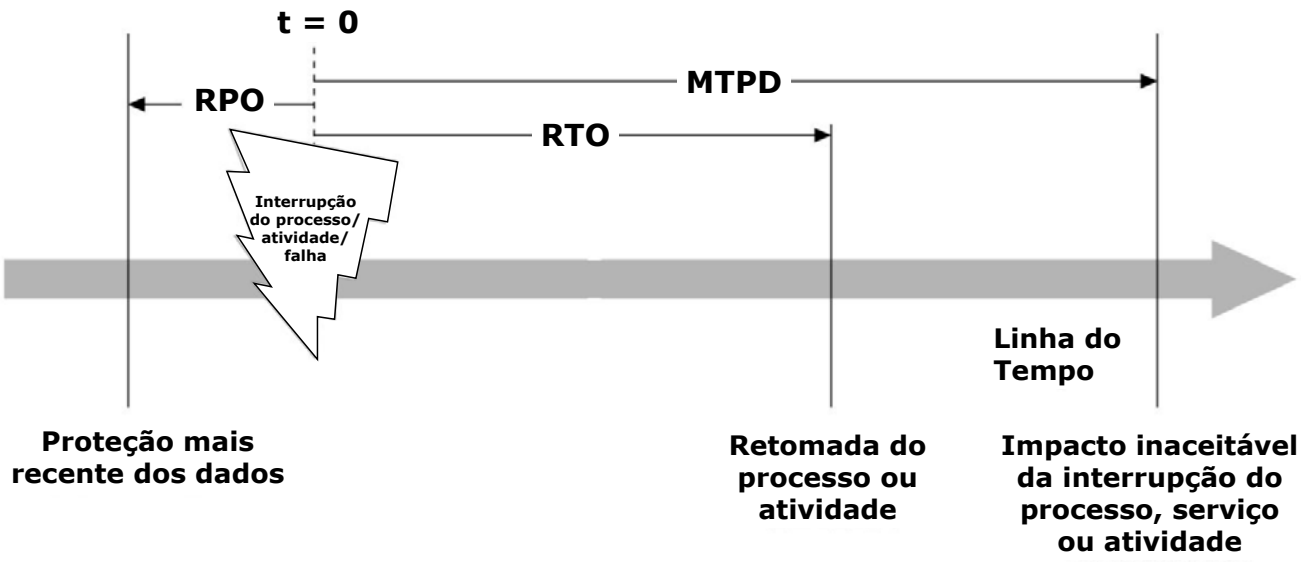


Figura – Relação Temporal entre RPO, RTO e MTPD. Fonte: Gomes (2015)

Após a **BIA**, a organização deve ser capaz de identificar as **atividades críticas** que contribuem para a entrega de seus mais importantes produtos e serviços, a lista de todos os **recursos** necessários para a recuperação, e **priorizar atividades e recursos** por objetivo à recuperação.

Existem diversos modelos de **matriz** para identificação e classificação dos potenciais eventos, usualmente, uma **planilha de BIA tem minimamente** as seguintes informações:

Processo de negócio	Evento	Dano potencial (por dia)	Probabilidade	RPO	RTO	MTPD
Atendimento ao cliente	Paralisação do sistema	R$ 10.000,00	Alta	1 dia	1 dia	1 dia
Atendimento ao cliente	Greve de ônibus/ metrô	R$ 10.000,00	Baixa	1 dia	1 dia	1 dia
Vendas	Paralisação do sistema	R$ 5.000,00	Baixa	2 dias	2 dias	2 dias
Faturamento	Paralisação do sistema	R$ 30.000,00	Baixa	5 dias	7 dias	8 dias

*Figura– Matriz BIA (***Business Impact Analysis***)*

O que vale destacar nesse exemplo é que o **processo de faturamento**, embora tenha o **dano potencial** (prejuízo estimado) diário de R$30.000,00, pode suportar até 5 dias (**R.P.O**) de dados perdidos, pode tolerar até 7 dias de recuperação do que é crítico (**R.T.O**) e pode tolerar até 8 dias para recuperação plena (**M.T.P.D.**) do sistema.
Isso pois, no exemplo hipotético acima, esta empresa fatura dos seus clientes a cada período de 10 dias e, portanto, 8 dias seria o período máximo que ela poderia tolerar até colocar suas informações em dia para faturar os clientes.

Direto do Concurso

005. (FCC/2018/PREFEITURA DE SÃO LUÍS-MA/AUDITOR-FISCAL DE TRIBUTOS I/ TECNOLOGIA DA INFORMAÇÃO/TI) Considere, por hipótese, que um incêndio danificou um servidor da Prefeitura e um Auditor foi acionado para restaurar um backup completo do que havia em uma fita em um novo servidor. Apesar de o Auditor ter levado cerca de 30 minutos para restaurar os dados do backup, o total de tempo entre a notificação da interrupção dos serviços dependentes dos dados do servidor danificado, a recuperação total dos dados e a restauração dos serviços foi de aproximadamente 50 minutos, dentro do tempo tolerável previsto no Plano de Recuperação de Desastres associado ao Plano de Continuidade de Negócio.
Este limite de tempo é conhecido como
a) Recovery Time Point (RTP).
b) Business Process Recovery Objective (BPRO).
c) Recovery Point Objective (RPO).
d) Business Recovery Time (BRT).
e) Recovery Time Objective (RTO).

Itens A, B e D, errados. Nomenclaturas inexistentes no cenário de um PCN.
Item C, errado. **RPO (Ponto Objetivado de Recuperação – *Recovery Point Objective*)** é o tempo MÁXIMO que podemos ficar paralisados (perdendo dados), até que se atinja um nível muito crítico para o negócio.
Item E, correto. A banca destacou o seguinte: "o total de tempo entre a notificação da interrupção dos serviços dependentes dos dados do servidor danificado, a recuperação total dos dados e a restauração dos serviços foi de aproximadamente 50 minutos, **dentro do tempo tolerável previsto** (...)".
Nesse ponto, cabe destacar que esse **período de tempo que uma atividade ou processo deve ser retomada após uma interrupção** é o **Tempo Objetivado de Recuperação (RTO – *Recovery Time Objective*).** Em outras palavras, **RTO** é o tempo entre o incidente e o tempo para restaurar o que é crítico para o negócio.
Letra e.

Implantação, Testes e Acompanhamento

Feito o BIA (***Business Impact Analysis)***, um **parecer executivo** é apresentado para o *board* da empresa e neste **decide-se em quais processos deve haver investimento para reduzir o impacto de uma paralisação**.

No exemplo aqui destacado, vamos tomar o incidente "Paralisação do sistema de atendimento ao cliente" como o mais crítico, haja visto que a probabilidade de acontecimentos é alta (possivelmente pois o sistema não possui as proteções necessárias) e a tolerância a paralisação é pequena (1 dia).
Parte-se então para o estudo dos investimentos necessários para reduzir o tempo de falha, neste caso, estudos de redundância de servidores, *site backup,* tempo de armazenamento de dados e muitas outras variáveis podem ser implantadas. Este levantamento gera um **plano de ação** que deve ser então implantando.

Finalizada a implantação, devemos realizar os testes, que são fundamentais para que se coloque a prova tudo aquilo que foi feito. Os **testes** devem ser os mais profundos possíveis, assim, se for possível paralisar todo o sistema, simulando uma falha de *hardware* ou *software* é o mais adequado. Lembrando que os testes são um conjunto de procedimentos que devem ser seguidos de forma a garantir o R.P.O, R.T.O e M.T.P.D. **Os testes nos ensinam muito sobre o que foi planejado e executado e onde há falhas.**

É fundamental que o **plano de continuidade de negócios, seja revisitado a cada ano, ou em outro período que a organização entender,** baseado em suas mudanças recentes. Isso garante que a organização estará preparada em caso de incidentes que a coloquem entre a continuidade ou não de suas operações.

Aplicação da Continuidade de Negócio

A aplicação da Continuidade de Negócio torna-se tarefa essencial para as organizações que se apresentam em constante movimentação. Uma interrupção pode gerar prejuízos para as organizações e estes podem ser muito elevados e seguramente superiores aos custos de implementação de um Plano de Continuidade de Negócios.

Um bom **plano de Continuidade de Negócio** é aquele que permite que as organizações estejam seguras, em sua completude e que os custos sejam compatíveis e menores com os impactos possíveis.

Direto do Concurso

006. (FCC/2017/DPE-RS/ANALISTA/SEGURANÇA DA INFORMAÇÃO) O Plano de Continuidade dos Negócios é um roteiro de operações contínuas para quando as operações normais dos negócios são interrompidas por condições adversas.

O Plano de Continuidade dos Negócios

a) deve incluir, dentre outras coisas, a definição dos cenários de impacto e a análise de ameaças e riscos.

b) deve ser de responsabilidade do departamento de TI, que é considerado o único com competências necessárias para conter possíveis desastres.

c) também é conhecido como Plano de Recuperação de Desastres, uma vez que inclui ações para retornar a organização a seus níveis originais de operação.

d) deve possuir ações genéricas para conter qualquer tipo de desastre, evitando assim que tenha que ser revisado periodicamente.

e) deve ser executado integralmente em resposta a incidentes que causem interrupção total ou parcial das operações normais de negócios.

a) Certa**. Três pilares são essenciais ao elaborar o Plano de Continuidade de Negócios (PCN):**

- **1) Análise de risco:** o que de ruim pode vir a acontecer? Ou seja, quais as principais ameaças;
- **2) Análise de impacto:** de que forma eventuais ameaças podem impactar o negócio da organizacão?**;** e
- **3) Planejamento Estratégico:** Se uma ameaça se apresentar, quais atitudes e ações se fariam necessárias para a retomada das operações da empresa?

b) Errada. A **responsabilidade pela implementação** do **PCN** é dos **dirigentes da organizaçã**o. A equipe de gerência da segurança pode auxiliar nessa tarefa, na criação, manutenção, divulgação e coordenação do plano de contingências.

c) Errada. O Plano de Recuperação de Desastres (PRD) é um dos subplanos do PCN, e não sinônimo dele.

d) Errada. O **Plano de Continuidade de Negócios** deve ser **revisado periodicamente**, porque mudanças significativas em componentes, atividades ou processos críticos de negócio podem fazer com que novas estratégias e planos de ação sejam previstos.

e) Errada**.** O **Plano de Continuidade de Negócios** não deve sempre ser executado integralmente, podendo ser executado também parcialmente.

Letra a.

Avaliação dos Procedimentos de Continuidade dos Negócios

- A organização deve **conduzir avaliações de seus procedimentos e capacidades de continuidade dos negócios** de forma a assegurar sua contínua aptidão, adequação e eficácia;
- Essas avaliações devem ser realizadas através de **análises críticas periódicas**, exercícios, testes, relatórios pós-incidente e avaliações de desempenho. Mudanças significativas decorrentes devem ser refletidas nos procedimentos em tempo hábil;

- A organização deve avaliar **periodicamente** a **conformidade com requisitos legais e regulatórios, com suas melhores práticas, com seus objetivos e com a política de continuidade dos negócios**; e
- A organização deve conduzir avaliações em intervalos planejados e quando mudanças significantes ocorrerem.
- Quando um incidente que cause interrupção e resulte na ativação dos seus procedimentos de continuidade dos negócios ocorre, a organização deve realizar **uma análise crítica pós-incidente** e registrar os resultados.

Auditoria Interna

A organização deve conduzir **auditorias internas em intervalos planejados** para prover informações sobre se o sistema de gestão de continuidade dos negócios

- Está em conformidade :
  - com os requisitos próprios da organização para SGCN;
  - com os requisitos desta Norma e;
- Está implementado e mantido eficazmente.

A **organização deve**:

- planejar, estabelecer implementar e manter um **programa de auditoria**, inclusive frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. O programa de auditoria deve levar em consideração a importância dos processos relevantes e os resultados das auditorias anteriores;
- definir o critério e o escopo para cada auditoria;
- selecionar auditores e conduzir auditorias para assegurar objetividade e imparcialidade do processo de auditoria;
- assegurar que os resultados das auditorias sejam reportados para a gerência; e
- manter a informação documentada como evidência da implementação do programa de auditoria e seus resultados.

Informações Complementares

- O programa de auditoria, incluindo qualquer cronograma, deve ser baseado nos resultados das atividades do **processo de avaliação de risco da organização** e nos resultados de **auditorias anteriores**.
- Os procedimentos de auditoria devem cobrir o **escopo**, **frequência**, **metodologias** e **competências**, bem como as **responsabilidades** e **requisitos** para a realização de **auditorias** e comunicação dos resultados.

- A gerência responsável pela área sendo auditada deve garantir que quaisquer correções necessárias e ações corretivas sejam realizadas sem demora indevida para eliminar as não conformidades detectadas e suas causas.
- As atividades de acompanhamento devem incluir a verificação das ações realizadas e a comunicação dos resultados.

Análise Crítica pela Direção

A Alta Direção deve analisar criticamente o SGCN da organização, em intervalos planejados, para garantir sua contínua aptidão, adequação e eficácia, considerando:

- O *status* das ações de análises críticas anteriores;
- As mudanças em questões internas e externas que são relevantes para o SGCN;
- Informação do desempenho da continuidade dos negócios, inclusive tendências em:
  - não conformidades e ações corretivas;
  - resultados da avaliação de monitoração e medição; e
  - resultados de auditorias;
- Oportunidade de melhoria contínua.

As **saídas da análise crítica devem incluir decisões relacionadas a oportunidades de melhoria contínua** e a possível necessidade de mudanças do SGCN, tais como:

- variações do escopo do SGCN;
- melhoria da eficácia do SGCN;
- atualização do processo de avaliação de riscos, análise de impacto nos negócios, plano de continuidade dos negócios e processos relacionados;
- modificação de procedimento e controles para responder eventos externos ou internos que possam impactar no SGCN, inclusive mudanças em:
- requisitos operacionais e de negócio;
- condições operacionais e processos;
- requisitos legais, regulatórios e obrigações contratuais; e
- necessidades e requisitos de recursos.
- como a eficácia dos controles é medida.

A organização deve **comunicar os resultados da análise crítica** às partes interessadas, e **realizar ações apropriadas para os resultados**

Melhoria

Quando ocorrer uma não conformidade, a organização deve:

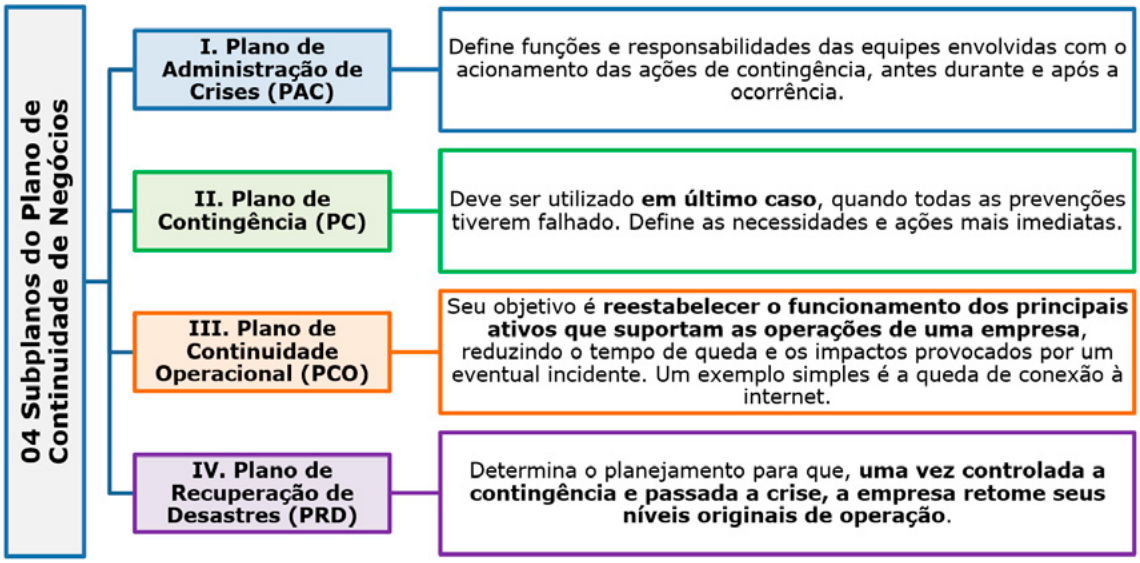
- **Identificar** a não conformidade;
- **Reagir** à não conformidade, e, quando aplicável:

  - tomar ações para contenção e correção; e
  - lidar com as consequências;
- **Avaliar** a necessidade para a eliminação das causas de não conformidades, de modo que não ocorra em outro lugar, através da:
  - análise crítica;
  - determinação das causas;
  - avaliação da necessidade de ações corretivas para que voltem a ocorrer;
  - análise crítica da eficácia de qualquer ação corretiva tomada;
  - mudanças no SGCN, se necessário.

