

## **Aula 0: Aula Demonstrativa/Apresentação do Curso**

Salve, salve, Galera! Prof. Walter Cunha novamente na área...

É com muita satisfação que damos início ao curso de Gestão de Riscos de Segurança da Informa (ISO 27005) em Questões. Se você ainda não sabe, a Norma ISO 27005 é figurinha carimbada em praticamente todos os concursos de Tecnologia da Informação. Portanto, vamos nos dedicar de modo a não darmos mole e perdermos esses preciosos pontos!

Primeiramente, gostaria de me apresentar:

Aos que ainda não me conhecem, sou o Prof. Walter Cunha, natural de Fortaleza-CE, pós-graduado em Gerência de Projetos pela Fundação Getúlio Vargas (FGV) e Engenheiro Eletrônico pelo Instituto Tecnológico de Aeronáutica (ITA).

Atualmente, ocupo o cargo de Auditor Federal de Finanças e Controle da Controladoria-Geral da União (AFCF), aprovado na especialidade de Tecnologia da Informação, lotado em Brasília-DF, mais especificamente atuando na área de Governança Corporativa. A maior parte do meu tempo hoje é destinada a entender, harmonizar e gerar valor a partir da aplicação adaptada dos mais diversos frameworks de mercado e de governo. Muito papel? Sim, mas é o que acontece naturalmente quando se migra da do nível técnico-operacional para o de gestão estratégica. Particularmente, eu me adaptei muito bem, obrigado!

Antes de assumir o meu cargo atual, ocupei durante três anos o cargo de Analista Tributário da Receita Federal do Brasil (ATRFB), no qual exerci a atividade de Analista de Projetos de Infraestrutura de TI. No entanto, a minha carreira profissional começou bem antes, em 2000, como Oficial Engenheiro Eletrônico da Força Aérea Brasileira (FAB), em Manaus-AM, onde permaneci até o final da implantação do Sistema de Vigilância da Amazônia (SIVAM), em 2006. Lá, atuei predominantemente na área de Redes de Computadores, minha área técnica de origem.

No mundo dos concursos, depois de muita dedicação, consegui alguns resultados expressivos: 2005 – Analista de Tecnologia da Informa na SEFAZ-AM; 2006 – Analista Tributário da Receita Federal do Brasil TI (1o lugar da 3a Região Fiscal); 2006 – Analista de Finanças e Controle da Controladoria-Geral da União; 2007 – Analista de Tecnologia da Informa na SEFAZ-CE; 2009 – Analista de Finanças e Controle da Controladoria-Geral da União (sim, de novo! E antes da mudança de nomenclatura para Auditor), onde, se tudo continuar correndo bem, planejo aposentar a caneta.

Confesso ter relutado muito antes de aceitar o desafio de voltar a elaborar cursos escritos, mas, dadas as minhas dificuldades atuais em gravar videoaulas em casa, esta opção se mostrou a válvula ideal para eu continuar produzindo.

Atualmente, mantenho também um grupo de apoio (MasterMind) via slack (<https://wc-teamgroup.slack.com/>), ao qual os alunos fiéis tem acesso livre. Entenda-se por alunos fiéis aqueles que adquirem de forma oficial os meus cursos e/ou participam de minhas aulas presenciais, e/ou, mais recentemente, apoiam o meu patreom (<https://www.patreon.com/timasters>).

Quanto a este curso, os objetivos são não só consolidar o conhecimento das disciplinas, mas derrubar alguns mitos e mostrar que, com postura e tática adequadas, é possível estar bem preparado para concorrer em qualquer certame, independentemente da banca.

Hoje, apresentarei uma aula demonstrativa para que vocês tenham ideia de como será a estrutura do curso, que será dividido em 5 (cinco) aulas, conforme a seguinte distribuição:

- Aula 0: Banca CESPE Parte I;
- Aula 1: Banca CESPE Parte II;
- Aula 2: Banca CESPE Parte III;
- Aula 3: Banca FCC;
- Aula 4: Outras Bancas.

A maioria das Questões apresentadas aqui foram retiradas do site Gabaritou (<https://www.gabaritou.com.br/>), onde rotineiramente posto as minhas considerações. Após a apresentação da questão, colocarei os comentários e argumentos explicando o gabarito. E, ao final de cada aula, serão disponibilizadas todas as questões em sequência, sem as respostas, caso você queira imprimi-las e praticá-las antes de olhar os gabaritos e explicações.

Importante ressaltar que a abordagem será a mais objetiva possível nos temas, sem divagações ou retóricas desnecessárias – o “academicismo” e o “praticismo” serão evitados ao máximo. A meta será o “concursismo”! Pois, de fato, é o que aprova!

Por fim, cabe lembrar que este é um curso em QUESTÕES, como tal, com limitações para comentários extensos. Portanto, o foco será aprender como resolver as questões da forma como elas são cobradas pelas principais bancas. É claro que certamente não deixaremos de abordar os conceitos fundamentais de cada assunto abordado.

Sem mais delongas, segue a aula demonstrativa Gestão de Riscos de Segurança da Informação (27005) em Questões:

**ATENÇÃO!** Esta é apenas uma aula demonstrativa para que você possa avaliar o nosso trabalho.

1. (CESPE/TCE-PI 2016) Considere que a equipe composta por quatro analistas de sistemas de um órgão do judiciário federal brasileiro deva desenvolver um plano de implantação da gerência de riscos de segurança da informação nesse órgão. Acerca das atividades que podem ser realizadas pela equipe, e considerando os conceitos de gerência de riscos, de classificação e controle dos ativos de informação, e a norma ISO/IEC 27005, é correto afirmar que essa equipe

*A deve produzir ou obter a lista de processos de negócios aos quais estarão vinculados os demais ativos de informação a serem identificados na atividade de identificação de riscos*

*B deve particionar entre os quatro membros a responsabilidade pelo desempenho dos seguintes papéis, entre outros: identificação e análise das partes interessadas, estabelecimento de ligações com as funções de gerência de riscos de alto nível, especificação dos critérios para a avaliação dos riscos, estimativa de impactos e aceitação do risco para a organização*

*C deve aplicar uma metodologia de análise quantitativa de riscos, excluindo a aplicação de uma metodologia qualitativa*

*D deve implantar o sistema de gestão de segurança da informação, antes de desenvolver o plano de gestão de riscos*

*E deve particionar entre seus quatro membros a responsabilidade da execução simultânea das seguintes atividades: definição do escopo, identificação dos riscos, tratamento dos riscos e comunicação do risco*

Comentários:

- a) CORRETA. A. Segundo a ISO 27005:2011, "8.2.2 Identificação dos ativos Saída: Uma lista de ativos com riscos a serem gerenciados, e uma lista dos processos de negócio relacionados aos ativos e suas relevâncias";

- b) ERRADA. Estimar impactos e aceitar riscos convém serem feitos pela equipe de negócio;
- c) ERRADA. Excluir a análise qualitativa não faz sentido, uma vez que ela é básica. E não há essa obrigação;
- d) ERRADA. Não há essa ordem. Inclusive é comum o PGR servir de insumo para o SGSI;
- e) ERRADA. Essas etapas são sequenciais, e não simultâneas.