Direto do Concurso

007. (FCC/2018/DPE-AM/ANALISTA EM GESTÃO ESPECIALIZADO DE DEFENSORIA/ ANALISTA DE SISTEMA) Um Plano de Continuidade de Negócios pode ser estruturado em quatro outros planos ligados entre si, cada qual criado para cuidar de um estágio diferente:
I – Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.
II – Deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.
III – Seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.
IV – Determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.
O plano
a) II se refere ao Plano de Gerenciamento de Crises.
b) III se refere ao Plano de Recuperação de Desastres.
c) I se refere ao Plano de Continuidade Operacional.
d) III se refere ao Plano de Contingência.
e) IV se refere ao Plano de Recuperação de Desastres.

O **Plano de Continuidade de Negócios**, via de regra, é estruturado em **quatro subplanos menores. São eles:**



Conforme visto, o item (IV) refere-se ao Plano de Recuperação de Desastres (PRD) e a letra E é a resposta dessa questão.

Letra e.

---

008. (CESPE/2019/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I) Acerca do plano de continuidade de negócios (PCN), assinale a opção correta.

a) Para operacionalizar o PCN de uma empresa que já foi elaborado, é altamente recomendável o desenvolvimento de um sistema de gestão de continuidade de negócios (SGCN).

b) PCN e plano de contingência são sinônimos, uma vez que contemplam os mesmos itens.

c) Os prazos decorrentes de ações realizadas por agentes externos à organização não necessitam ser considerados para elaboração do PCN dessa organização.

d) Na perspectiva do PCN, o funcionamento de uma empresa deve-se, fundamentalmente, às variáveis recursos e pessoas.

e) O PCN estabelece controles de segurança da informação como resultado de uma ampla análise de riscos.

Vamos analisar cada uma das assertivas:

a) Errada. Se o **Plano de Continuidade de Negócios (PCN)** foi elaborado, entende-se que o Sistema de Gestão de Continuidade de Negócios (**SGCN**) já tenha sido desenvolvido. O **SGCN** é **parte do sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantem e melhora a continuidade de negócios.**

b) Errada. PCN e Plano de Contingência são termos distintos! O **Plano de Continuidade de Negócios (PCN)** é estruturado em **quatro subplanos menores, sendo o Plano de Contingência**

(PC) um deles. O PC deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

c) Errada. Os prazos decorrentes de ações realizadas por agentes externos à organização necessitam ser considerados para a elaboração do **Plano de Continuidade de Negócios (PCN)** dessa organização.

d) Errada. Sob o ponto de vista do PCN, o funcionamento de uma empresa **deve-se, fundamentalmente, a duas variáveis**:

- 1. **processos**: as **atividades** realizadas para operar os negócios da empresa;
- 2. **componentes**: todas as variáveis utilizadas para realização dos processos: **energia** (Operadoras fornecedoras de energia elétrica), **telecomunicações** (empresas que fornecem comunicação usando dados e voz), **infraestrutura** (localização, para-raios, instalações elétricas, segurança física etc.), **pessoas** (Contingência das atividades e atendimento através de Sites Remotos etc.); **informática** (Equipamentos, Sistemas, Conectividade etc.).

e) Certa. O **Plano de Continuidade de Negócios (PCN)** estabelece **controles de segurança da informação** tomando-se como base os resultados da análise de impacto nos negócios e do processo de **avaliação de riscos**.

Letra e.

---

009. (CESPE/2012/TJ-AL/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS) No que se refere ao plano de continuidade de negócios, assinale a opção correta.

a) Os objetivos do plano em tela incluem evitar a interrupção das atividades do negócio, proteger os processos críticos contra o acesso de pessoas estranhas ao ambiente e assegurar a retomada dos processos em tempo hábil, caso necessário.

b) A contratação de seguro compatível é desconsiderada na gestão da continuidade do negócio.

c) A existência de um gestor específico para cada plano de continuidade é desvantajoso, visto que causa aumentos significativos dos custos dos planos como um todo.

d) Os planos de continuidade do negócio devem ser testados e atualizados infrequentemente, já que a realização regular dessas ações acarreta o aumento significativo dos custos dos planos.

e) A estrutura de planejamento para continuidade de negócios deve abranger os ativos e os recursos críticos para uma eventual utilização dos procedimentos de emergência, recuperação e ativação.

a) Errada. Deve-se impedir a interrupção das atividades do negócio e proteger os processos críticos **contra efeitos de falhas ou desastres significativos**, e assegurar que a sua retomada ocorra em tempo hábil.

Para isso, planos de continuidade do negócio, incluindo controles para identificar e reduzir riscos, devem ser desenvolvidos e implementados, visando assegurar que as operações essenciais sejam rapidamente recuperadas.

b) Errada. A contratação de seguro compatível **pode ser considerada** na gestão da continuidade do negócio.

c) Errada. A existência de um gestor específico para cada plano de continuidade é vantajosa.

d) Errada. Os planos de continuidade do negócio devem ser testados e atualizados frequentemente.

e) Certa. A estrutura de planejamento para continuidade de negócios deve abranger os **ativos** e os **recursos críticos** para uma eventual utilização dos procedimentos de emergência, recuperação e ativação.

Letra e.

---

010. (FADESP/2018/BANPARÁ/TÉCNICO EM INFORMÁTICA/SUPORTE) O objetivo de um Plano de Continuidade de Negócios (PCN) é garantir que serviços essenciais, por exemplo, de uma empresa sejam devidamente identificados e preservados mesmo após a ocorrência de desastres. Não compõe o PCN o

a) Plano de Contingência (PC).

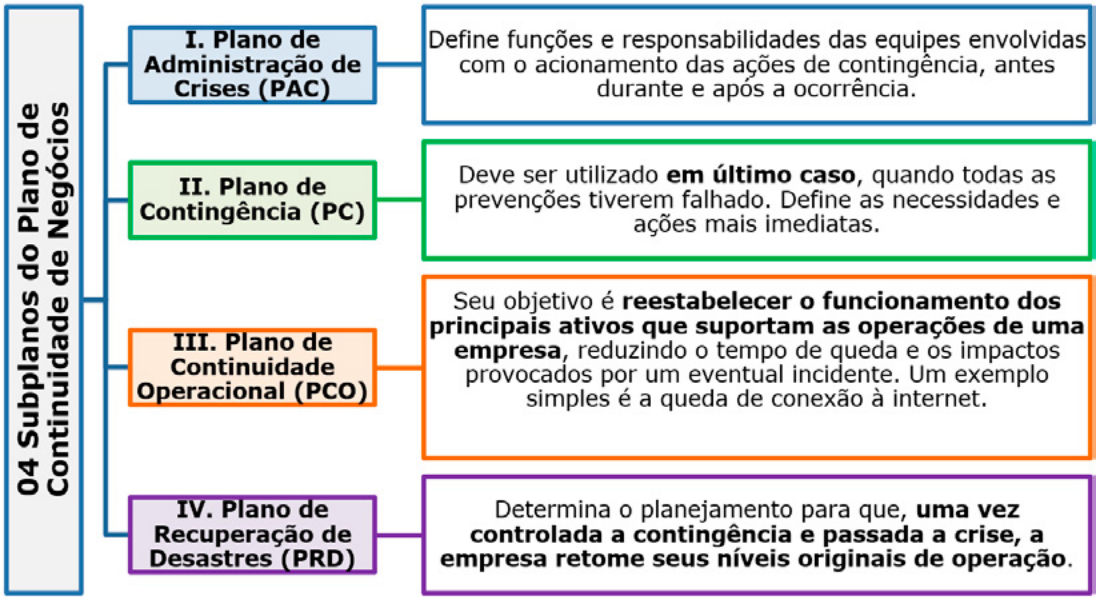
b) Plano de Administração de Crises (PAC).

c) Plano de Recuperação de Desastres (PRD).

d) Plano de Prevenção de Crises (PVC).

e) Plano de Continuidade Operacional (PCO).

O **Plano de Continuidade de Negócios**, geralmente, é estruturado em **quatro subplanos menores**. **São eles:**



Conforme visto, o item (D) – Plano de Prevenção de Crises (PVC) – não existe nesse contexto.

Letra d.

---

011. (FCC/2017/TRT-24ª REGIÃO/MS/TÉCNICO JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO) Considere a lista a seguir:

1. Um processo para ativar a resposta da organização a um incidente de interrupção e, dentro de cada procedimento documentado, seus critérios e procedimentos de ativação.
2. Um processo para desmobilizar equipes após o incidente ter passado.
3. Regras e padrões para proteção das informações, possibilitando manter a confidencialidade, integridade e disponibilidade.
4. Papéis e responsabilidades definidos para pessoas e equipes que usarão o plano.
5. Orientações e critérios sobre quem tem a autoridade de invocar os procedimentos e sob quais circunstâncias.
6. A definição clara de como serão tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários e as informações institucionais.
7. Gestão das consequências imediatas de um incidente de interrupção considerando as questões de bem-estar de pessoas afetadas, as ações para responder a interrupção e prevenção.
8. Detalhes de contato para os membros da equipe e outras pessoas com funções e responsabilidades dentro de cada procedimento.
9. Detalhes indicando como e em que circunstâncias a organização irá se comunicar com os funcionários, com as principais partes interessadas e contatos de emergência.

No Plano de Continuidade de Negócio deve estar claramente identificável o que consta em 1, 2,

a) 3, 4, 5 e 7.
b) 7, 8 e 9.
c) 3, 6 e 8.
d) 3, 4, 5, 6, 7 e 9.
e) 4, 5, 7, 8 e 9.

Os planos de continuidade de negócios devem coletivamente conter:

- **Papéis e responsabilidades** definidos para pessoas e equipes com autoridade durante e após um incidente;
- Um **processo** para ativar a estrutura de **resposta a incidentes**;
- Detalhes para **gerenciar os impactos imediatos** de um incidente de interrupção, dando a devida atenção a:
  - bem-estar dos colaboradores;
  - alternativas estratégicas, táticas e operacionais para responder à interrupção; e
  - prevenção de novas perdas ou indisponibilidade de atividades prioritárias.
- Detalhes sobre como e em que circunstâncias a organização irá se comunicar com os funcionários e seus familiares, os principais interessados e contatos de emergência;

- Como a organização vai continuar ou recuperar suas atividades prioritárias dentro de prazos predefinidos;
- Detalhes de resposta após incidente da organização **à mídia**, incluindo:
  - a estratégia de comunicação;
  - meio de comunicação preferido;
  - diretriz ou modelo para a elaboração de uma declaração para a mídia; e
  - porta-voz apropriado;
- Um processo para **retorno à normalidade** quando o incidente terminar.

Cada plano deve definir:

- **propósito e escopo;**
- **objetivos;**
- **critérios e procedimentos para sua ativação;**
- **procedimentos de implementação;**
- **papéis, responsabilidades e autoridades;**
- **requisitos e procedimentos de comunicação;**
- **interdependências internas, externas e suas interações;**
- **recursos necessários; e**
- **fluxo de informações e processos documentados.**

Conforme visto, no Plano de Continuidade de Negócio deve estar claramente identificável o que consta em 1, 2, 4, 5, 7, 8 e 9. Os itens 3 e 6 não são tratados no PCN e podem ser especificados em outros planos, como a PSI (Política de Segurança da Informação), etc.
Letra e.

---

012. (FCC/2014/TRF-3ª REGIÃO/ANALISTA JUDICIÁRIO/INFORMÁTICA) Os responsáveis pela Segurança da Informação do TRF da 3a Região foram encarregados de produzir dois documentos:
1. Documenta procedimentos de gerenciamento, desenhados para manter ou recuperar operações de negócio, incluindo operações de computadores, no caso de eventuais emergências, desastres ou falhas de sistemas. É elaborado para situações em que exista perda de recursos, porém, esses recursos podem ser recuperados de uma forma menos traumática.
2. Documenta uma série de instruções ou procedimentos pré-determinados que descrevam como as funções de negócios da organização serão sustentadas durante e após uma interrupção significante. É elaborado para possibilitar que a organização funcione em um nível aceitável para sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem.
Os documentos 1 e 2 são, respectivamente,
a) Plano de Emergência e Política de Segurança da Informação.

b) Plano de Contingência e Plano de Continuidade de Negócios.
c) Plano de Administração de Crises e Plano de Auditoria.
d) Política de Recuperação de Desastres e Política de Segurança da Informação.
e) Plano de Continuidade Operacional e Plano de Negócios.

Observe que inicialmente já conseguimos eliminar os itens Política de Segurança da Informação, Plano de Negócios e Plano de Auditoria. Sobrou, então, a letra B.

a) Plano de Emergência e ~~Política de Segurança da Informação~~.
b) Plano de Contingência e Plano de Continuidade de Negócios.
c) Plano de Administração de Crises e ~~Plano de Auditoria~~.
d) Política de Recuperação de Desastres e ~~Política de Segurança da Informação~~.
e) Plano de Continuidade Operacional e ~~Plano de Negócios~~.

Plano de Contingência	**Documenta procedimentos de gerenciamento,** desenhados **para manter ou recuperar operações de negócio**, incluindo operações de computadores, **no caso de eventuais emergências, desastres ou falhas de sistemas**. É elaborado para situações em que exista perda de recursos, porém, esses recursos podem ser recuperados de uma forma menos traumática.
Plano de Continuidade de Negócios	**Documenta uma série de instruções ou procedimentos predeterminados que descrevam como as funções de negócios da organização serão sustentadas durante e após uma interrupção significante.** É elaborado para possibilitar que a organização funcione em um nível aceitável para sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem.

Letra b.

013. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO/TI/AMBIENTE OPERACIONAL/2009) A estruturação de planos de contingência requer que a avaliação dos riscos e dos respectivos impactos, relativos à infraestrutura de TI, anteceda a identificação dos eventos em geral que possam causar interrupção nos processos do negócio.

A identificação desses eventos ocorre durante o processo de avaliação dos riscos, e não posteriormente!

Errado.

014. (ESAF/CGU/AFC/INFRAESTRUTURA E SUPORTE/2008) Um plano de contingência não compreende

a) respostas imediatas a desastres.
b) identificação e compreensão do problema (desastre).
c) processo de restauração.
d) contenção de danos e a eliminação das causas.
e) análise crítica dos direitos de acesso dos usuários.

Plano de Contingências consiste num conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços.

Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

O Plano de Contingências é um conjunto de medidas que combinam ações preventivas e de recuperação. Obviamente, os tipos de riscos a que estão sujeitas as organizações variam no tempo e no espaço. Porém, pode-se citar como exemplos de riscos mais comuns a ocorrência de desastres naturais (enchentes, terremotos, furacões), incêndios, desabamentos, falhas de equipamentos, acidentes, greves, terrorismo, sabotagem, ações intencionais.

De maneira geral, o Plano de Contingências contém informações sobre:

- condições e procedimentos para ativação do Plano (como se avaliar a situação provocada por um incidente);
- procedimentos a serem seguidos imediatamente APÓS a ocorrência de um desastre (como, por exemplo, contato eficaz com as autoridades públicas apropriadas: polícia, bombeiro, governo local);
- a instalação reserva, com especificação dos bens de informática nela disponíveis, como hardware, software e equipamentos de telecomunicações;
- a escala de prioridade dos aplicativos, de acordo com seu grau de interferência nos resultados operacionais e financeiros da organização. Quanto mais o aplicativo influenciar na capacidade de funcionamento da organização, na sua situação econômica e na sua imagem, mais crítico ele será;
- arquivos, programas, procedimentos necessários para que os aplicativos críticos entrem em operação no menor tempo possível, mesmo que parcialmente;
- sistema operacional, utilitários e recursos de telecomunicações necessários para assegurar o processamento dos aplicativos críticos, em grau pré-estabelecido;
- documentação dos aplicativos críticos, sistema operacional e utilitários, bem como suprimentos de informática, ambos disponíveis na instalação reserva e capazes de garantir a boa execução dos processos definidos;
- dependência de recursos e serviços externos ao negócio;
- procedimentos necessários para restaurar os serviços computacionais na instalação reserva;

- pessoas responsáveis por executar e comandar cada uma das atividades previstas no Plano (é interessante definir suplentes, quando se julgar necessário);
- referências para contato dos responsáveis, sejam eles funcionários ou terceiros;
- organizações responsáveis por oferecer serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração;
- contratos e acordos que façam parte do plano para recuperação dos serviços.

Conforme visto, os itens de A ao D estão diretamente relacionados a Planos de Contingência de TI escritos, divulgados, testados, mantidos e atualizados com o objetivo real de proteger o negócio. Itens **CORRETOS**.
Item E. A atividade em questão não está relacionada ao escopo do Plano de Contingência. Item **ERRADO**.
Letra e.

---

015. (FCC/TRT-12ª REGIÃO/SC/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/SEGURANÇA DA INFORMAÇÃO/2013) O PCN – Plano de Continuidade de Negócios deve ser planejado antes da ocorrência de desastres, de forma a diminuir ou mitigar o impacto causado pelos mesmos. Desastres se referem a qualquer situação que afeta os processos estratégicos considerados críticos para o funcionamento de uma organização. Ao criar o PCN, as variáveis ETIPI devem ser devidamente consideradas. ETIPI se refere a
a) **E**letricidade – **T**erminais – **I**nformações – **P**rédios – **I**ntranet.
b) **E**laboração – **T**reinamento – **I**nfraestrutura – **P**lanejamento – **I**mplantação.
c) **E**nergia – **T**elecomunicações – **I**nfraestrutura – **P**essoas – **I**nformática.
d) **E**letricidade – **T**ransportes – **I**nformações – **P**rodutos – **I**nternet.
e) **E**nergia – **T**ransmissões – **I**ntranet – **P**rocessos – **I**nternet.

Conforme visto no enunciado da questão, **desastres** referem-se a qualquer situação que afeta os processos estratégicos considerados críticos para o funcionamento de uma organização.
O **Plano de Continuidade de Negócios (PCN), tradução do termo *Business Continuity Plan*(BCP)**, deve ser planejado antes da ocorrência de desastres, para diminuir ou mitigar o impacto causado pelos mesmos.
Ao criar o PCN (ou BCP, em inglês) devemos manipular as **variáveis "ETIPI"**, destacadas a seguir:

- **E** – **Energia** – Operadoras fornecedoras de energia elétrica;
- **T** – **Telecomunicações** – Empresas que fornecem comunicação usando dados e voz;
- **I** – **Infraestrutura** – Localização, para-raios, Instalações Elétricas, Segurança Física, etc.;
- **P** – **Pessoas** – Contingência das atividades e atendimento através de Sites Remotos;
- **I** – **Informática** – Equipamentos, Sistemas, Conectividade, etc.

Referência: https://paulosec.wordpress.com/2011/01/07/plano-de-continuidade-de-negocios-necessario/

Letra c.

---

016. (FCC/TCM-PA/TÉCNICO EM INFORMÁTICA/2010) Um Plano de Continuidade de Negócios (PCN) é um conjunto de três outros planos:

a) Plano Orçamentário de TI (POTI), Plano de Contingência Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

b) Plano de Administração Financeira (PAF), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

c) Plano de Administração Financeira (PAF), Plano de Contingência Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

d) Plano de Gerenciamento de Crises (PGC), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

e) Plano Estratégico de TI (PETI), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

Um **Plano de Continuidade de Negócios (PCN)** tem como propósito **permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.**

O PCN é subdividido em:

- **Plano de Gerenciamento de Crises (PGC),**
- **Plano de Continuidade Operacional (PCO), e**
- **Plano de Recuperação de Desastres (PRD).**

Vide descrição de cada um deles a seguir:

Plano	Descrição
Plano de Gerenciamento de Crises (PGC)	Define as responsabilidades de cada membro da equipe envolvida com o acionamento da contingência e os procedimentos a serem executados para retornar a normalidade.
Plano de Continuidade Operacional (PCO)	Visa definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos do negócio.

Plano de Recuperação de Desastres (PRD)	Tem o objetivo de **restabelecer as atividades o mais breve possível, minimizando o impacto causado pelo desastre**. Esse plano possui seu escopo restrito, não tratando de interrupções menores que não requerem mudanças de locais. Pense numa organização localizada num local onde ocorreram chuvas torrenciais fora do horário do expediente e os funcionários não conseguirão chegar a tempo hábil para início do expediente. O PCO pode restaurar as atividades num site remoto localizado em outra cidade com características climáticas diferentes e de fácil acesso, podendo ser um site da própria empresa ou terceirizado. Se for uma equipe de atendimento telefônico, poderá ser substituído por uma central de Call Center até a normalização das atividades. Cada cenário precisa de um estudo detalhado. O PRD **recupera e restaura as funcionalidades restabelecendo o ambiente e as condições originais de operação**.

Letra d.

017. (FCC/MPE-AP/ANALISTA MINISTERIAL/TECNOLOGIA DA INFORMAÇÃO/2012) O plano de continuidade do negócio deve

a) ter a mesma definição e desenvolvimento para todas as organizações e utilizar uma abordagem genérica, já que dessa forma poderá abranger todos os aspectos críticos que causam impactos negativos ao negócio.

b) ser eficiente e eficaz, ser mantido atualizado e ser testado periodicamente contando com a participação de todos os envolvidos.

c) ser do conhecimento apenas da alta administração que deve conhecer e aprovar as ameaças e riscos que estão fora do escopo do plano.

d) ser elaborado de forma que possibilite seu funcionamento em condições perfeitas, em nível otimizado, garantindo que não haja a possibilidade de incidentes que gerem impactos financeiros ou operacionais.

e) prever um plano para recuperação de desastre elaborado apenas em situações em que não haja perda de recursos, apesar da imagem da organização ser afetada, por exemplo, pela falha de um produto.

a) Errada. Segundo ABNT NBR 15999-01:2007, “o conteúdo e os componentes dos PCN variam de organização para organização e possuem diferentes níveis de detalhe, dependendo da escala, ambiente, cultura e complexidade técnica da organização”. O desenvolvimento do PCN deve ser específico para cada organização, pois deve ser baseado em uma análise de impacto no negócio caso ocorra uma indisponibilidade dos recursos de informação.

b) Certa. De acordo com a ABNT ISO 27002, na seção 14.1.5, convém que os **planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade**. Além disso, os testes deverão contar com a participação de todos os envolvidos. A ABNT NBR 15999-01:2007, na seção 10.3, destaca que habilidades e competências de resposta na organização devem ser desenvolvidas por meio de treinamentos práticos, incluindo participação ativa em testes.
c) Errada. O PCN deve ser de conhecimento de todos os envolvidos na continuidade do negócio, devendo ter o apoio permanente da alta administração. Conforme destaca também a ABNT NBR 15999-01:2007, criar e manter uma consciência quanto à importância da GCN (Gestão de Continuidade de Negócios) com toda a equipe da organização é importante para garantir que todos entendam o motivo da importância da GCN para a organização. A alta administração, os acionistas da organização e outras partes interessadas precisam conhecer as ameaças e riscos relacionados ao PCN, pois esses indivíduos é que irão aprovar o que irá ficar fora do plano!
d) Errada. O PCN será colocado em ação quando incidentes ocorrem. É uma utopia dizer que funcionará em condições perfeitas!
e) Errada. Deve ser elaborado para todas as situações em que haja perda de recursos.
Letra b.

---

018. (FCC/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA/2012) Convém que o processo de planejamento da continuidade de negócios considere:
I – Identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio.
II – Identificação da perda aceitável de informações e serviços.
III – Implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários.
IV – Educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise.
Está correto o que consta APENAS em
a) I, II, III e IV.
b) I, II e III.
c) II e III.
d) I e IV.
e) II e IV.

A questão retrata o descrito na **Norma ABNT NBR ISO/IEC 27002, seção 14 (Gestão da Continuidade do Negócio),** controle 14.1.3 (Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação):

Diretrizes para implementação

"Convém que o processo de planejamento da continuidade de negócios considere os seguintes itens:

a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;

b) identificação da perda aceitável de informações e serviços;

c) implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários;

d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;

e) documentação dos processos e procedimentos acordados;

f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;

g) teste e atualização dos planos".

Conforme visto, itens I, II, III e IV foram descritos na íntegra acima.

Letra a.

---

019. (FCC/TCE-AP/ANALISTA DE CONTROLE EXTERNO/TECNOLOGIA DA INFORMAÇÃO/2012) Com relação ao Plano de Continuidade de Negócio é INCORRETO afirmar:

a) Deve ser elaborado um Plano de Continuidade de Negócio que possibilite que a organização funcione em um nível aceitável para sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem

b) O desenvolvimento do Plano de Continuidade de Negócio deve ser específico para cada organização, pois deve ser baseado em uma análise de impacto no negócio caso ocorra uma indisponibilidade dos recursos de informação.

c) A alta administração e os acionistas da organização não precisam conhecer e aprovar as ameaças e riscos que estão fora de cada versão do Plano de Continuidade de Negócio, pois esses aspectos são definidos e homologados pela gerência de TI.

d) O Plano de Continuidade de Negócio deve ser eficiente/eficaz, mantido atualizado e testado periodicamente com a participação de todos os envolvidos.

e) Seu objetivo é o planejamento de ações para serem executadas quando da ocorrência de uma situação de contingência, de maneira a garantir que a organização mantenha suas atividades críticas em um nível previamente definido pela área de negócio e direção como aceitável.

A única assertiva indevida é a letra C. **A alta administração, os acionistas da organização e outras partes interessadas precisam conhecer as ameaças e riscos relacionados ao PCN**, pois esses indivíduos é que irão aprovar o que irá ficar fora do plano!

Observe que a assertiva D, foi questão da prova do MPE, neste mesmo ano de 2012.

Letra c.

---

020. (FCC/INFRAERO/ANALISTA/SEGURANÇA DA INFORMAÇÃO/2011) Sobre a Gestão da Continuidade do Negócio, é correto afirmar:

a) As cópias dos Planos de Continuidade do Negócio devem estar atualizadas mas não precisam ser protegidas no mesmo nível de segurança como aplicado no ambiente principal. Outros materiais necessários para a execução do plano de continuidade do negócio devem estar armazenados no ambiente principal, em local de fácil acesso.

b) O processo de planejamento da continuidade de negócios deve considerar a implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários, sem dispensar atenção à avaliação de dependências externas ao negócio e aos contratos existentes.

c) Convém que uma estrutura de planejamento, para continuidade de negócios, contemple os requisitos de segurança da informação identificados e considere condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado.

d) É conveniente que cópias do plano de continuidade do negócio sejam guardadas no ambiente principal, em um local de fácil acesso.

e) Apesar de ser necessário atualizar os planos de continuidade do negócio regularmente, não é aconselhável que eles sejam testados com frequência para não impactar em aumento de custos para a área de TI.

a/d) Erradas. As cópias devem ser de fácil acesso, com nível de proteção adequado, e armazenadas em ambientes alternativos. Assim, em caso de incidente ou desastre no ambiente principal, poderão ser recuperadas.

b) Errada. O processo de planejamento da continuidade de negócios deve considerar a implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários; **atenção especial precisa ser dada à avaliação de dependências externas ao negócio e de contratos existentes**, conforme destacado na ABNT NBR ISO/IEC 27002, seção 14 (Gestão da Continuidade do Negócio), controle 14.1.3-Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação (item c).

c) Certa. Conforme especificado na ABNT NBR ISO/IEC 27002, seção 14 (Gestão da Continuidade do Negócio), controle 14.1.4-Estrutura do Plano de Continuidade do Negócio (item a): "Convém que uma estrutura de planejamento para continuidade de negócios contemple os requisitos de segurança da informação identificados e considere os seguintes itens: condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado;"

e) Errada. Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade (ABNT NBR ISO/IEC 27002, seção 14 (Gestão da Continuidade do Negócio), controle 14.1.5).

Nota: o item B foi motivo de vários recursos na época da prova, em virtude do uso da palavra DISPENSAR, que possui dois sentidos: um positivo (dar, conceder) e outro negativo (desobrigar). Mas a banca considerou a assertiva C como a correta.

Letra c (com ressalvas).

021. (FCC/INFRAERO/ANALISTA DE SISTEMAS/SEGURANÇA DA INFORMAÇÃO/2011) O Plano de Continuidade do Negócio

a) não precisa ser testado antes que se torne realmente necessário, pois testes por si só implicam em riscos aos ativos de informação.

b) deve ser elaborado com base em premissas departamentais particulares do que é considerado importante ou não.

c) prioriza e estabelece as ações de implantação como resultado de uma ampla análise de risco.

d) define uma ação de continuidade imediata e temporária.

e) precisa ser contínuo, evoluir com a organização, mas não precisa ser gerido sob a responsabilidade de alguém como os processos organizacionais.

O **Plano de Continuidade do Negócio (PCN)** prioriza e estabelece as ações de implantação em função dos resultados da análise/avaliação de riscos.

Letra c.

Auditoria e Conformidade

Definição de Auditoria

Auditoria é uma atividade que engloba o exame de **operações**, **processos**, **sistemas** e **responsabilidades** gerenciais de uma determinada entidade, com intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

A **auditoria da tecnologia da informação (TI)** é fundamental para as organizações modernas, por se tratar de uma atividade que tem por base a análise detalhada dos dados de uma empresa, abrangendo a verificação de várias informações que a mesma produz, com objetivos específicos que podem contribuir para se evitar erros ou mesmo fraudes na mesma.

A **auditoria da TI** já foi conceituada anteriormente, mas vale destacar o disposto por Imoniana (2005), que afirma ser:

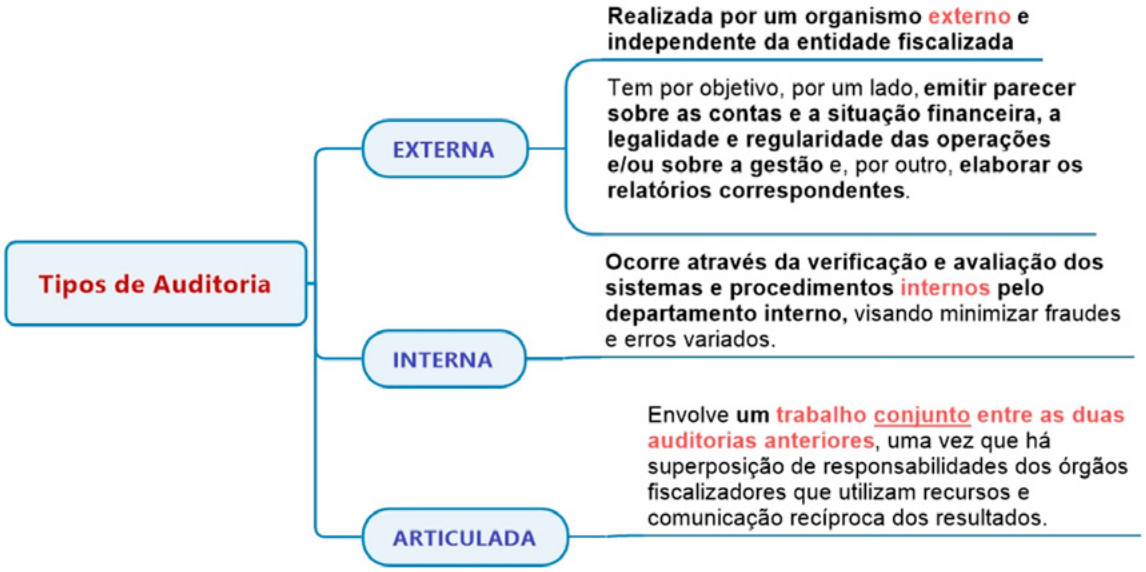
(...) *essencialmente operacional, por meio das quais os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade auditada, indicando seus pontos fortes e/ou deficiências. Em alguns países é conhecida como auditoria de informática computacional ou de sistemas*.