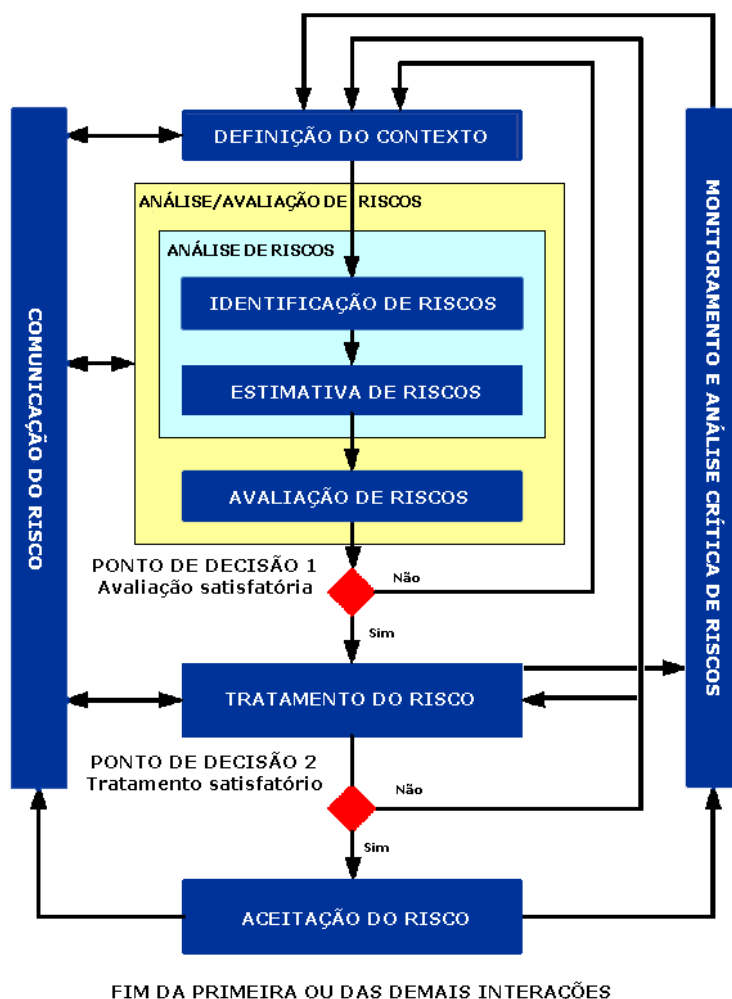
Gabarito Oficial: A

**2. (CESPE/TCE-PA 2016) À luz da NBR ISO/IEC 27005:2011, que dispõe diretrizes para o processo de gestão de riscos de segurança da informação (GRSI), julgue os itens a seguir.**

***O processo de GRSI é iterativo tanto para o processo de avaliação de riscos quanto para as atividades de tratamento de risco***

Comentários:

Questão polêmica. Para mim, item CORRETO. Para o CESPE, item ERRADO. Tudo em gestão de riscos é iterativo! Não faz sentido dizer o contrário. Até mesmo a base das normas ISO, desde sempre, é a ideia de processos, ciclo PDCA e melhoria contínua. Veja a Figura da norma ISO 27005 que mostra a relação entre as atividades do processo de GRSI:



Ora, na figura vemos que há um ponto de decisão após a etapa de Avaliação e também um ponto de decisão após a etapa de Tratamento. Em ambos os casos, se a Avaliação ou o Tratamento não forem satisfatórios, o ciclo recomeça (com uma nova iteração) a partir da atividade de "Definição do Contexto". Na verdade, bastaria pensar de forma bem óbvia. Trata-se de um processo. O processo, por definição, é composto por atividades e obedece a um ciclo de melhoria contínua. Melhoria contínua envolve várias iterações no famoso ciclo Plan Do Check Act.

O único erro que vejo neste item (o qual não tem sido a base das polêmicas), é se referir à "avaliação de riscos" como um processo e ao "tratamento de riscos" como uma atividade. Avaliação de riscos, segundo a norma, seria uma atividade do processo de GRSI. Mas, mesmo isso é relativo (um processo pode ser composto por subprocessos). Enfim, questão péssima. daquelas que quanto mais você conhece o assunto, mais difícil fica de responder. E eu prefiro dizer que, no caso, a questão está mal elaborada e o examinador não

sabia direito o que estava fazendo. Como estive do outro lado durante muito tempo, posso dizer que isso é possível sim e acontece muito.

Gabarito Oficial: ERRADO, contudo discordamos da Banca.

**3. (CESPE/TJDF 2016) Com relação à gestão de segurança da informação, julgue os itens a seguir.**

***A norma ISO/IEC 27005 determina que, se uma ameaça tem valor constante, o impacto resultante será o mesmo para todos os ativos, independentemente de qual deles seja afetado.***

Comentários:

O processo de GRSI é iterativo tanto para o processo de avaliação de riscos quanto para as atividades de tratamento de risco.

O texto é meio formal (como em toda a Norma), mas a ideia é muito simples. Costumo pedir para os alunos decorarem uma "formulinha" macete que ajuda muito:

$$\text{Risco} = [(\text{Ameaça} * \text{Vulnerabilidade} * \text{Impacto}) / \text{Contra-Medidas}].$$

Dela tiramos muitas conclusões. Por exemplo, se a ameaça for nula, o risco também será nulo. Se a vulnerabilidade aumenta, o risco também aumenta. Etc. Agora, veja a questão.... Ela diz, em resumo, que se uma ameaça é constante, o impacto também será constante. Na verdade, não, pois são coisas independentes. O impacto tem a ver com o valor do ativo. Se uma ameaça for constante, para dois ativos com valor diferente, teremos riscos diferentes, óbvio (o ativo de maior valor, se corrompido, causa um impacto maior, claro).

Para sermos mais formais, veja a letra da Norma ISO 27005:2011: "8.2.3 *Identificação das ameaças - Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados.*"

Gabarito Oficial: ERRADO.

**4. (CESPE/STJ 2015) Com base nas normas ISO 27001, ISO 27002, ISO 27003, ISO 27004 e ISO 27005, relativas à segurança de ativos de informação das organizações, julgue os itens a seguir.**

***De acordo com a norma ISO 27005, na estimativa de riscos, podem ser aplicadas metodologias qualitativas para a identificação de riscos.***

Comentários:

Conforme a própria norma:

### *8.3 Análise de riscos*

#### *8.3.1 Metodologias de análise de riscos*

*A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Uma metodologia para a análise pode ser qualitativa ou quantitativa ou uma combinação de ambos, dependendo das circunstâncias.*

Gabarito Oficial: CERTO.

**5. (CESPE/MEC 2015) Com relação a norma ISO/IEC 27005, julgue os itens subsequentes.**

***O conteúdo da norma ISO/IEC 27005 influenciou a criação de outras normas, tais como a ISO/IEC 27001 e ISO/IEC 27002.***

Comentários:

Na verdade, a 27005 é posterior a norma 27002, a qual tomou como base a norma ISO/IEC 17799:2005.

Gabarito Oficial: ERRADO.

**6. (CESPE/TCU 2015) Com relação à gestão de riscos, julgue os próximos itens.**

***Conforme a NBR ISO/IEC 27005:2011, para a avaliação dos riscos de segurança da informação na organização, convém que os critérios de avaliação sejam desenvolvidos considerando-se a criticidade dos ativos de informação envolvidos.***



Comentários:

*ISO 27005:2011:*

*7.2.2 Critérios para a avaliação de riscos*

*Convém que os critérios para a avaliação de riscos sejam desenvolvidos para avaliar os riscos de segurança da informação na organização, considerando os seguintes itens:*

*(...)*

*A criticidade dos ativos de informação envolvidos*

Gabarito Oficial: CERTO.

**7. (CESPE/TCU 2010) Julgue os itens subsequentes, relativos às Normas NBR ISO/IEC 15999 e 27005.**

***A norma NBR ISO/IEC 27005 prescreve que o gerenciamento de incidentes pode ser realizado iniciando-se com uma definição de contexto, seguido por uma análise e avaliação, tratamento, aceitação, comunicação, monitoramento e análise crítica dos incidentes.***

Comentários:

Em vez de “Gestão de Incidentes” deveria ser “Gestão de Riscos”.

Gabarito Oficial: ERRADO.

**8. (CESPE/TCE-ES 2013) Com relação à gestão de riscos, assinale a opção correta.**

***A O escopo da análise dos riscos deve sempre atuar sobre toda a organização.***

***B A NBR ISO/IEC 15999 estabelece as bases para a gestão de riscos em segurança da informação e a NBR ISO/IEC 27005 trata da gestão de continuidade de negócios.***

***C Gerenciar os riscos é um dos principais processos da gestão de segurança da informação, pois visa identificar, avaliar e priorizar riscos para, em seguida, se poder aplicar, de forma coordenada e econômica, os recursos para minimizar, monitorar e controlar a***



***probabilidade e o impacto de eventos negativos, de modo a se reduzir o risco a um nível aceitável.***

***D No sentido de ganhar agilidade na identificação, avaliação e priorização dos riscos, o gestor de segurança da informação pode deixar de consultar a alta direção, sem que isso acarrete prejuízo à gestão de riscos.***

***E A gestão de segurança da informação pode arbitrar alguns riscos a priori e realizar o tratamento do risco sem prejuízo dos resultados.***

Comentários:

- a) ERRADA - Os Erros estão em "Deve" e "Sempre";
- b) ERRADA – 27005 trata de gestão de riscos de SI e 15999 trata de continuidade de negócio;
- c) CERTA.
- d) ERRADA - A alta direção é a responsável primária pela GSI, portanto não pode deixar de ser consultada;
- e) ERRADA - A gestão de SI não pode simplesmente arbitrar alguns riscos, ele deve sempre contar com a participação dos gestores responsáveis.

Gabarito Oficial: C

***9. (CESPE/CNJ 2013) Acerca da gestão de segurança da informação, conforme as normas da ABNT, julgue os itens a seguir.***

***De acordo com a ABNT NBR ISO/IEC 27005, é preciso identificar controles existentes e planejados em uma organização. Além disso, é necessário manter uma lista que descreva sua implantação e seu status de utilização.***

Comentários:

***8.2.1.4 Identificação de controles existentes***

***Entrada: Documentação de controles, planos de implementação do tratamento do risco***

***Ação: Convém que os controles existentes e os planejados sejam identificados***

***Saída: Uma lista de todos os controles existentes e planejados, sua implantação e status de utilização***

Gabarito Oficial: CERTO

**10. (CESPE/TC-DF 2014) Julgue os próximos itens referentes à gestão de segurança da informação e à gestão de riscos e continuidade de negócio.**

***Conforme a norma ISO/IEC 27005, é recomendável que o nível de risco seja estimado em todos os cenários de incidentes relevantes. Essa estimativa serve para designar valores qualitativos ou quantitativos para a probabilidade e para as consequências do risco.***

Comentários:

A Análise de Cenários pode ser utilizada para auxiliar na tomada de decisões de políticas e no planejamento de futuras estratégias, bem como em considerar as atividades existentes de uma organização. Pode desempenhar um importante papel em todos os três componentes do processo de avaliação de riscos, conforme definido na norma ISO 27005.

Para a identificação e análise de riscos, conjuntos de cenários refletindo, por exemplo, o “melhor caso”, o “pior caso” e o “caso esperado” podem ser utilizados para identificar o que poderia acontecer sob circunstâncias específicas e analisar as consequências potenciais (negativas e positivas) e suas probabilidades para cada cenário.

Gabarito Oficial: CERTO

**11. (CESPE/TJ-RO 2012) Conforme as normas ABNT NBR 27001, 27002 e 27005, um documento da política de segurança da informação deve**  
***A revelar informações sensíveis da organização.***

***B ser aprovado pela direção, bem como publicado e comunicado para todos que tenham contato com a organização.***

***C conter uma declaração de comprometimento elaborada por todos aqueles que atuam na organização, inclusive pela direção.***

***D apresentar uma declaração de aplicabilidade dos controles de segurança da informação, além de definir como será o processo de gestão de riscos.***

***E conter o registro dos incidentes de segurança da organização.***

Comentários:

QUESTÃO POLÊMICA! Vejamos o que a norma diz:

*"Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes."*

Gabarito Oficial: CERTO

**12. (CESPE/TJ-RO 2012) Com relação à NBR 27005, assinale a opção correta, no que se refere à gestão de riscos de segurança da informação.**

**A Aceitar ou reter um risco durante o seu tratamento equivale a transferi-lo.**

**B Os riscos residuais são conhecidos antes da comunicação do risco.**

**C Os riscos são reduzidos ou mitigados sem que ocorra a seleção de controles.**

**D Qualquer atividade de comunicação do risco de segurança da informação deve ocorrer apenas após a aceitação do plano de tratamento do risco pelos gestores da organização.**

**E A definição do contexto da gestão de riscos deve preceder a identificação dos ativos de valor.**

Comentários:

a) ERRADA. Aceitar, Reter e Transferir, junto com Evitar, são diferentes tipos de tratamento de riscos;

b) ERRADA. A comunicação, assim como o monitoramento, se dá durante todo o processo;

c) ERRADA. Primeiro o controle deve ser selecionado para só então se mitigar o risco;

d) ERRADA. A comunicação, assim como o monitoramento, se dá durante todo o processo;

e) CERTA.

Gabarito Oficial: E

**13. (CESPE/MEC 2015) Os procedimentos de produção de métricas e indicadores de gestão de segurança da informação devem ser mais**

***bem orientados pelo conjunto de prescrições encontradas na norma NBR 27005, de gestão de riscos de segurança da informação, que pelos processos descritos na norma NBR 27001.***

Comentários:

Depois de muita firula, esta acaba sendo apenas mais uma questão em que é cobrado a velha pergunta de sempre: "qual é a norma da família 27000 que tem foco na gestão de riscos de SI?"