A **abordagem ao redor do computador** não envolve a utilização de muitas tecnologias de informação e sim o exame de níveis de anuência associados à aplicação de controles organizacionais, conforme dispõe Imoniana (2005). Trata-se de uma abordagem que não é muito indicada para ambientes complexos, mas é muito útil em sistemas menores, que não exijam um conhecimento mais profundo de TI.

A **abordagem através do computador** vai além da verificação de documentos, havendo o acompanhamento e análise de dados por meio do computador (IMONIANA, 2005).

Quanto à **abordagem com o computador**, pode-se dizer que permite uma análise com maior precisão, por meio da compilação do processo, possibilitando a utilização das "capacidades lógicas e aritméticas do computador para verificar os cálculos das transações econômicas e financeiras, dentre outros" (IMONIANA, 2005).

Tipos de Auditoria:



Fases da Auditoria de TI

As principais **fases** da auditoria de TI estão listadas a seguir:

- **Planejamento**
- Busca **obter as informações de todos os procedimentos e mapa de risco da área auditada, entrevistar os envolvidos e, em seguida, elaborar uma narrativa do processo, identificando os riscos e os controles**.

- No decorrer do planejamento, a auditoria terá por base a **revisão e avaliação do processo de construção de sistemas de informação**, que deve partir do levantamento e estudo do sistema.

- **Execução**
- Esta fase tem por base a **análise das evidências e a forma de coleta de dados**.
- Evidências são **informações que sustentam os relatórios elaborados pelo auditor, objetivando a comunicação de fatos verificados durante a execução do trabalho de auditoria**. Os relatos são fundamentais, sem os quais não se tem conhecimento das falhas nos controles internos para saná-las.
- **Evidência** em auditoria: (...) **é o conjunto de fatos comprovados, suficientes, competentes e pertinentes, obtidos durante os trabalhos de auditoria, através de observações, inspeções, entrevistas e exames dos registros, que sustentam as conclusões do auditor.** É algo que contribui para o estabelecimento da prova, ajudando na convicção sobre as reais condições existentes na área sob exame.
- Peter (*et. al.*, 2003, p. 89) afirmam existir **quatro tipos de evidências**, segundo a forma, ou seja, **física, testemunhal, documental e analítica**.

A **física** é obtida por meio de observação direta. A **testemunhal** surge por meio de entrevistas e depoimentos; enquanto a **documental**, como o próprio nome diz, através de documentos. Por fim, a **evidência analítica** é aquela que tem por base o exame comparativo de dados, cálculos etc.

Direto do Concurso

022. (INÉDITA/2021) As evidências podem ser divididas em 4 tipos, que são: evidência física, evidência documentária, evidência testemunhal e evidência analítica.

Dias (2000, p. 33) cita 4 tipos de evidências, considerando a evidência testemunhal como a evidência fornecida pelo auditada. TCE-CE (2013) também corrobora a classificação reportada no enunciado da questão. Os **quatro tipos de evidências** são descritos a seguir:

Tipo	Descrição
Física	Observação de pessoas, locais ou eventos. Pode ser obtida por meio de fotografias, vídeos e mapas, e costumam causar grande impacto. A fotografia de uma situação insalubre, por exemplo, pode ser mais convincente que uma longa descrição (TCE-CE, 2013). **Dias (2000) destaca as observações de atividades desenvolvidas por funcionários e gerentes, sistemas de informação em funcionamento, local, equipamentos, etc.**
Documental (ou Documentária, conforme destacado por Dias,2000)	É o tipo mais comum de evidência. Pode estar disponível em meio físico ou eletrônico. É obtida de ofícios, memorandos, correspondências, contratos, extratos e relatórios, sendo essencial avaliar a confiabilidade e a relevância dessas informações para os objetivos do trabalho de auditoria (TCE-CE,2013). **Dias (2000) cita aqui os resultados da extração de dados, registros de transações, listagens, etc.**
Testemunhal (ou Fornecida pelo Auditado, conforme destacado por Dias,2000)	Obtida em entrevistas, grupos focais e questionários assinados. Para que possa ser considerada evidência, e não apenas contexto, é preciso validá-la por meio de confirmação por escrito do entrevistado ou existência de múltiplas fontes que confirmem os fatos. **Dias (2000) cita nessa categoria as transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, políticas internas, e-mails trocados com a gerência da entidade, justificativas, relatórios publicados pelo auditado (impressos ou on-line),** etc.
Analítica	Obtida por meio de análises, comparações e interpretações de dados e informações existentes. Pode envolver análise de padrões e tendências. É o tipo de evidência mais difícil de se conseguir. **Dias (2000) destaca nessa categoria as comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempo diferentes.**

Certo.

- Quanto à **confiabilidade das evidências**, pode-se dizer que a menos confiável são as entrevistas, uma vez que é difícil comprovar a veracidade das informações contidas na mesma.
- É importante a utilização de uma medida de controle e segurança de sistemas de informações em operação para garantir a confiabilidade das informações, o que se faz por meio da auditoria, de forma a validar e avaliar os resultados gerados pelos sistemas.
- Um ponto que merece destaque no que tange aos objetivos de um sistema geral, é justamente manter a integridade, correção e confiabilidade dos registros.

- **EMISSÃO E DIVULGAÇÃO DE RELATÓRIOS**
- O auditor de TI deve prover um **relatório**, **em forma apropriada**, **para os destinatários**, por ocasião da conclusão do trabalho de auditoria.
- O relatório de auditoria deve apresentar **escopo**, **objetivos**, **período de abrangência**, **natureza e extensão do trabalho executado**. **Deve identificar a organização, os usuários desejáveis e quaisquer restrições à sua circulação**. Ainda, neste relatório, devem-se incluir as **observações**, **conclusões**, **recomendações** e quaisquer ressalvas ou conceitos que o auditor possua a respeito da auditoria.
- Importante ainda que **o relatório contenha o parecer final do auditor sobre o processo auditado, bem como os pontos e as ações corretivas desenhadas.**

- **FOLLOW-UP**
- Interessante que haja **um acompanhamento da auditoria**, para **revisar e avaliar os pontos relevantes apontados no relatório**, realizando, dessa forma, o *follow-up* dos **pontos de controle que possam apresentar algum tipo de deficiência em trabalhos anteriores**.
- "O auditor de tecnologia de informação deve requisitar e avaliar informações apropriadas sobre **pontos**, **conclusões** e **recomendações anteriores** e relevantes para determinar se ações apropriadas foram implementadas em tempo hábil".
- Trata-se, portanto, de uma fase de suma importância no contexto da auditoria de TI, uma vez que **permite verificar se os problemas apresentados anteriormente foram resolvidos ou não, bem como se as medidas adotadas geram a redução das deficiências identificadas**.

Técnicas de Auditoria

São necessárias **técnicas de auditoria específicas** para realizar a avaliação de pontos de controle sobre aplicativos, o que possibilitam a validação dos programas, dados e todas as informações que tiverem relação com os sistemas.

Para a aplicação das referidas técnicas é comum a exigência de características do sistema a ser avaliado, bem como dos objetivos da auditoria e abrangência dos exames (ARIMA *et. al.*, 2005).

Importante observar que **há técnicas de difícil aplicação e adaptação às condições inerentes a cada sistema analisado**, sendo fundamental o papel do auditor neste processo, uma vez que **deve conhecer e validar custos e benefícios efetivos que permitam sua utilização** (ARIMA *et. al.*, 2005).

Existem várias **técnicas básicas que merecem destaque**, como as listadas a seguir:

- "**Dados de teste ou *Test-Deck***", na qual se **busca preparar dados de entrada**, utilizando-se, para tanto, inúmeras condições e variáveis diferentes para testar. Os dados de entrada referidos são alimentados e processados pelas rotinas e programas normais

de produção, em processamento separado, valendo destacar que ocorre a simulação de um ambiente real, possibilitando a avaliação de sua exatidão e os controles existentes (IMONIANA, 2005).

O objetivo principal da técnica de dados de teste é a **identificação e avaliação dos controles, políticas, normas e procedimentos definidos**. O auditor não necessita de assistência ou ajuda para preparar os dados de entrada e avaliar os resultados esperados e não se exige um profundo conhecimento de informática. Ocorre, porém, que há uma **desvantagem** técnica a ser observada, qual seja, a **possibilidade de não serem consideradas todas as possibilidades e situações geradoras de transações e ainda, dependendo do escopo do teste, pode tornar-se bastante complexa e demorada** (ARIMA *et. al*., 2005).

- A técnica da **verificação "*In-Loco*"** consiste na **observação pessoal do auditor de sistemas aos processos e funções inerentes ao sistema**, devendo ocorrer o cumprimento de uma sequência específica de procedimentos, iniciando-se pela marcação antecipada de data e hora com o responsável pelo sistema; anotação dos procedimentos e acontecimentos, bem como coleta de documentos; anotação do nome completo das pessoas que prestaram depoimentos e respectivas data e hora; finalmente, análise dos resultados obtidos e exposição de opinião via relatório de fraquezas de controle interno (ARIMA *et. al*., 2005).
- **Análise de "*Job Accounting*"/"*Log*"** tem por base arquivos de *Log/Accounting* que são gerados por uma rotina componente do sistema operacional, a qual possui registros de utilização do hardware e software que compõem o ambiente computacional. A técnica em tela possibilita a identificação da ineficiência do sistema auditado, a apuração do desbalanceamento da configuração do computador, pela caracterização de dispositivos de entrada e saída (disco, fitas, terminais, impressoras) que estão com folga ou sobrecarregados, a determinação de erros de programas ou de operação, o uso de programas fraudulentos ou utilização indevida e ainda a identificação de tentativas de acesso a arquivos ou ao sistema por senhas não autorizadas, tratando-se de um importante instrumento, mas que requer grande conhecimento de computação (ARIMA *et. al*., 2005).
- A **análise de Relatórios/Telas** tem por base a **análise de documentos, relatórios e telas do sistema**, como forma de determinar o nível de utilização pelo usuário, esquemas de distribuição e número de vias emitido, grau de confidencialidade de seu conteúdo, forma de utilização e integração e distribuição das informações, segundo o layout vigente (ARIMA *et. al*., 2005).
- A próxima técnica a ser destacada são os **questionários**, ou seja, **a elaboração de uma série de perguntas como forma de verificar determinado ponto de controle,** de forma a adequar o ponto de controle aos parâmetros do controle interno, sejam eles, segurança

física e lógica, controle de acesso, confidencialidade, obediência à legislação ou eficiência e eficácia (CARLOS, 1999). Segundo Magalhães (2001) os questionários visam o esclarecimento de situações de operação do sistema, sendo interessantes exemplos: plano diretor de informática; ambiente de banco de dados; ambiente de auditoria interna.

- **Entrevistas**: importante técnica que **busca realizar reuniões entre auditor e auditados visando revisar e avaliar o grau de controle interno existente**.
- A aplicação desta técnica pode ocorrer em qualquer ponto de controle como um complemento à aplicação das demais técnicas, além de permitir reduzir o tempo de avaliação do ponto de controle e possibilitar esclarecimentos de pontos duvidosos ou polêmicos.
- ***Integrated Test Facility* – ITF:** é uma variante da Massa de Teste **que busca gerar uma entidade fictícia dentro do sistema e consequentemente, transações para esta entidade, as quais serão processadas dentro do ciclo normal de processamento do sistema.**
  O objetivo principal desta técnica é **testar e verificar sistemas complexos e de grande porte, onde não é possível separar o processamento num outro ambiente**, apresentando como vantagem a constatação de um exame bastante abrangente, sem a necessidade de processamento especial e separado, além do custo operacional reduzido, o que se deve, principalmente, ao tempo reduzido para criar um ambiente de testes. Por outro lado, sua desvantagem principal é a necessidade de se estabelecer procedimentos de separação e retirada dos dados de auditoria das transações normais.

Mais sobre Auditoria

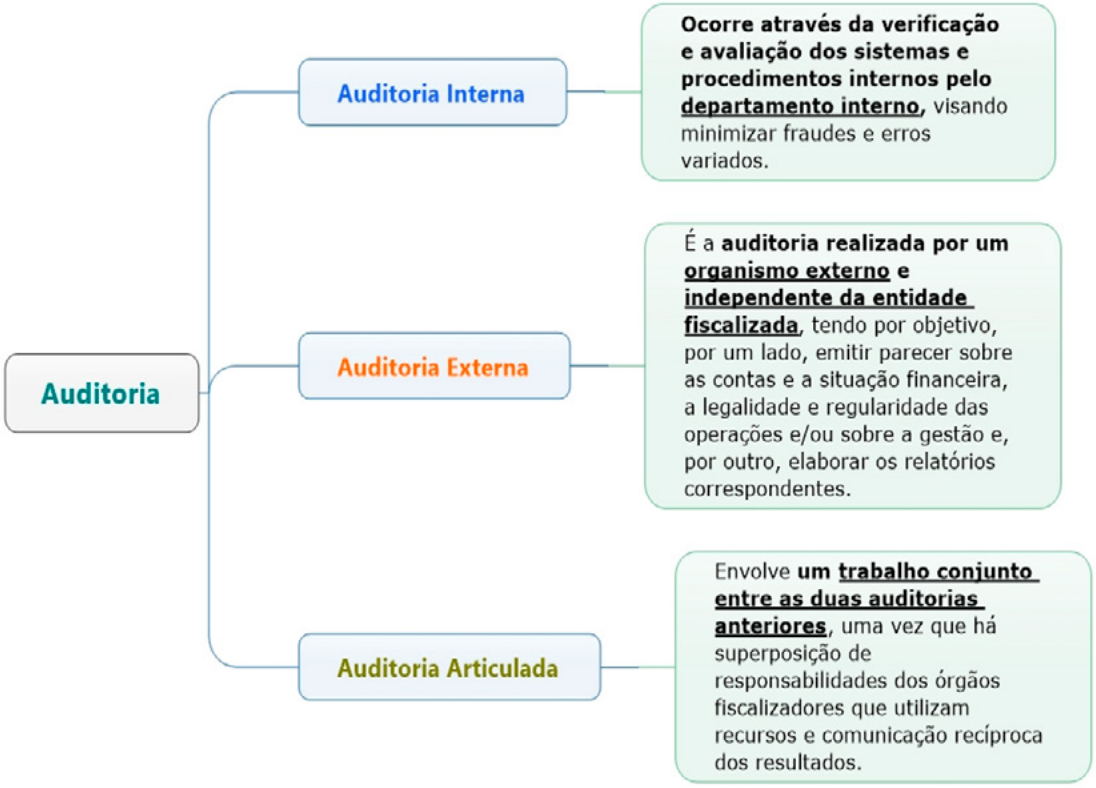
- É importante a **realização de análises críticas regulares da eficácia do SGSI** – Sistema de Gestão de Segurança da Informação (incluindo o atendimento da política de segurança e de seus objetivos, e a análise crítica de **controles** de segurança), levando em consideração os resultados de **auditorias** de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas.
- Um **programa de auditoria** deve ser planejado levando em consideração a situação e a importância dos processos e áreas a serem auditadas, bem como os resultados de auditorias anteriores. Os critérios (requisitos tomados como padrão) da auditoria, escopo (o que o auditor irá verificar na auditoria), frequência e métodos devem ser definidos. A seleção dos auditores e a execução das auditorias devem assegurar objetividade e imparcialidade do processo de auditoria, para isso, uma regra básica na auditoria é que os auditores não devem auditar seu próprio trabalho.
- As responsabilidades e os requisitos para planejamento e para execução de auditorias e para relatar os resultados e a manutenção dos registros devem ser definidos em um