A 27001 é mais abrangente, mas não se aprofunda nos temas de que trata. Como toda norma de certificação, ela é sucinta (e, como disse em meu curso no Provas de TI, ela é auxiliada pelas outras normas da família para detalhamento). Seu foco está somente em definir requisitos para "estabelecer, implementar, manter e melhorar continuamente" o SGSI. Até existe um trecho desta Norma onde ela trata de riscos de SI (seções 6.1 e 6.2). Mas somente listando requisitos.

A 27005, por sua vez, trata da Gestão de Riscos de Segurança da Informação de forma que ela seja "um processo contínuo". A norma tem seções como "Contextualização", "Análise dos Riscos (Identificação e Estimação)", "Avaliação dos Riscos", "Tratamento dos Riscos" etc. Enfim, o que é escrito por alto em poucos parágrafos das seções 6.1 e 6.2 da 27001, está bem mais detalhado em dezenas de páginas da 27005.

Gabarito Oficial: CERTO

14. ***(CESPE/TCU 2009) O subsistema de planejamento do SGSI (ABNT NBR ISO/IEC 27001) possui sobreposição de atividades com a fase de definição do contexto presente na norma ABNT NBR ISO/IEC 27005 bem como produz uma informação de saída similar àquela produzida durante o processo de aceitação do risco da mesma ABNT NBR ISO/IEC 27005.***

Comentários:

Vajamos o que diz o escopo da ABNT NBR ISO/IEC 27005:

*Esta Norma fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001. Entretanto, esta Norma Internacional não inclui um método específico para a gestão de riscos de segurança da*

*informação. Cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica. Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita nesta Norma Internacional para implementar os requisitos de um SGSI.*

Gabarito Oficial: CERTO

Galerinha, por hoje é só! Espero encontrá-los na Aula 1, a qual será a parte II da Banca CESPE com relação à Gestão de Riscos de Segurança da Informação segundo a ISO 27005.

Até lá e Bons Estudos!

WC

## **Lista de Questões Abordadas nessa aula**

- 1. (CESPE/TCE-PI 2016) Considere que a equipe composta por quatro analistas de sistemas de um órgão do judiciário federal brasileiro deva desenvolver um plano de implantação da gerência de riscos de segurança da informação nesse órgão. Acerca das atividades que podem ser realizadas pela equipe, e considerando os conceitos de gerência de riscos, de classificação e controle dos ativos de informação, e a norma ISO/IEC 27005, é correto afirmar que essa equipe**

***A deve produzir ou obter a lista de processos de negócios aos quais estarão vinculados os demais ativos de informação a serem identificados na atividade de identificação de riscos***

***B deve particionar entre os quatro membros a responsabilidade pelo desempenho dos seguintes papéis, entre outros: identificação e análise das partes interessadas, estabelecimento de ligações com as funções de gerência de riscos de alto nível, especificação dos critérios para a avaliação dos riscos, estimativa de impactos e aceitação do risco para a organização***

***C deve aplicar uma metodologia de análise quantitativa de riscos, excluindo a aplicação de uma metodologia qualitativa***

***D deve implantar o sistema de gestão de segurança da informação, antes de desenvolver o plano de gestão de riscos***

***E deve particionar entre seus quatro membros a responsabilidade da execução simultânea das seguintes atividades: definição do escopo, identificação dos riscos, tratamento dos riscos e comunicação do risco***

- 2. (CESPE/TCE-PA 2016) À luz da NBR ISO/IEC 27005:2011, que dispõe diretrizes para o processo de gestão de riscos de segurança da informação (GRSI), julgue os itens a seguir.**

***O processo de GRSI é iterativo tanto para o processo de avaliação de riscos quanto para as atividades de tratamento de risco.***

3. **(CESPE/TJDF 2016)** Com relação à gestão de segurança da informação, julgue os itens a seguir.

*A norma ISO/IEC 27005 determina que, se uma ameaça tem valor constante, o impacto resultante será o mesmo para todos os ativos, independentemente de qual deles seja afetado.*

4. **(CESPE/STJ 2015)** Com base nas normas ISO 27001, ISO 27002, ISO 27003, ISO 27004 e ISO 27005, relativas à segurança de ativos de informação das organizações, julgue os itens a seguir.

*De acordo com a norma ISO 27005, na estimativa de riscos, podem ser aplicadas metodologias qualitativas para a identificação de riscos.*

5. **(CESPE/MEC 2015)** Com relação a norma ISO/IEC 27005, julgue os itens subsequentes.

*O conteúdo da norma ISO/IEC 27005 influenciou a criação de outras normas, tais como a ISO/IEC 27001 e ISO/IEC 27002.*

6. **(CESPE/TCU 2015)** Com relação à gestão de riscos, julgue os próximos itens.

*Conforme a NBR ISO/IEC 27005:2011, para a avaliação dos riscos de segurança da informação na organização, convém que os critérios de avaliação sejam desenvolvidos considerando-se a criticidade dos ativos de informação envolvidos.*

7. **(CESPE/TCU 2010)** Julgue os itens subsequentes, relativos às Normas NBR ISO/IEC 15999 e 27005.

*A norma NBR ISO/IEC 27005 prescreve que o gerenciamento de incidentes pode ser realizado iniciando-se com uma definição de contexto, seguido por uma análise e avaliação, tratamento, aceitação, comunicação, monitoramento e análise crítica dos incidentes.*

8. **(CESPE/TCE-ES 2013)** Com relação à gestão de riscos, assinale a opção correta.



***A O escopo da análise dos riscos deve sempre atuar sobre toda a organização.***

***B A NBR ISO/IEC 15999 estabelece as bases para a gestão de riscos em segurança da informação e a NBR ISO/IEC 27005 trata da gestão de continuidade de negócios.***

***C Gerenciar os riscos é um dos principais processos da gestão de segurança da informação, pois visa identificar, avaliar e priorizar riscos para, em seguida, se poder aplicar, de forma coordenada e econômica, os recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, de modo a se reduzir o risco a um nível aceitável.***

***D No sentido de ganhar agilidade na identificação, avaliação e priorização dos riscos, o gestor de segurança da informação pode deixar de consultar a alta direção, sem que isso acarrete prejuízo à gestão de riscos.***

***E A gestão de segurança da informação pode arbitrar alguns riscos a priori e realizar o tratamento do risco sem prejuízo dos resultados.***

- 9. (CESPE/CNJ 2013) Acerca da gestão de segurança da informação, conforme as normas da ABNT, julgue os itens a seguir.**

***De acordo com a ABNT NBR ISO/IEC 27005, é preciso identificar controles existentes e planejados em uma organização. Além disso, é necessário manter uma lista que descreva sua implantação e seu status de utilização.***

- 10. (CESPE/TC-DF 2014) Julgue os próximos itens referentes à gestão de segurança da informação e à gestão de riscos e continuidade de negócio.**

***Conforme a norma ISO/IEC 27005, é recomendável que o nível de risco seja estimado em todos os cenários de incidentes relevantes. Essa estimativa serve para designar valores qualitativos ou quantitativos para a probabilidade e para as consequências do risco.***

11. **(CESPE/TJ-RO 2012) Conforme as normas ABNT NBR 27001, 27002 e 27005, um documento da política de segurança da informação deve**  
**A revelar informações sensíveis da organização.**  
**B ser aprovado pela direção, bem como publicado e comunicado para todos que tenham contato com a organização.**  
**C conter uma declaração de comprometimento elaborada por todos aqueles que atuam na organização, inclusive pela direção.**  
**D apresentar uma declaração de aplicabilidade dos controles de segurança da informação, além de definir como será o processo de gestão de riscos.**  
**E conter o registro dos incidentes de segurança da organização.**
12. **(CESPE/TJ-RO 2012) Com relação à NBR 27005, assinale a opção correta, no que se refere à gestão de riscos de segurança da informação.**
13. **(CESPE/MEC 2015) Os procedimentos de produção de métricas e indicadores de gestão de segurança da informação devem ser mais bem orientados pelo conjunto de prescrições encontradas na norma NBR 27005, de gestão de riscos de segurança da informação, que pelos processos descritos na norma NBR 27001.**
14. **(CESPE/TCU 2009) O subsistema de planejamento do SGSI (ABNT NBR ISO/IEC 27001) possui sobreposição de atividades com a fase de definição do contexto presente na norma ABNT NBR ISO/IEC 27005 bem como produz uma informação de saída similar àquela produzida durante o processo de aceitação do risco da mesma ABNT NBR ISO/IEC 27005.**

## **Aula 1: Banca CESPE Parte II**

Salve, salve, Galera! Prof. Walter Cunha novamente na área...

E aí? Prontos para mais uma “saraivada” de Questões? Sem mais delongas...

Sigam-me os bons!

- 1. (CESPE/SECONT-ES 2009) Considere que, em uma organização, os auditores observaram que algumas das atividades de identificação de riscos foram efetuadas parcialmente, na seguinte sequência: inventário dos ativos; identificação de ameaças; e identificação de vulnerabilidades. Nesse caso, a sequência de levantamento de dados realizada está coerente com o indicado na Norma 27.005.**

Comentários:

Segundo a norma 27.005, temos a seguinte ordem:

8.2 Identificação de riscos

8.2.1 Introdução à identificação de riscos

8.2.2 Identificação dos ativos

8.2.3 Identificação das ameaças

8.2.4 Identificação dos controles existentes

8.2.5 Identificação das vulnerabilidades

8.2.6 Identificação das consequências

Daí, decorre duas observações.

- i. O enunciado fala em “Inventário de Ativos”, enquanto a norma usa expressão “Identificação de Ativos”.
- ii. Alguns dos passos não estão presentes no enunciado.

Para a observação (i), podemos relativizar que “Inventário” e “Identificação” seriam expressões análogas. Já para a observação (ii), a expressão “parcialmente” relativizaria a falta de itens na sequência.

Contudo, o fato é ter que relativizar demais é ficar na mão da banca. Ou seja, ela fica com o poder de decidir se a questão está CERTA ou ERRADA, e não

temos muito o que fazer. Sinceramente, não sei o que ela a Banca a manter esse tipo de questão escorregadia.

Gabarito Oficial: CERTA (mas a questão é polêmica)

**2. (CESPE/TRT-21 2010) Os processos que fazem parte da análise/avaliação de riscos são identificação de riscos, estimativa de riscos e avaliação de riscos.**

Comentários:

Segundo a ISO 27005:2011, o processo de Avaliação de Riscos consiste nas seguintes atividades:

8.2 Identificação de riscos

8.3 Análise de riscos

8.4 Avaliação de riscos

Pelo comentário acima, o enunciado tem uma ligeira modificação em relação à letra da norma. Contudo, atente que a questão data de 2010, ou seja, antes da última versão da norma (2011).

Gabarito Oficial: CERTA (com ressalvas)

**3. (CESPE/ANTT 2013) Na estimativa de risco, atribuem-se valores às probabilidades e também às consequências de um risco.**

Comentários:

Termos definidos na ABNT NBR ISO/IEC 27005:2008

*3.5 Estimativa de Riscos*

*processo utilizado para atribuir valores à probabilidade e consequências de um risco*

Termos definidos na ABNT NBR ISO/IEC 27005:2011

*Este termo foi removido. (Estimativa de Riscos)*

Embora a enunciado faça todo o sentido, e questão seja posterior à versão mais recente da norma, ela ainda usa o termo “estimativa de riscos”, o qual foi abolido.

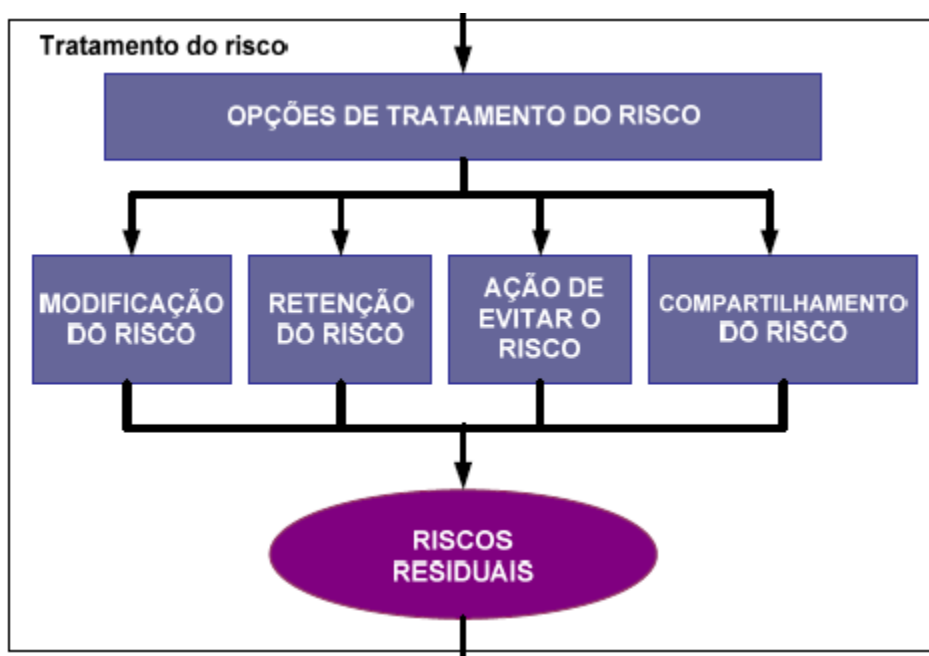
Gabarito Oficial: CERTA (com ressalvas)

4. (CESPE/TJ-AL 2012) De acordo com a NBR ISO/IEC n.º 27.005/2011, as quatro possíveis ações para o tratamento do risco de segurança da informação correspondem a

- a) planejamento, identificação, mitigação e eliminação do risco.
- b) redução, retenção, prevenção e transferência do risco.
- c) identificação, redução, mitigação e eliminação do risco.
- d) retenção, redução, mitigação e transferência do risco.
- e) prevenção, identificação, redução e eliminação do risco.