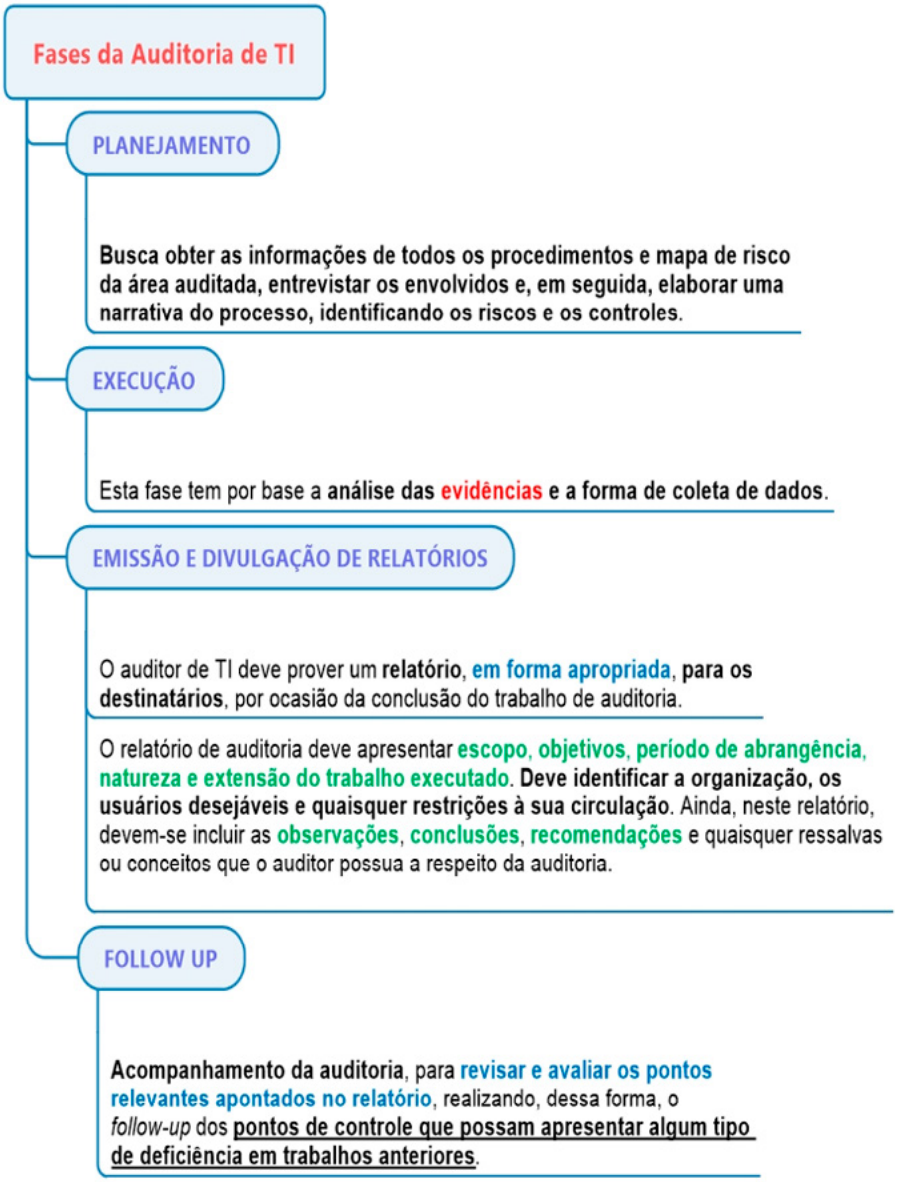
procedimento documentado. O responsável pela área a ser auditada deve assegurar que as ações sejam executadas pela área auditada, sem demora indevida, para eliminar as **não conformidades** detectadas e suas causas, por meio de atividades de acompanhamento.

RESUMO

Auditoria é uma atividade que engloba o exame de operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

Tipos de auditoria (Interna, Externa, Articulada):





A **auditoria da tecnologia da informação (TI)** é fundamental para as organizações modernas, por se tratar de uma **atividade que tem por base a análise detalhada dos dados de uma empresa**, abrangendo a verificação de várias informações que a mesma produz, com objetivos específicos que podem contribuir para se evitar erros ou mesmo fraudes na mesma.

Por meio da **Auditoria de TI os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade auditada, indicando seus PONTOS FORTES e/ou DEFICIÊNCIAS (Imoniana, 2008).**

Imoniana ainda define que os **objetivos globais de uma auditoria de sistemas** são: **integridade, confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenibilidade**.

Uma questão recorrente em provas afirma que o planejamento se encerra junto com o início dos trabalhos de campo do auditor, e isso está errado! Lembre-se sempre de que o planejamento não é uma fase isolada da auditoria, mas um **PROCESSO CONTÍNUO e ITERATIVO** que começa já nos primeiros contatos do auditor com a empresa e só se encerra com a emissão do seu relatório.

Ao término da investigação **em cada área auditada**, segundo Dias (2000), é recomendável apresentar, aos responsáveis da área, **um relatório parcial contendo as deficiências encontradas**.

Essa apresentação normalmente ocorre em entrevistas para discussão das falhas apresentadas. Nessa ocasião, os responsáveis expõem seus motivos e justificam a ocorrência da falha. Suas justificativas podem ser anexadas ao parecer da equipe de auditoria e incluídas no relatório final.

A apresentação desses relatórios intermediários evita quaisquer constrangimentos, erros ou inconsistências, que poderão ser identificados, corrigidos ou eliminados antes da apresentação do relatório final.

O auditor não é responsável nem pode ser responsabilizado pela prevenção de fraudes ou erros. No entanto, **DEVE planejar seu trabalho avaliando o risco de sua ocorrência**.

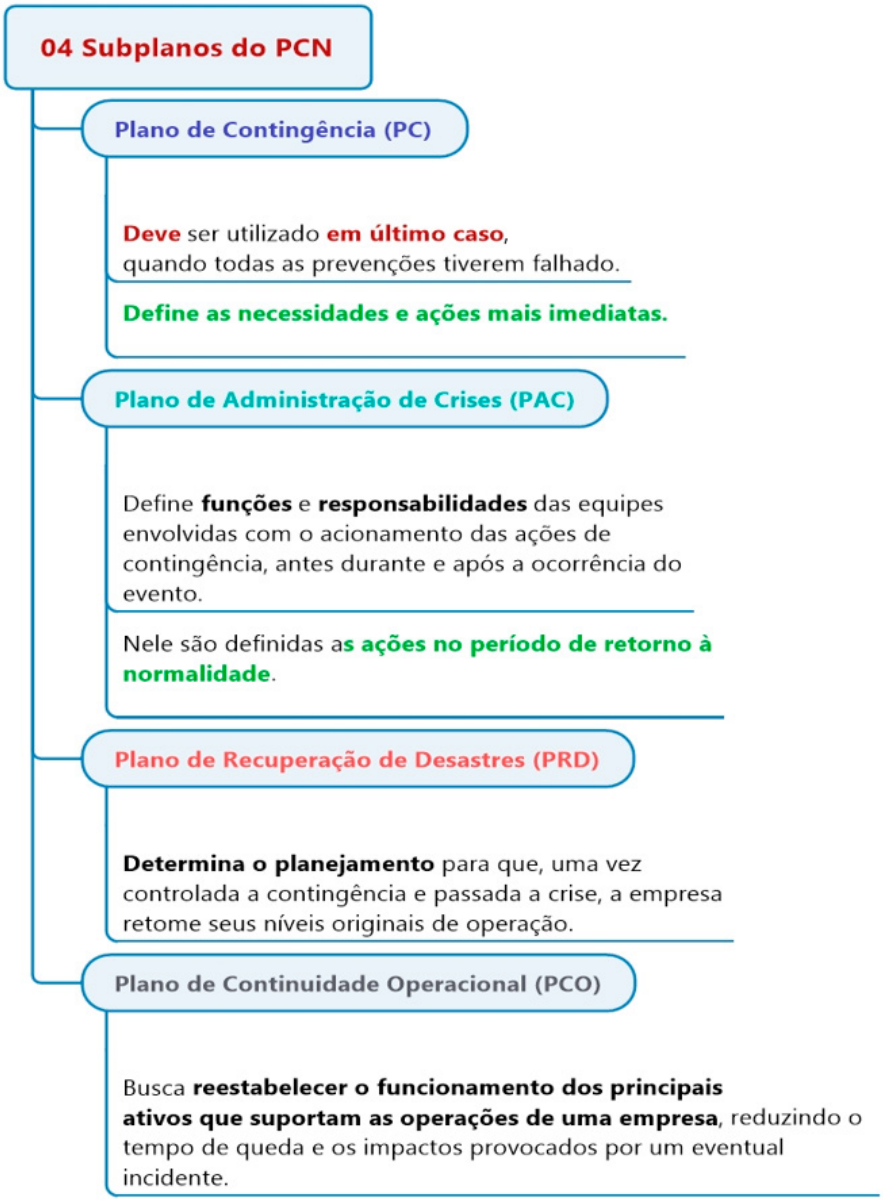
RISCO de auditoria é a probabilidade de que o auditor emita uma opinião inadequada sobre um objeto que contém distorções ou irregularidades relevantes.

Os principais critérios usados para a seleção de objeto de auditoria são: **materialidade, relevância** e **vulnerabilidade a riscos.**

Vamos à distinção entre cada um deles:

Materialidade	**A seleção deve levar em consideração os valores financeiros envolvidos no objeto de auditoria**, importando ressaltar, porém, que **nem sempre os benefícios de um trabalho de auditoria são vinculados apenas aos recursos financeiros envolvidos.** Aperfeiçoar processos e procedimentos dos objetos com alta materialidade possibilita gerar economia ou eliminar desperdícios.
Relevância	Indica que **as auditorias selecionadas devem procurar responder, quando possíveis, questões de interesse do Tribunal de Justiça do Estado do Ceará e da própria Sociedade,** possibilitando **agregação de valor** quanto a produzir novos conhecimentos e perspectivas sobre o objeto de auditoria.

Vulnerabilidade a Riscos	Este critério se **relaciona às possíveis vulnerabilidades ou propriedades intrínsecas do objeto de auditoria que podem estar associadas à ocorrência de eventos como fraudes, desvios e gestão ineficiente.**



Assim, terminamos a parte teórica da nossa aula. Vamos praticar agora!

QUESTÕES COMENTADAS EM AULA

001. (FCC/INFRAERO/ANALISTA DE REDES E COMUNICAÇÃO DE DADOS/2011) Um plano de contingência se situa no contexto dos resultados da criação de uma estrutura de gestão e numa estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação de negócios que detalhem os passos a serem tomados durante e após um incidente para manter ou restaurar as operações.
No ciclo de vida da Gestão de Continuidade de Negócio, tal afirmação está associada ao elemento:
a) Desenvolvendo e implementando uma resposta de GCN.
b) Entendendo a organização.
c) Determinando a estratégia de continuidade de negócios.
d) Testando, mantendo e analisando criticamente os preparativos de GCN.
e) Incluindo a GCN na cultura da organização.

002. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO/TI/ARQUITETURA DE SOLUÇÕES/2009) Testes de mesa, testes de recuperação em local alternativo e ensaio geral são técnicas que podem ser empregadas na gestão da continuidade de negócios, conforme prescrição na norma ABNT NBR ISO/IEC 17799:2005.

003. (FCC/2016/PREFEITURA DE TERESINA-PI/ANALISTA TECNOLÓGICO/ANALISTA DE NEGÓCIOS) Um dos objetivos principais da Gestão de Continuidade de Negócios é
a) promover avaliação de desempenho dos responsáveis pela organização.
b) identificar as ameaças à organização e seus impactos, bem como prover resiliência a tais ameaças.
c) realizar um estudo para contenção dos gastos da organização.
d) promover um ambiente harmonioso entre os funcionários da organização.
e) substituir o parque computacional da organização a cada 2 anos.

004. (FCC/2018/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA) Estabelecer um plano de continuidade de negócios é primordial para as empresas, sendo que o plano de continuidade é constituído de subplanos. O subplano estabelecido para ser utilizado em último caso quando todas as prevenções tiverem falhado é conhecido como Plano de
a) Gerenciamento de Crises.
b) Contingência.
c) Recuperação de Desastres.
d) Administração.
e) Continuidade Operacional.

005. (FCC/2018/PREFEITURA DE SÃO LUÍS-MA/AUDITOR-FISCAL DE TRIBUTOS I/ TECNOLOGIA DA INFORMAÇÃO (TI)) Considere, por hipótese, que um incêndio danificou um servidor da Prefeitura e um Auditor foi acionado para restaurar um backup completo do que havia em uma fita em um novo servidor. Apesar de o Auditor ter levado cerca de 30 minutos para restaurar os dados do backup, o total de tempo entre a notificação da interrupção dos serviços dependentes dos dados do servidor danificado, a recuperação total dos dados e a restauração dos serviços foi de aproximadamente 50 minutos, dentro do tempo tolerável previsto no Plano de Recuperação de Desastres associado ao Plano de Continuidade de Negócio.
Este limite de tempo é conhecido como
a) Recovery Time Point (RTP).
b) Business Process Recovery Objective (BPRO).
c) Recovery Point Objective (RPO).
d) Business Recovery Time (BRT).
e) Recovery Time Objective (RTO).

006. (FCC/2017/DPE-RS/ANALISTA/SEGURANÇA DA INFORMAÇÃO) O Plano de Continuidade dos Negócios é um roteiro de operações contínuas para quando as operações normais dos negócios são interrompidas por condições adversas.
O Plano de Continuidade dos Negócios
a) deve incluir, dentre outras coisas, a definição dos cenários de impacto e a análise de ameaças e riscos.
b) deve ser de responsabilidade do departamento de TI, que é considerado o único com competências necessárias para conter possíveis desastres.
c) também é conhecido como Plano de Recuperação de Desastres, uma vez que inclui ações para retornar a organização a seus níveis originais de operação.
d) deve possuir ações genéricas para conter qualquer tipo de desastre, evitando assim que tenha que ser revisado periodicamente.
e) deve ser executado integralmente em resposta a incidentes que causem interrupção total ou parcial das operações normais de negócios.

007. (FCC/2018/DPE-AM/ANALISTA EM GESTÃO ESPECIALIZADO DE DEFENSORIA/ ANALISTA DE SISTEMA) Um Plano de Continuidade de Negócios pode ser estruturado em quatro outros planos ligados entre si, cada qual criado para cuidar de um estágio diferente:
I – Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.
II – Deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

III – Seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.
IV – Determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.
O plano
a) II se refere ao Plano de Gerenciamento de Crises.
b) III se refere ao Plano de Recuperação de Desastres.
c) I se refere ao Plano de Continuidade Operacional.
d) III se refere ao Plano de Contingência.
e) IV se refere ao Plano de Recuperação de Desastres.

008. (CESPE/2019/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I) Acerca do plano de continuidade de negócios (PCN), assinale a opção correta.
a) Para operacionalizar o PCN de uma empresa que já foi elaborado, é altamente recomendável o desenvolvimento de um sistema de gestão de continuidade de negócios (SGCN).
b) PCN e plano de contingência são sinônimos, uma vez que contemplam os mesmos itens.
c) Os prazos decorrentes de ações realizadas por agentes externos à organização não necessitam ser considerados para elaboração do PCN dessa organização.
d) Na perspectiva do PCN, o funcionamento de uma empresa deve-se, fundamentalmente, às variáveis recursos e pessoas.
e) O PCN estabelece controles de segurança da informação como resultado de uma ampla análise de riscos.

009. (CESPE/2012/TJ-AL/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS) No que se refere ao plano de continuidade de negócios, assinale a opção correta.
a) Os objetivos do plano em tela incluem evitar a interrupção das atividades do negócio, proteger os processos críticos contra o acesso de pessoas estranhas ao ambiente e assegurar a retomada dos processos em tempo hábil, caso necessário.
b) A contratação de seguro compatível é desconsiderada na gestão da continuidade do negócio.
c) A existência de um gestor específico para cada plano de continuidade é desvantajoso, visto que causa aumentos significativos dos custos dos planos como um todo.
d) Os planos de continuidade do negócio devem ser testados e atualizados infrequentemente, já que a realização regular dessas ações acarreta o aumento significativo dos custos dos planos.
e) A estrutura de planejamento para continuidade de negócios deve abranger os ativos e os recursos críticos para uma eventual utilização dos procedimentos de emergência, recuperação e ativação.

010. (FADESP/2018/BANPARÁ/TÉCNICO EM INFORMÁTICA/SUPORTE) O objetivo de um Plano de Continuidade de Negócios (PCN) é garantir que serviços essenciais, por exemplo, de uma empresa sejam devidamente identificados e preservados mesmo após a ocorrência de desastres. Não compõe o PCN o

a) Plano de Contingência (PC).
b) Plano de Administração de Crises (PAC).
c) Plano de Recuperação de Desastres (PRD).
d) Plano de Prevenção de Crises (PVC).
e) Plano de Continuidade Operacional (PCO).