Comentários:

Vejamos, de acordo com a NBR ISO/IEC n.º 27.005/2011:



Veja que o enunciado da questão usou:

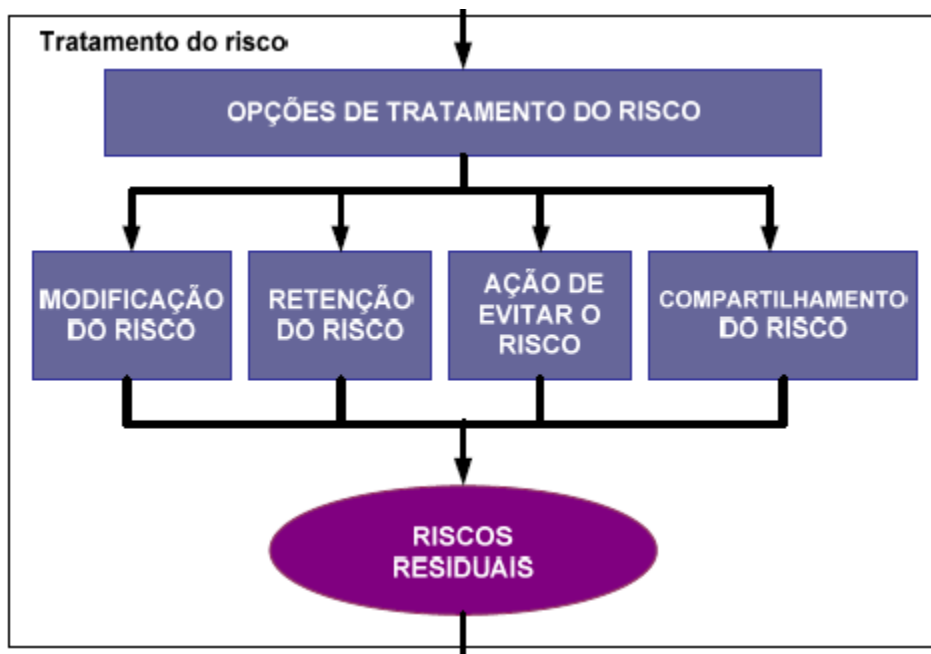
- (i) REDUZIR em vez de MODIFICAR;
- (ii) TRANSFERIR em vez de COMPARTILHAR
- (iii) PREVENIR em vez de EVITAR.

Gabarito Oficial: CERTA (com ressalvas)

5. (CESPE/TJ-SE 20014) *Entre as formas de abordagem do risco inclui-se a transferência do risco, atividade que não se confunde com a abstenção do tratamento do risco.*

Comentários:

Vejamos, de acordo com a NBR ISO/IEC n.º 27.005/2011:



### 9.2 Modificação do risco

*Ação: Convém que o nível de risco seja gerenciado através da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.*

Gabarito Oficial: ERRADA

6. (CESPE/MEC 2015) *O tratamento de risco geralmente aumenta as despesas organizacionais. As opções para o tratamento do risco não podem ser usadas em conjunto.*

Comentários:

A afirmação que o tratamento de risco geralmente aumenta as despesas organizacionais é um tanto quanto polêmica. Se de um lado, não se concebe a implementação de um plano de gestão de riscos se destacar

orçamento para ele. De outro, a organização fica muito menos sujeita a prejuízos decorrentes da não-gestão.

Felizmente, quanto a usar a poder usar as medidas de tratamento em conjunto não há controvérsia alguma. Vejamos o que diz a Norma:

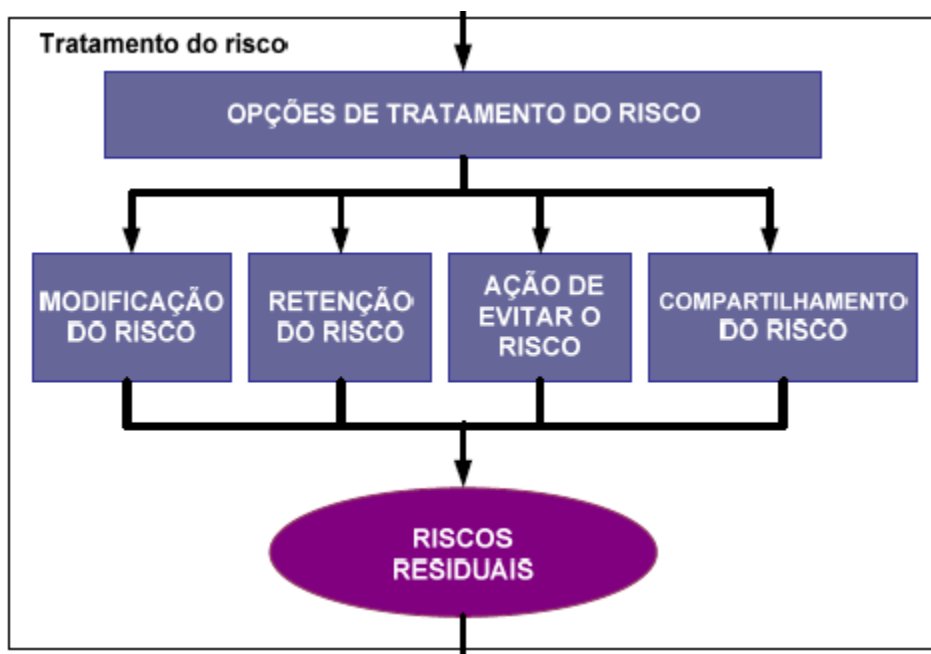
*As quatro opções para o tratamento do risco não são mutuamente exclusivas. Às vezes, a organização pode beneficiar-se substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais.*

Gabarito Oficial: ERRADA

- 7. (CESPE/MEC 2015) Entre as formas de abordagem do risco inclui-se a transferência do risco, atividade que não se confunde com a abstenção do tratamento do risco.**

Comentários:

Vejamos, de acordo com a NBR ISO/IEC n.º 27.005/2011:



Podemos entender:

TRANSFERÊNCIA como COMPARTILHAMENTO e  
ABSTENÇÃO NO TRATAMENTO como retenção.



E, como mostrado na figura, são de fato medidas de tratamento diferentes.

9.5 Compartilhamento do risco

*Ação: Convém que um determinado risco seja compartilhado com outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.*

9.4 Ação de evitar o risco

*Ação: Convém que a atividade ou condição que dá origem a um determinado risco seja evitada.*

Gabarito Oficial: CERTA

**8. (CESPE/TRE-MS 2013) De acordo com a norma ABNT NBR ISO/IEC 27.005, os processos da análise de riscos incluem**

- a) a identificação de consequências.**
- b) a definição e mensuração da efetividade de controles.**
- c) a detecção de erros no resultado de processamento de informações.**
- d) o contato com autoridades.**
- e) os acordos de confidencialidade.**

Comentários:

Questão tranquila, extraída diretamente da Norma.

**8 Processo de Avaliação de Riscos de Segurança da Informação**

(...)

**8.2 Identificação de riscos**

8.2.1 Introdução à identificação de riscos

8.2.2 Identificação dos ativos

8.2.3 Identificação das ameaças

8.2.4 Identificação dos controles existentes

8.2.5 Identificação das vulnerabilidades

8.2.6 Identificação das consequências

(...)

8.3 Análise de riscos

8.4 Avaliação de riscos

Gabarito Oficial: A

- 9. (CESPE/PREVIC 2011) Uma ameaça pode causar impacto em vários ativos ou apenas em parte de um deles, podendo ter efeitos imediatos (operacionais) ou futuros (negócios).**

Comentários:

De acordo com a norma:

*Uma ameaça tem o potencial de comprometer ativos (tais como, informações, processos e sistemas) e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais.*

(...)

*Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados.*

Destaquei o primeiro parágrafo para termos a definição de ameaça.

O primeiro período do segundo parágrafo destacado arremata a questão.

Procurei por algum trecho na norma que remetesse ao segundo período do segundo parágrafo, mas não encontrei. Porém, ele é praticamente uma decorrência lógica do primeiro.

Gabarito Oficial: CERTA

- 10. (CESPE/TER-PI 2016) Considere que a equipe composta por quatro analistas de sistemas de um órgão do judiciário federal brasileiro deva desenvolver um plano de implantação da gerência de riscos de segurança da informação nesse órgão. Acerca das atividades que podem ser realizadas pela equipe, e considerando os conceitos de gerência de riscos, de classificação e controle dos ativos de informação, e a norma ISO/IEC 27005, é correto afirmar que essa equipe**

***a) deve produzir ou obter a lista de processos de negócios aos quais estarão vinculados os demais ativos de informação a serem identificados na atividade de identificação de riscos.***

***b) deve particionar entre os quatro membros a responsabilidade pelo desempenho dos seguintes papéis, entre outros: identificação e análise das partes interessadas, estabelecimento de ligações com as funções de gerência de riscos de alto nível, especificação dos critérios para a avaliação dos riscos, estimativa de impactos e aceitação do risco para a organização.***

***c) deve aplicar uma metodologia de análise quantitativa de riscos, excluindo a aplicação de uma metodologia qualitativa.***

***d) deve implantar o sistema de gestão de segurança da informação, antes de desenvolver o plano de gestão de riscos.***

***e) deve particionar entre seus quatro membros a responsabilidade da execução simultânea das seguintes atividades: definição do escopo, identificação dos riscos, tratamento dos riscos e comunicação do risco.***

Comentários:

De acordo com a Norma:

#### **8.2.2 Identificação dos ativos**

*Entrada: Escopo e limites para o processo de avaliação de riscos a ser executado; lista de componentes com responsáveis, localidade, função etc..*

*Ação: Convém que os ativos dentro do escopo estabelecido sejam identificados (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1.d) 1)).*

*(...)*

*Saída: Uma lista de ativos com riscos a serem gerenciados, e uma lista dos processos de negócio relacionados aos ativos e suas relevâncias.*

Mais uma questão que foi extraída da Norma com algumas pequenas variações no texto, mas que significam a mesma coisa.

Gabarito Oficial: A

- 11. (CESPE/MEC 2015) O processo para a gestão de riscos de segurança da informação descrito pela referida norma pode ser usado para avaliações de riscos em um projeto; porém, não pode ser aplicado à operação cotidiana de um SGSI.**

Comentários:

É fato que a disciplina de Gerenciamento de Projetos (PMBok) vem há muito pregando uma boa gestão de riscos como fator decisivo no sucesso dos projetos. Contudo, Gestão de Riscos não só pode como deve ser aplicado às operações cotidianas, por exemplo, por meio da disciplina de Gerenciamento de Processos.

Bom, mas se eu apenas falar, é provável que você não leve muita fé. Portanto, vamos ver o que a Norma diz.

### **5 Contextualização**

(...)

*Convém que os esforços de segurança lidem com riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários. Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI.*

Gabarito Oficial: ERRADA

- 12. (CESPE/MEC 2015) Conforme descreve a norma em questão, a metodologia para estimativa de riscos qualitativa pode ser utilizada: como uma verificação inicial a fim de identificar riscos que exigirão uma análise mais detalhada; quando esse tipo de análise é suficiente para a tomada de decisões; e quando os dados numéricos ou recursos são insuficientes para uma estimativa quantitativa.**

Comentários:

Já sabe, né? Vamos à Norma...

### **8.3 Análise de riscos**

#### **8.3.1 Metodologias de análise de riscos**

*A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Uma metodologia para a análise pode ser qualitativa ou*

*quantitativa ou uma combinação de ambos, dependendo das circunstâncias. Na prática, a análise qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Depois, poderá ser necessário efetuar uma análise quantitativa ou mais específica, nos grandes riscos. Isso ocorre porque normalmente é menos complexo e menos oneroso realizar análises qualitativas do que quantitativas.*

Gabarito Oficial: CERTA

- 13. (CESPE/ANATEL 2014) Como o processo de gestão de riscos de segurança da informação contribui para a identificação de riscos, para a análise de riscos e para o estabelecimento da ordem prioritária para tratamento de riscos, ele deve ser aplicado à organização como um todo, e não apenas a uma área específica.**

Comentários:

Soa até incoerente admitir que determinado framework pode ser aplicado ao todo, mas não à determinada parte. Mas, vai saber... De modo a sanar a insegurança, vamos recorrer novamente à Norma:

### **5 Contextualização** **(...)**

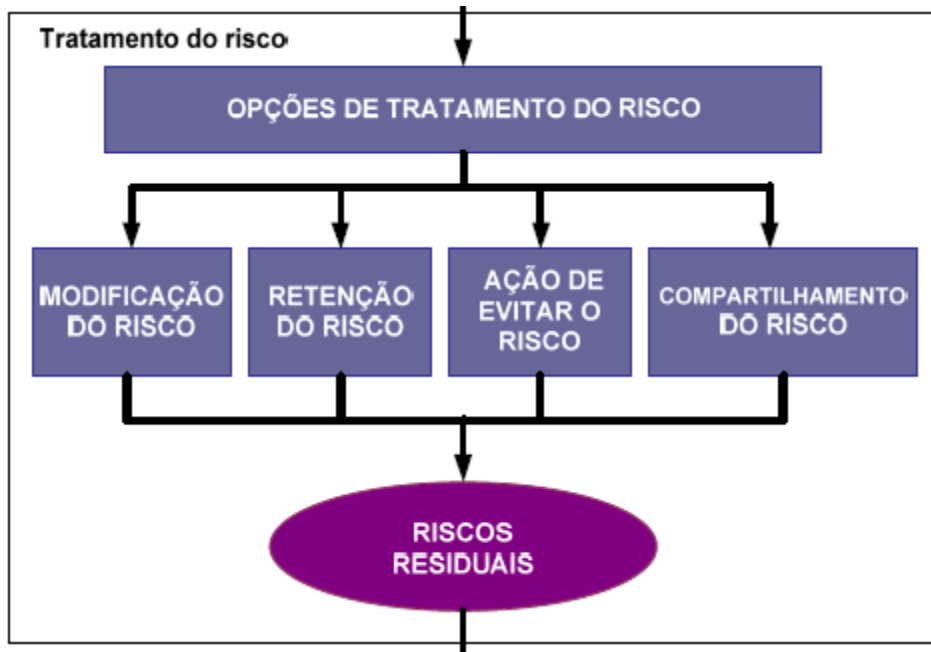
*O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo, um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo: o plano de continuidade de negócios).*

Gabarito Oficial: ERRADA

- 14. (CESPE/ANATEL 2014) A referida norma prevê quatro opções para o tratamento de um risco identificado: redução do risco por meio de controles, para que o risco residual seja considerado aceitável; retenção do risco: que considera o risco como aceitável; transferência do risco: em que se transfere o risco para outra entidade que possa gerenciá-lo de forma eficaz; e reversão do risco, em que o risco é transformado em oportunidade de negócio.**

Comentários:

Relembrando...