011. (FCC/2017/TRT-24ª REGIÃO/MS/TÉCNICO JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO) Considere a lista a seguir:

1. Um processo para ativar a resposta da organização a um incidente de interrupção e, dentro de cada procedimento documentado, seus critérios e procedimentos de ativação.
2. Um processo para desmobilizar equipes após o incidente ter passado.
3. Regras e padrões para proteção das informações, possibilitando manter a confidencialidade, integridade e disponibilidade.
4. Papéis e responsabilidades definidos para pessoas e equipes que usarão o plano.
5. Orientações e critérios sobre quem tem a autoridade de invocar os procedimentos e sob quais circunstâncias.
6. A definição clara de como serão tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários e as informações institucionais.
7. Gestão das consequências imediatas de um incidente de interrupção considerando as questões de bem-estar de pessoas afetadas, as ações para responder a interrupção e prevenção.
8. Detalhes de contato para os membros da equipe e outras pessoas com funções e responsabilidades dentro de cada procedimento.
9. Detalhes indicando como e em que circunstâncias a organização irá se comunicar com os funcionários, com as principais partes interessadas e contatos de emergência.

No Plano de Continuidade de Negócio deve estar claramente identificável o que consta em 1, 2,

a) 3, 4, 5 e 7.
b) 7, 8 e 9.
c) 3, 6 e 8.
d) 3, 4, 5, 6, 7 e 9.
e) 4, 5, 7, 8 e 9.

012. (FCC/2014/TRF-3ª REGIÃO/ANALISTA JUDICIÁRIO/INFORMÁTICA) Os responsáveis pela Segurança da Informação do TRF da 3a Região foram encarregados de produzir dois documentos:

1. Documenta procedimentos de gerenciamento, desenhados para manter ou recuperar operações de negócio, incluindo operações de computadores, no caso de eventuais emergências, desastres ou falhas de sistemas. É elaborado para situações em que exista perda de recursos, porém, esses recursos podem ser recuperados de uma forma menos traumática.
2. Documenta uma série de instruções ou procedimentos pré-determinados que descrevam como as funções de negócios da organização serão sustentadas durante e após uma interrupção significante. É elaborado para possibilitar que a organização funcione em um nível aceitável para sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem.
Os documentos 1 e 2 são, respectivamente,
a) Plano de Emergência e Política de Segurança da Informação.
b) Plano de Contingência e Plano de Continuidade de Negócios.
c) Plano de Administração de Crises e Plano de Auditoria.
d) Política de Recuperação de Desastres e Política de Segurança da Informação.
e) Plano de Continuidade Operacional e Plano de Negócios.

013. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO-TI/AMBIENTE OPERACIONAL/2009) A estruturação de planos de contingência requer que a avaliação dos riscos e dos respectivos impactos, relativos à infraestrutura de TI, anteceda a identificação dos eventos em geral que possam causar interrupção nos processos do negócio.

014. (ESAF/CGU/AFC/INFRAESTRUTURA E SUPORTE/2008) Um plano de contingência não compreende
a) respostas imediatas a desastres.
b) identificação e compreensão do problema (desastre).
c) processo de restauração.
d) contenção de danos e a eliminação das causas.
e) análise crítica dos direitos de acesso dos usuários.

015. (FCC/TRT-12ª REGIÃO/SC/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/SEGURANÇA DA INFORMAÇÃO/2013) O PCN – Plano de Continuidade de Negócios deve ser planejado antes da ocorrência de desastres, de forma a diminuir ou mitigar o impacto causado pelos mesmos. Desastres se referem a qualquer situação que afeta os processos estratégicos considerados críticos para o funcionamento de uma organização. Ao criar o PCN, as variáveis ETIPI devem ser devidamente consideradas. ETIPI se refere a
a) **E**letricidade – **T**erminais – **I**nformações – **P**rédios – **I**ntranet.
b) **E**laboração – **T**reinamento – **I**nfraestrutura – **P**lanejamento – **I**mplantação.
c) **E**nergia – **T**elecomunicações – **I**nfraestrutura – **P**essoas – **I**nformática.
d) **E**letricidade – **T**ransportes – **I**nformações – **P**rodutos – **I**nternet.
e) **E**nergia – **T**ransmissões – **I**ntranet – **P**rocessos – **I**nternet.

016. (FCC/TCM-PA/TÉCNICO EM INFORMÁTICA/2010) Um Plano de Continuidade de Negócios (PCN) é um conjunto de três outros planos:

a) Plano Orçamentário de TI (POTI), Plano de Contingência Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

b) Plano de Administração Financeira (PAF), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

c) Plano de Administração Financeira (PAF), Plano de Contingência Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

d) Plano de Gerenciamento de Crises (PGC), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

e) Plano Estratégico de TI (PETI), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

017. (FCC/MPE-AP/ANALISTA MINISTERIAL/TECNOLOGIA DA INFORMAÇÃO/2012) O plano de continuidade do negócio deve

a) ter a mesma definição e desenvolvimento para todas as organizações e utilizar uma abordagem genérica, já que dessa forma poderá abranger todos os aspectos críticos que causam impactos negativos ao negócio.

b) ser eficiente e eficaz, ser mantido atualizado e ser testado periodicamente contando com a participação de todos os envolvidos.

c) ser do conhecimento apenas da alta administração que deve conhecer e aprovar as ameaças e riscos que estão fora do escopo do plano.

d) ser elaborado de forma que possibilite seu funcionamento em condições perfeitas, em nível otimizado, garantindo que não haja a possibilidade de incidentes que gerem impactos financeiros ou operacionais.

e) prever um plano para recuperação de desastre elaborado apenas em situações em que não haja perda de recursos, apesar da imagem da organização ser afetada, por exemplo, pela falha de um produto.

018. (FCC/MPE-PE/ANALISTA MINISTERIAL/INFORMÁTICA/2012) Convém que o processo de planejamento da continuidade de negócios considere:

I – Identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio.

II – Identificação da perda aceitável de informações e serviços.

III – Implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários.

IV – Educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise.

Está correto o que consta APENAS em

a) I, II, III e IV.
b) I, II e III.
c) II e III.
d) I e IV.
e) II e IV.

019. (FCC/TCE-AP/ANALISTA DE CONTROLE EXTERNO/TECNOLOGIA DA INFORMAÇÃO/2012) Com relação ao Plano de Continuidade de Negócio é INCORRETO afirmar:
a) Deve ser elaborado um Plano de Continuidade de Negócio que possibilite que a organização funcione em um nível aceitável para sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem
b) O desenvolvimento do Plano de Continuidade de Negócio deve ser específico para cada organização, pois deve ser baseado em uma análise de impacto no negócio caso ocorra uma indisponibilidade dos recursos de informação.
c) A alta administração e os acionistas da organização não precisam conhecer e aprovar as ameaças e riscos que estão fora de cada versão do Plano de Continuidade de Negócio, pois esses aspectos são definidos e homologados pela gerência de TI.
d) O Plano de Continuidade de Negócio deve ser eficiente/eficaz, mantido atualizado e testado periodicamente com a participação de todos os envolvidos.
e) Seu objetivo é o planejamento de ações para serem executadas quando da ocorrência de uma situação de contingência, de maneira a garantir que a organização mantenha suas atividades críticas em um nível previamente definido pela área de negócio e direção como aceitável.

020. (FCC/INFRAERO/ANALISTA/SEGURANÇA DA INFORMAÇÃO/2011) Sobre a Gestão da Continuidade do Negócio, é correto afirmar:
a) As cópias dos Planos de Continuidade do Negócio devem estar atualizadas mas não precisam ser protegidas no mesmo nível de segurança como aplicado no ambiente principal. Outros materiais necessários para a execução do plano de continuidade do negócio devem estar armazenados no ambiente principal, em local de fácil acesso.
b) O processo de planejamento da continuidade de negócios deve considerar a implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários, sem dispensar atenção à avaliação de dependências externas ao negócio e aos contratos existentes.
c) Convém que uma estrutura de planejamento, para continuidade de negócios, contemple os requisitos de segurança da informação identificados e considere condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado.

d) É conveniente que cópias do plano de continuidade do negócio sejam guardadas no ambiente principal, em um local de fácil acesso.
e) Apesar de ser necessário atualizar os planos de continuidade do negócio regularmente, não é aconselhável que eles sejam testados com frequência para não impactar em aumento de custos para a área de TI.

021. (FCC/INFRAERO/ANALISTA DE SISTEMAS/SEGURANÇA DA INFORMAÇÃO/2011) O Plano de Continuidade do Negócio
a) não precisa ser testado antes que se torne realmente necessário, pois testes por si só implicam em riscos aos ativos de informação.
b) deve ser elaborado com base em premissas departamentais particulares do que é considerado importante ou não.
c) prioriza e estabelece as ações de implantação como resultado de uma ampla análise de risco.
d) define uma ação de continuidade imediata e temporária.
e) precisa ser contínuo, evoluir com a organização, mas não precisa ser gerido sob a responsabilidade de alguém como os processos organizacionais.

022. (INÉDITA/2021) As evidências podem ser divididas em 4 tipos, que são: evidência física, evidência documentária, evidência testemunhal e evidência analítica.

QUESTÕES DE CONCURSO

023. (CESPE/TRE-PR/TÉCNICO JUDICIÁRIO/APOIO ESPECIALIZADO/ESPECIALIDADE: OPERAÇÃO DE COMPUTADORES/2009) A criação de cópias de segurança é um procedimento básico para a continuidade do negócio e recuperação de desastres.

Sabemos que tanto em TI, quanto em outra área de negócio, **as cópias de segurança são imprescindíveis para a continuidade dos negócios**.

As informações são o **ativo** mais importante para as organizações, por isso a preocupação com a continuidade dos negócios deve ser uma constante. Deve ser estabelecido um ambiente que garanta a continuidade operacional de todos os processos críticos de TI e forme alta disponibilidade na reposição de serviços e sistemas críticos ao negócio da empresa.

O objetivo é garantir que em casos de sinistros e falhas em ambientes físicos/lógicos, as atividades não sejam interrompidas afetando os negócios da organização. Em ambientes corporativos, devem ser estabelecidas políticas de cópias de segurança (que devem ser constantemente testadas e armazenadas em locais seguros e diferentes do local de origem).

A fusão dos planos de contingência e dos planos de recuperação de desastres, formam a Gestão da Continuidade dos Negócios (GCN) que tem por objetivo garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, softwares, hardware, infraestrutura etc.) por ele utilizados.

Certo.

024. (CESPE/TCU/ANALISTA DE CONTROLE EXTERNO/AUDITORIA DE TI/2007) Um plano de continuidade de negócios distingue-se de um plano de recuperação de desastres por vários aspectos, entre os quais a maior ênfase no gerenciamento de riscos.

Planos de continuidade de negócios (PCNs) têm como propósito permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

Os PCNs são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização, e podem ser executados integral ou parcialmente e em qualquer etapa da resposta a um incidente.

Segundo ALASI (2006), **a fase de avaliação de riscos e análise de impactos no negócio compõe uma das etapas de elaboração de um PCN e tem como objetivo levantar as ameaças a que o negócio está exposto**; uma inspeção física é realizada nos sites em que há processamento de

dados ou operação de processos considerados críticos para o negócio, essa inspeção física busca controles de segurança física nas instalações.

De posse dessa análise e através de entrevistas com pessoas envolvidas com a manutenção e operação das instalações é possível fazer uma análise de risco que será base para implementação de controles que mitigam esses riscos e análise de uma possível estratégia de contingência.

Já a Análise de Impactos nos Negócios é feita buscando identificar os processos críticos que suportam a cadeia de valor, e qual impacto para o negócio caso as ameaças mapeadas venham a se concretizar.

O **plano de recuperação de desastres** (também conhecido como *Disaster Recovery Plan*) **é um plano focado exclusivamente na recuperação de ativos de TI danificados por uma catástrofe ou por uma falha de sistema.**

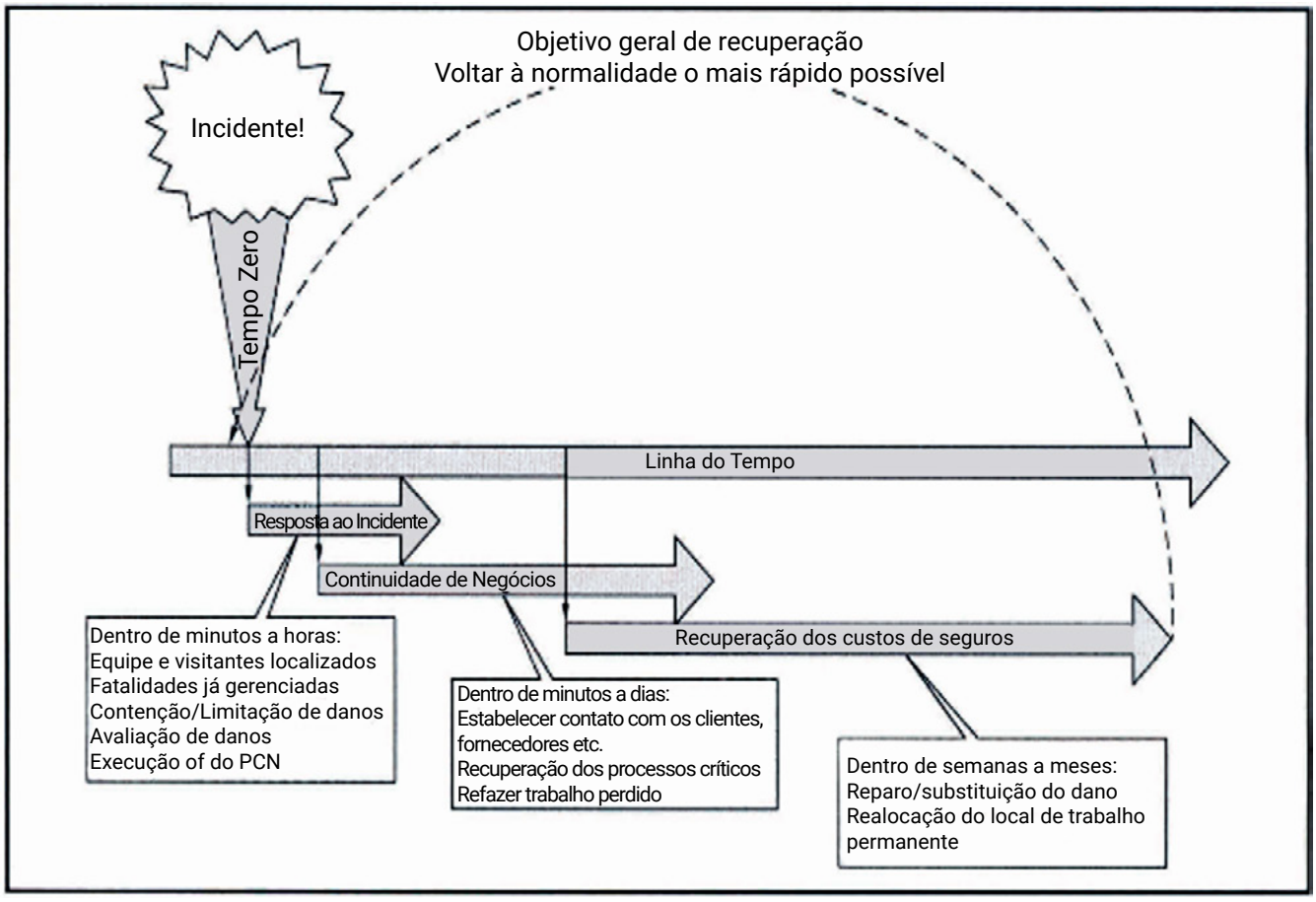


Figura. Linha do Tempo do Incidente
Fonte: (ABNT NBR ISO/IEC 15999-1:2007, p. 25)

Certo.

025. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO-TI/AMBIENTE OPERACIONAL/2009) Os planos de continuidade de negócios devem ser periodicamente testados. Ao testá-los, as falhas podem se dar por suposições incorretas, omissões ou mudanças em equipamentos ou pessoal.

Segundo a norma ABNT NBR 15999-1:2007, p. 33, é de suma importância que o programa de testes esteja consistente com o escopo do plano de continuidade de negócios, levando em conta a legislação e as regulamentações em vigor.
Os **testes podem** (norma ABNT NBR 15999-1:2007, p. 33):

- a) adiantar um resultado previsto, ou seja, que tenha sido antecipadamente planejado e incluído no escopo; ou
- b) permitir que a organização desenvolva soluções inovadoras.

Ainda, segundo a norma, **um programa de testes deve ser criado de forma que, ao longo do tempo, possa ser garantido objetivamente que o PCN funcionará como previsto quando necessário.**
A questão está correta. É difícil elencar TODAS as possibilidades de falhas, mas é certo que as falhas poderão ocorrer por: omissões (esqueceu-se de especificar algo correto), suposições incorretas ou mudanças em equipamentos ou pessoal.
Certo.

026. (CESPE/ANATEL/ANALISTA ADMINISTRATIVO-TI/AMBIENTE OPERACIONAL/2009) A responsabilidade pelo gerenciamento da continuidade dos negócios pode ser atribuída a um fórum de técnicos de segurança de tecnologia da informação.

A norma ABNT NBR 15999-1:2007, p. 11, prevê que se podem designar pessoas para cuidar do processo de gerenciamento da continuidade de negócios (GCN).
Algumas observações nesse quesito:

- **a participação da alta direção é fundamental para garantir que o processo de GCN seja corretamente introduzido, suportado e estabelecido como parte da cultura da organização;**
- **convém que a direção da organização aponte ou nomeie uma pessoa com a senioridade e autoridade apropriadas para ser responsável pela política de GCN e sua implementação; aponte ou nomeie um ou mais indivíduos para implementar ou manter o programa de GCN.**

Assim, o fórum de técnicos de segurança poderia atender à proposta, no entanto, esses técnicos entendem muito de TI, mas podem ter dificuldades no entendimento de questões pertinentes a outras áreas, que não sejam atreladas à área de TI. O ideal é que se tenha uma equipe **multidisciplinar**, e o CESPE queria isso nessa questão! A equipe responsável por gerenciar o processo de GCN não pode deter um tipo específico de conhecimento (tem que ter conhecimento da organização como um todo), para que esse processo seja mais produtivo.

Obs.: No edital referente a essa questão a norma 15999 não havia sido contemplada, somente a 27001 e a 27002 foram cobradas.

Errado.

---

027. (VUNESP/2014/TCE-SP/AGENTE DA FISCALIZAÇÃO FINANCEIRA/SISTEMAS, GESTÃO DE PROJETOS E GOVERNANÇA DE TI) Considerando as definições apresentadas na literatura a respeito da auditoria de sistemas, é correto afirmar que a auditoria de sistemas de informação

a) pode ser feita por profissionais internos à empresa proprietária dos sistemas.
b) não abrange os sistemas de bancos de dados da empresa.
c) não pode ser feita por profissionais externos à empresa proprietária dos sistemas.
d) não se importa com o tipo de controles existentes nos sistemas de informação.
e) somente deve ser feita uma vez a cada dois anos.

a) Certa. Isso mesmo! Tem-se nesse contexto a **Auditoria Interna**, **que ocorre através da verificação e avaliação dos sistemas e procedimentos internos pelo departamento interno, visando minimizar fraudes e erros variados.**
b) Errada. Na auditoria de TI (ou de sistemas de informação) **os auditores analisam os sistemas de informática, o ambiente computacional, os riscos associados à TI, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências.** Essa auditoria abrange, portanto, os sistemas de banco de dados da empresa e a assertiva é falsa.
c) Errada. A auditoria de sistemas de informação pode ser feita por profissionais externos à empresa proprietária dos sistemas. Importante destacar que o auditor interno não tem o mesmo nível de independência que um auditor externo, por estar ligado a uma hierarquia organizacional.
d) Errada. **A auditoria de sistemas de informação está calcada em confiança e em controles internos**. Estes visam confirmar se os controles internos foram implementados e se existem; caso afirmativo, se são efetivos.
e) Errada. Poderá ser feita sempre que necessária.
Letra a.

---

028. (CESPE/2010/ABIN/AGENTE TÉCNICO DE INTELIGÊNCIA/ÁREA DE TECNOLOGIA DA INFORMAÇÃO) Acerca de auditoria na área de tecnologia da informação (TI), julgue o item abaixo.
[A auditoria realizada em TI engloba a verificação de operações, processos, sistemas e responsabilidades].

A **Auditoria de TI engloba o exame das operações, processos, sistemas e responsabilidades de uma das áreas mais críticas e dispendiosas das empresas.** Verifica o retorno dos investimentos em Tecnologia da Informação. Exerce uma função preventiva e saneadora ao confirmar a veracidade e integridade dos registros e a confiabilidade das informações.

Certo.

029. (FCC/2014/TCE-GO/ANALISTA DE CONTROLE EXTERNO/ TECNOLOGIA DA INFORMAÇÃO/ADAPTADA) Em relação ao processo e organização da função de auditoria de TI, é correto afirmar:

[O gestor e a alta Administração são responsáveis pelos controles da organização, mas os processos de gestão de risco são delegados e controlados pela equipe de TI].

"O gestor e a alta administração são responsáveis pelos processos de gestão de risco e controles da organização" (IIA, IPPF, 2120-1).

Errado.

030. (FCC/2014/TCE-GO/ANALISTA DE CONTROLE EXTERNO/TECNOLOGIA DA INFORMAÇÃO/ADAPTADA) Em relação ao processo e organização da função de auditoria de TI, é correto afirmar:

[Auditores são parte do modelo governamental de controle interno, mas eles não são responsáveis pela implementação dos procedimentos de controle em uma organização. Este trabalho é do gestor].

Isso mesmo! **Auditores são parte do modelo governamental de controle interno**, mas eles **não** são responsáveis pela implementação dos procedimentos de controle numa organização. Este trabalho é específico do gestor, conforme destaca http://portal2.tcu.gov.br/ (*apud* INTOSAI – Padrões de Controle Interno, tradução livre).

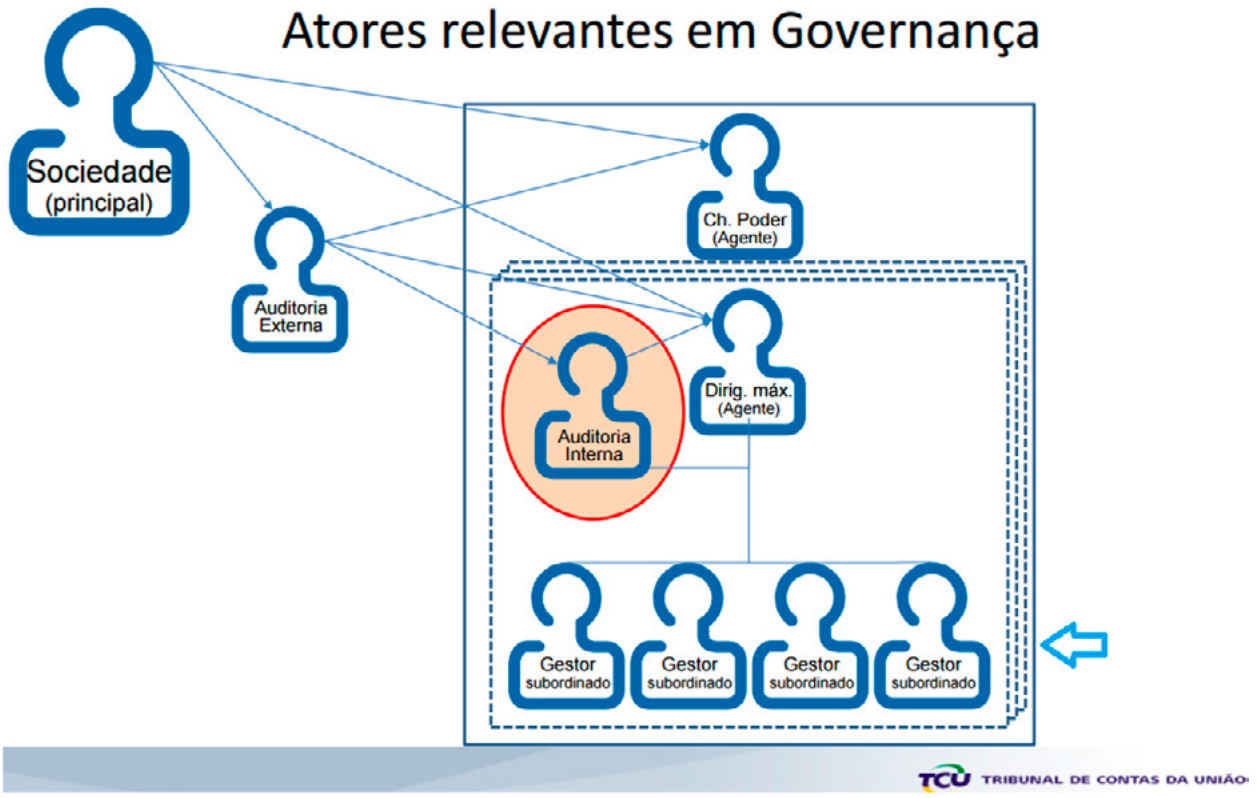


Figura. Atores Relevantes em Governança. Fonte: (Bemquerer, 2015)

Certo.

---

031. (FCC/2014/TRF-3ª REGIÃO/ANALISTA JUDICIÁRIO/INFORMÁTICA) O TRF da 3a Região necessita que seus sistemas sejam monitorados e eventos de segurança da informação sejam registrados. Com relação a esses registros, é correto afirmar que

a) todos os administradores de sistemas devem ter permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

b) registros (log) de auditoria devem incluir registros das tentativas de acesso a outros recursos e dados aceitos, mas não a dados rejeitados.

c) o estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros (log) de auditoria.

d) registros (log) de auditoria são úteis para a coleta e retenção de evidência, mas não podem ser guardados como parte da política de retenção de registros.

e) os registros (log) de auditoria devem ser produzidos e mantidos por um prazo máximo de um mês.

Conforme destaca TCU (2007), os **LOGS são REGISTROS CRONOLÓGICOS DE ATIVIDADES DO SISTEMA que possibilitam a reconstrução, revisão e análise dos ambientes e das atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim**.

São utilizados como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando. Com os dados dos logs, pode-se identificar e corrigir falhas da estratégia de segurança.

CertBr destaca que "muitas vezes os logs são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo".

a) Errada. Por conterem informações essenciais para a detecção de acesso não autorizado, **os arquivos de log devem ser protegidos contra alteração ou destruição por usuários (inclui-se aqui os administradores do sistema!) ou invasores que queiram encobrir suas atividades**.

b) Errada. Normalmente, os registros de log incluem:

- identificação dos usuários;
- datas e horários de entrada (logon) e saída do sistema (logoff);
- identificação da estação de trabalho e, quando possível, sua localização;
- registros das tentativas de acesso (aceitas e rejeitadas) ao sistema;
- **registros das tentativas de acesso (aceitas e rejeitadas) a outros recursos e dados**.

c) Certa. O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros (log) de auditoria. Ainda, cabe destacar que ao se analisar os logs, é importante

certificar-se do fuso horário (**timezone)** usado para registrar o horário dos eventos. O desconhecimento do timezone em que estão os logs pode facilmente invalidar uma análise e levá-lo a conclusões equivocadas (CertBr).

d) Errada. É justamente o contrário! **Os registros (log) de auditoria são úteis para a coleta e retenção de evidência**, e, portanto, **devem ser guardados como parte da política de retenção de registros.**

e) Errada. O prazo deve ser definido na política de segurança de acordo com as especificidades e objetivos da organização**.**

Letra c.

---

032. (FCC/ICMS-SP/2009) O trabalho da auditoria interna

a) tem maior independência que o de auditoria externa.

b) é responsável pela implantação e pelo cumprimento dos controles internos.

c) deve estar subordinado ao da Controladoria da empresa.

d) deve emitir parecer, que será publicado com as demonstrações contábeis.

e) deve efetuar a revisão e o aperfeiçoamento dos controles internos.

Conforme destaca Bemquerer (2015), a **auditoria interna** é uma atividade independente e objetiva que presta serviços de avaliação e de consultoria com o objetivo de adicionar valor e

melhorar as operações de uma organização. A auditoria auxilia a organização a alcançar seus objetivos através de uma abordagem sistemática e disciplinada para a **avaliação** e melhoria da eficácia dos **processos de gerenciamento de risco, controle e governança corporativa**. (IIA IPPF, tradução livre)

A atividade de auditoria interna tem que **avaliar** a adequação e eficácia dos **controles** em resposta aos **riscos** relativos à **governança** da organização, **operações** e **sistemas de informação**, quanto à (Bemquerer, 2015):

- confiabilidade e integridade da informação financeira e operacional;
- eficiência e eficácia das operações;
- salvaguarda dos ativos;
- conformidade com as leis, regulamentos e contratos (IIA IPPF, Padrão 2130.A1, tradução livre).

À semelhança da auditoria interna, a função das Entidades de Fiscalização Superiores (auditoria externa) é **avaliar a eficácia dos processos de governança, gestão e controles** dos seus jurisdicionados (INTOSAI ISSAI 9100 Governança; tradução livre).

Vamos às assertivas:

a) Errada.

> Quanto à independência, **a auditoria interna possui menor grau de independência e a auditoria externa maior grau de independência.**

Alguns autores afirmam que a auditoria externa possui independência e auditoria interna possui autonomia. Assim, o trabalho da auditoria interna tem **menor independência que o de auditoria externa**.

b) Errada. Os auditores internos examinam e contribuem para a eficácia do sistema de controle interno através de suas avaliações e recomendações, mas não possuem responsabilidade primária pelo planejamento, implantação e manutenção do processo.

c) Errada. O trabalho da auditoria interna deve estar subordinado à alta administração da empresa, para assegurar a sua independência das demais áreas da empresa.

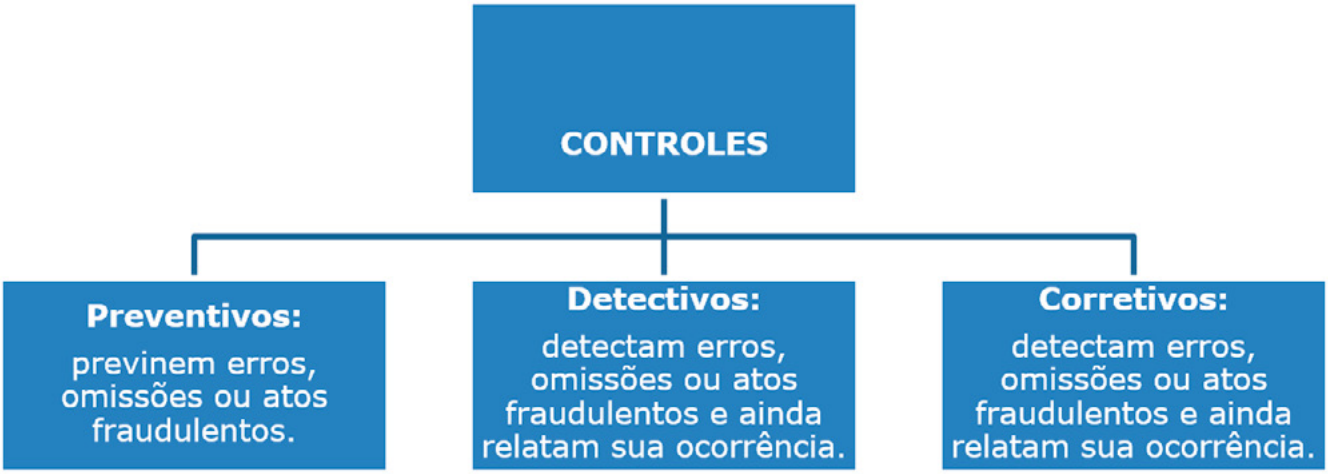
d) Errada. A auditoria interna não emite parecer sobre as demonstrações contábeis. Este é o papel da auditoria externa.

e) Certa. A auditoria interna efetua a revisão e o aperfeiçoamento dos controles internos da organização, para auxiliá-la a atingir seus objetivos.

Letra e.

033. (INÉDITA/2021) Em auditoria, os controles detectivos previnem erros, omissões ou atos fraudulentos, enquanto que os controles corretivos são utilizados para reduzir impactos ou corrigir erros uma vez detectados.

Controle é a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos ou produtos para que as atividades ou produtos não se desviem das normas preestabelecidas.
Os controles podem ser:



A assertiva está errada, pois são os controles preventivos que previnem erros, omissões ou atos fraudulentos!
Errado.

034. (INÉDITA/2021) Os principais critérios usados para a seleção de objeto são os de materialidade, relevância e vulnerabilidade a riscos.

A afirmativa está correta, em conformidade com o Manual de Procedimentos de Auditoria do TCE-CE. Os principais critérios usados para a seleção de objeto de auditoria são: **materialidade, relevância** e **vulnerabilidade a riscos.**
Vamos à distinção entre cada um deles:

Materialidade	**A seleção deve levar em consideração os valores financeiros envolvidos no objeto de auditoria**, importando ressaltar, porém, que **nem sempre os benefícios de um trabalho de auditoria são vinculados apenas aos recursos financeiros envolvidos.** Aperfeiçoar processos e procedimentos dos objetos com alta materialidade possibilita gerar economia ou eliminar desperdícios.

Relevância	Indica que **as auditorias selecionadas devem procurar responder, quando possíveis, questões de interesse do Tribunal de Justiça do Estado do Ceará e da própria Sociedade,** possibilitando **agregação de valor** quanto a produzir novos conhecimentos e perspectivas sobre o objeto de auditoria.
Vulnerabilidade a Riscos	Este critério se **relaciona às possíveis vulnerabilidades ou propriedades intrínsecas do objeto de auditoria que podem estar associadas à ocorrência de eventos como fraudes, desvios e gestão ineficiente**.

Certo.

035. (INÉDITA/2021) Planejamento é a fase do trabalho realizado no órgão auditado. Trata-se da fase de aplicação dos procedimentos de auditoria, objetivando a obtenção de provas ou evidências que deverão constar no relatório de auditoria. É nessa fase que o auditor realiza fundamentalmente seus exames.

FASE	DESCRIÇÃO
Planejamento	É a fase em que o auditor obtém uma visão geral do trabalho a ser realizado, ou seja, definem-se as finalidades da ação a ser realizada e identificam-se as questões que deverão ser respondidas (Araújo, 2001).
Execução	**É a fase do trabalho realizado no órgão auditado.** Araújo (2001) define a execução como sendo a fase de aplicação dos procedimentos de auditoria, objetivando a obtenção de provas ou evidências que deverão constar no relatório de auditoria. É nessa fase que o auditor realiza fundamentalmente seus exames.
Emissão e divulgação de relatórios	Segundo Arima (*et. al.*, 2006) os **relatórios** contribuem para que o auditor descubra as irregularidades de processamento de sistemas de informação, apurando a qualidade da mesma e auxiliando na busca por critérios para seleção de informações necessárias para a avaliação. Acerca da emissão de relatório, Imoniana (2005, p. 31) dispõe: **o auditor de TI deve prover um relatório, em forma apropriada, para os destinatários, por ocasião da conclusão do trabalho de auditoria.** O relatório de auditoria deve apresentar escopo, objetivos, período de abrangência, natureza e extensão do trabalho executado. Deve identificar a organização, os usuários desejáveis e quaisquer restrições à sua circulação. Ainda, neste relatório, devem-se incluir as observações, conclusões, recomendações e quaisquer ressalvas ou conceitos que o auditor possua a respeito da auditoria.

Follow-up (Acompanhamento)	Após a entrega do relatório de auditoria e da ciência de seu conteúdo pelo órgão jurisdicionado, faz-se necessário realizar um **acompanhamento** para verificar a efetiva adoção das recomendações e determinações realizadas.

Errado.

036. (FCC/2012/TRE-SP/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS) Sobre as etapas do processo de auditoria interna de TI é correto afirmar que possui 6 etapas: Planejamento, Análise, Projeto, Execução, Relatório e Plano de Ação.

As quatro FASES DA AUDITORIA DE TI, comumente destacadas na literatura, são:
-Planejamento;
-Execução;
-Emissão e divulgação de relatórios (reporte dos resultados);
-Follow-up (acompanhamento/plano de ação).

Errado.

037. (FCC/2012/FEMPERJ/TCE-RJ/ANALISTA DE CONTROLE EXTERNO/TECNOLOGIA DA INFORMAÇÃO) Uma auditoria de TI deve estar atenta:

a) aos parâmetros acordados de entrega de serviços, pois a área de TI deve estar estruturada adequadamente para atender aos SLAs (Service Level Agreement) nos contratos;

b) ao processo de gerenciamento de mudanças, para garantir que, depois de um incidente imprevisível, os serviços de TI possam ser restaurados dentro dos limites de tempo preestabelecidos;

c) ao planejamento orçamentário de TI, que deverá acompanhar a execução do planejamento institucional, não podendo haver ajustes em decorrência de variações no suprimento orçamentário ou de mudanças nas demandas;

d) à terceirização de serviços de TI, que não pode ser utilizada em atividades-meio da instituição;

e) ao uso de técnicas de auditoria assistidas por computador, pois essa decisão só pode ser tomada na fase de planejamento e não no decorrer dos exames.

Auditoria é uma atividade que engloba o exame de operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões. (Fonte:http://www.ituiutaba.uemg.br/sistemas1/material/seg_aud_sist/auditoria.pdf).

A **auditoria da tecnologia da informação (TI)** é fundamental para as organizações modernas, por se tratar de uma atividade que tem por base a análise detalhada dos dados de uma empresa, abrangendo a verificação de várias informações que a mesma produz, com objetivos específicos que podem contribuir para se evitar erros ou mesmo fraudes na mesma.

Vale referenciar aqui o disposto por Imoniana (2005), que destaca a **Auditoria de TI como *essencialmente operacional, por meio das qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade auditada, indicando seus pontos fortes e/ou deficiências*.** *Em alguns países é conhecida como auditoria de informática computacional ou de sistemas*.

Dentre os itens mencionados na questão, a auditoria de TI deve estar atenta aos parâmetros acordados de **entrega de serviços**, pois a área de TI deve estar estruturada adequadamente para atender aos os níveis de serviço (**SLA** – ***Service Level Agreement***, **ou acordo de nível de serviço**) estabelecidos nos contratos.

O **SLA** (ou **acordo de nível de serviço**) descreve o serviço de TI, documenta metas de nível de serviço e especifica as responsabilidades do provedor de serviço de TI e do cliente. Um único acordo pode cobrir múltiplos serviços de TI ou múltiplos clientes.

Letra a.

---

038. (FCC/2008/TCE-CE/ANALISTA DE CONTROLE EXTERNO/AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO) Uma auditoria deve avaliar uma amostra de acordos de nível de serviço, concluídos e vigentes, firmados com os

a) clientes, apenas.
b) usuários, clientes e provedores de serviços, apenas.
c) clientes e provedores de serviços, apenas.
d) usuários, clientes e funcionários de TI, apenas.
e) usuários, clientes, provedores de serviços e funcionários de TI.

Uma **auditoria** deve avaliar uma amostra de **acordos de nível de serviço**, concluídos e vigentes, firmados com os **usuários, clientes e provedores de serviços, apenas.**

Um nível de serviço descreve o nível de atendimento aos requisitos estabelecidos para o serviço. O serviço é mantido em operação e funcionamento de acordo com os níveis de serviço estabelecidos para gerar os resultados esperados.

Letra b.

---

039. (INÉDITA/2021) As abordagens mais comuns para auditar as informações em ambientes de tecnologia de informação são: abordagens ao redor do computador; através do computador; e com o computador.

Conforme destaca Imoniana (2008), para auditar as informações em ambiente de TI, o auditor poderá desenhar as abordagens que lhe convêm. **As abordagens mais comuns são: abordagens ao redor do computador; através do computador; e com o computador.**

- A **abordagem ao redor do computador** não envolve a utilização de muitas tecnologias de informação e sim o exame de níveis de anuência associados à aplicação de controles organizacionais, conforme dispõe Imoniana (2008). Trata-se de uma abordagem que não é muito indicada para ambientes complexos, mas é muito *útil em sistemas menores*, que não exijam um conhecimento mais profundo de TI.
- A **abordagem através do computador** vai além da verificação de documentos, havendo o acompanhamento e análise de dados por meio do computador (IMONIANA, 2008).
- Quanto à **abordagem com o computador**, pode-se dizer que permite uma análise com maior precisão, por meio da compilação do processo, possibilitando a utilização das "capacidades lógicas e aritméticas do computador para verificar os cálculos das transações econômicas e financeiras, dentre outros" (IMONIANA, 2008).

Certo.

040. (INÉDITA/2021) Conforme destaca o TCE-GO, no relatório "Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual", com o aumento da importância estratégica da área de TI, houve uma busca pela aplicação de modelos de governança, com o objetivo de tornar a área controlável, com resultados mensuráveis e orientada aos objetivos do negócio da instituição. Nesse contexto, a auditoria de TI pode ser utilizada para que se possa verificar um ou vários aspectos da Governança de TI de uma organização.

Nesta perspectiva, segundo TCE-GO, "a auditoria de TI consiste em verificar um ou vários aspectos da Governança de TI de uma organização. Assim, uma auditoria de TI pode, por exemplo, avaliar desde controles de acesso lógico ao ambiente de TI, por meio de análise de vulnerabilidade, até a segurança de sistemas de informação; ou ainda, verificar se a contratação de bens e serviços de TI é feita de acordo com as normas da organização e a legislação vigente.

***A auditoria de TI, tem como função principal** avaliar o processo de gestão, no que se refere aos seus diversos aspectos, tais como a governança corporativa, gestão de riscos de TI e procedimentos de aderência às normas regulatórias, **apontando eventuais desvios e vulnerabilidades, como também oferecendo alternativas de soluções para esses diversos problemas**", afirma o presente relatório do TCE-GO.*

Certo.

041. (FCC/2012/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS) São objetivos da auditoria, EXCETO:

a) Assegurar a adequação do sistema de controles que está implantado e que está sendo utilizado.

b) Determinar se os recursos estão sendo utilizados em função da análise de custo e benefício.

c) Gerenciar os riscos da organização e tomar ações para solucionar os problemas porventura identificados.

d) Checar se os ativos estão salvaguardados apropriadamente.

e) Revisar a integridade, confiabilidade e eficiência do sistema de informação e dos relatórios financeiros nele produzidos.

A auditoria de TI **visa confirmar se os controles internos foram implementados e se existem; caso afirmativo, se são efetivos** (Imoniana, 2008). A auditoria não estará relacionada a ações de nível operacional ou de gestão, como a de gerenciar os riscos da organização e tomar ações para solucionar os problemas ora identificados.

→ São **objetivos da auditoria**:

- Assegurar a adequação do sistema de controles que está implantado e que está sendo utilizado.
- Determinar se os recursos estão sendo utilizados em função da análise de custo e benefício.
- Checar se os ativos estão salvaguardados apropriadamente.
- Revisar a integridade, confiabilidade e eficiência do sistema de informação e dos relatórios financeiros nele produzidos.

Certo.

042. (ESAF/2005/AFRFB) Analise as seguintes afirmações relacionadas à Segurança da Informação.

I – Um plano de contingência consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não consigam evitar.

II – Entende-se por Política de Segurança um conjunto de regras que pode ser aplicado a qualquer empresa, que não necessite de processos de revisão e que possa atuar de forma independente em qualquer setor desta empresa.

III – Um Proxy Server é um sistema que atua como intermediário entre duas pontas de uma conexão, evitando a comunicação direta entre elas.

IV – A segurança da informação de uma organização deve ser de exclusiva responsabilidade do setor de segurança, deve ter uma estrutura de segurança estática e, uma vez implementada, todas as informações serão consideradas seguras.

Indique a opção que contenha todas as afirmações verdadeiras.

I – e II

b) II e III

c) III e IV

d) II e IV

e) I e III

Item I. A política de segurança deve assegurar a existência de um plano de contingência capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, incluindo também as atividades de teste e manutenção do documento. Em seu conteúdo devem ser abordados diversos aspectos com relação à avaliação de risco e impacto no negócio. A política deve ressaltar que, o plano a ser desenvolvido, resultará num conjunto de documentos onde estarão registradas as ações relativas às adequações da infraestrutura e às alterações nos procedimentos. Item **VERDADEIRO**.

Item II. A política de segurança deve ser revisada e atualizada sempre que necessário. Deve haver análise periódica da efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados! Item **FALSO**.

Item III. O Proxy Server pode gerenciar gerencia o tráfego da Internet de/para uma rede local e pode oferecer outros recursos, como o cache de documentos e o controle de acesso. Item **VERDADEIRO**.

Item IV. Que absurdo!!! “A segurança é responsabilidade de todos nós”, eu até uso essa frase em campanhas de segurança dentro da empresa em que trabalho. A estrutura é bem dinâmica, e obter 100% de segurança é uma utopia!!! Item **FALSO**.

Letra e.

GABARITO

1. a
2. C
3. b
4. b
5. e
6. a
7. e
8. e
9. e
10. d
11. e
12. b
13. E
14. e
15. c
16. d
17. b
18. a
19. c
20. c
21. c
22. C
23. C
24. C
25. C
26. E
27. a
28. C
29. E
30. C
31. c
32. e
33. E
34. C
35. E
36. E
37. a
38. b
39. C
40. C
41. C
42. e

REFERÊNCIAS

ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no Desenvolvimento de Software**. Rio de Janeiro: Campus, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 22301.** Rio de Janeiro. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 22301.** Rio de Janeiro. 2020.

CERTBR. **Cartilha de Segurança para Internet**. Versão 4.0. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. 2012.

QUINTÃO, P. L. **Notas de aula da disciplina "Tecnologia da Informação"**. 2021.

QUINTÃO, P. L. **Informática-FCC-Questões Comentadas e Organizadas por Assunto**, 3ª. Edição. Ed. Gen/Método, 2014.

QUINTÃO, P. L. **1001 Questões Comentadas de Informática Cespe**, 2ª. Edição. Ed. Gen/Método, 2017.

MAUSER, D; Diógenes, y. **Certificação Security +** – 2ª edição. 2013.

NAKAMURA, E. T., GEUS, P.L. **Segurança de Redes em Ambientes**

Cooperativos. Ed. Novatec. 2007.

RAMOS, A.; BASTOS, A.; LAYRA, A. **Guia Oficial para Formação de Gestores em Segurança da Informação**. 1. ed. Rio Grande do Sul: ZOUK. 2006.

STALLINGS, W., **Criptografia e Segurança de Redes: Princípios e**

Práticas., 4. ed. São Paulo: Pearson Prentice-Hall, 2008.

SCHNEIER, B., **Applied Cryptography: Protocols, Algorithms and Source Code in C**. 2. ed. John Wiley & Sons, 1996.

Patrícia Quintão

Mestre em Engenharia de Sistemas e computação pela COPPE/UFRJ, Especialista em Gerência de Informática e Bacharel em Informática pela UFV. Atualmente é professora no Gran Cursos Online; Analista Legislativo (Área de Governança de TI), na Assembleia Legislativa de MG; Escritora e Personal & Professional Coach.

Atua como professora de Cursinhos e Faculdades, na área de Tecnologia da Informação, desde 2008. É membro: da Sociedade Brasileira de Coaching, do PMI, da ISACA, da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da ABNT, responsável pela elaboração das normas brasileiras sobre gestão da Segurança da Informação.

Autora dos livros: Informática FCC - Questões comentadas e organizadas por assunto, 3ª. edição e 1001 questões comentadas de informática (Cespe/UnB), 2ª. edição, pela Editora Gen/Método.

Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista de TI/Suporte, PRODABEL; Analista do Ministério Público MG; Analista de Sistemas, DATAPREV, Segurança da Informação; Analista de Sistemas, INFRAERO; Analista - TIC, PRODEMGE; Analista de Sistemas, Prefeitura de Juiz de Fora; Analista de Sistemas, SERPRO; Analista Judiciário (Informática), TRF 2ª Região RJ/ES, etc.

@coachpatriciaquintao **/profapatriciaquintao**

@plquintao **t.me/coachpatriciaquintao**