Como já vimos em outras questões:

REDUÇÃO é aceita como MODIFICAÇÃO; e  
TRANSFERÊNCIA é aceita como COMPARTILHAMENTO;

Mas REVERSÃO não é prevista como medida de tratamento na norma. Em seu lugar, o enunciado deveria ter relacionado EVITAR.

#### 9.4 Ação de evitar o risco

*Ação: Convém que a atividade ou condição que dá origem a um determinado risco seja evitada.*

Gabarito Oficial: ERRADA

**15. (CESPE/TRF-1 2017) A qualidade e a exatidão do processo de análise quantitativa de riscos estão relacionadas à disponibilidade de dados históricos e auditáveis.**

Comentários:

Já falamos algumas vezes sobre a análise qualitativa de riscos, vamos então agora detalhar um pouco a análise quantitativa usando a Norma:

### **8.3 Análise de riscos**

#### **8.3.1 Metodologias de análise de riscos**

##### **(b) Análise quantitativa de riscos:**

*A análise quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na análise qualitativa) tanto para consequências quanto para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados. A análise quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização. Uma desvantagem é a falta de tais dados sobre novos riscos ou sobre fragilidades da segurança da informação. Uma desvantagem da abordagem quantitativa ocorre quando dados factuais e auditáveis não estão disponíveis. Nesse caso, a exatidão do processo de avaliação de riscos e os valores associados tornam-se ilusórios.*

Gabarito Oficial: CERTA

**16. (CESPE/MEC 2015) Parte interessada é a pessoa ou a organização passível de ser afetada pela decisão sobre a forma de tratar do risco.**

Comentários:

#### **Termos definidos na ABNT NBR ISO/IEC 27005:2011**

##### **3.18 parte interessada**

*pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade*

Apesar de pequenas diferenças os enunciados significam na prática a mesma coisa.

Gabarito Oficial: CERTA

**17. (CESPE/MEC 2015) As organizações não devem definir o escopo e o limite da gestão de riscos, pois necessitam estar preparadas para**



***atuarem quando da ocorrência de algum evento prejudicial aos negócios.***

Comentários:

De cara, a expressão “dever” não se coaduna com o preconizado na Norma, a qual sempre usa a expressão “convém”.

Outra coisa, estranha é o enunciado afirmar que as organizações não devem definir escopo. Ora, durante nossos estudos aprendemos que um dos fatores de sucesso de qualquer iniciativa é justamente a delimitação do escopo de atuação.

Contudo, como é a praxe, vamos recorrer à letra da Norma.

## **7 Definição do contexto**

### **7.1 Considerações Gerais**

*Entrada: Todas as informações sobre a organização relevantes para a definição do contexto da gestão de riscos de segurança da informação.*

*Ação: Convém que o contexto externo e interno para gestão de riscos de segurança da informação seja estabelecido, o que envolve a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação (7.2), a definição do escopo e dos limites (7.3) e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação (7.4).*

Gabarito Oficial: ERRADA

**18. (CESPE/MEC 2015) Os riscos que são integrantes do plano de gestão de risco devem ser identificados, mas não convém que sejam priorizados devido à incerteza do seu acontecimento.**

Comentários:

Essa é mamão com açúcar. Como pode se conceber não priorizar os riscos? Uma vez que os recursos não são infinitos, como faríamos para decidir quais riscos seriam tratados?

Bom, deixando de lado a filosofia, vamos consultar mais uma vez a Norma:

## **8 Processo de avaliação de riscos de segurança da informação**

### **8.1 Descrição geral do processo de avaliação de riscos de segurança da informação**

(...)

*Entrada: Critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos de segurança da informação que se está definindo.*

*Ação: Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, **priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.***

Gabarito Oficial: ERRADA

- 19. (CESPE/BASA 2012) A conscientização dos gestores a respeito dos riscos, da natureza dos controles aplicados para mitigá-los e das áreas definidas como de interesse pela organização auxilia a organização na gestão dos incidentes e eventos previstos, porém não influencia no tratamento dos incidentes não previstos.**

Comentários:

Se você já está se acostumando a lidar com Riscos (pelo menos para a prova), dever ter se sentido incomodado ao ler que “a conscientização dos gestores (...) não influencia no tratamento dos incidentes não previstos.

Medidas de tratamento além de tratarem os incidentes-alvo, normalmente ajudam a tratar outros incidentes, conhecidos ou não. Por exemplo, se faço um treinamento para que um usuário proteja seus dados para divulgação não autorizada, eu fatalmente o estarei preparando para evitar a perda dos dados.

Agora, vamos ver o que está escrito na norma:

### **6 Visão geral do processo de gestão de riscos de segurança da informação**

*Durante o processo de gestão de riscos de segurança da informação, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados. Mesmo antes do tratamento do risco, informações sobre riscos identificados*

*podem ser muito úteis para o gerenciamento de incidentes e ajudar a reduzir possíveis prejuízos. A conscientização dos gestores e pessoal no que diz respeito aos riscos, à natureza dos controles aplicados para mitigá-los e às áreas definidas como de interesse pela organização, auxiliam a lidar com os incidentes e eventos não previstos da maneira mais efetiva. Convém que os resultados detalhados de cada atividade do processo de gestão de riscos de segurança da informação, assim como as decisões sobre o processo de avaliação de riscos e sobre o tratamento do risco (representadas pelos dois pontos de decisão na Figura 2), sejam documentados.*

Gabarito Oficial: ERRADA

**20. (CESPE/TRF-1 2017) Entre os ativos de suporte e infraestrutura incluem-se os recursos humanos, as instalações físicas e a estrutura da organização.**

Comentários:

Que um humanista não nos ouça, mas é isso mesmo. Para GRSI, recursos humanos (pessoas) são sim ativos de suporte e infraestrutura.

Para variar, vamos à Norma:

### **B.1 Exemplos de identificação de ativos**

*Para estabelecer o valor de seus ativos, uma organização precisa primeiro identificá-los (num nível de detalhamento adequado). Dois tipos de ativos podem ser distinguidos:*

- *Ativos primários:*
  - *Processos e atividades do negócio*
  - *Informação*
- *Ativos de suporte e infraestrutura (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:*
  - *Hardware*
  - *Software*
  - *Rede*
  - *Recursos humanos*
  - *Instalações físicas*
  - *A estrutura da organização*

Gabarito Oficial: CERTA

Galerinha, por hoje é só! Espero sinceramente que vocês estejam apreciando o curso. Abraços!

WC

### **Enunciado das Questões Abordadas nessa aula**

1. *(CESPE/SECONT-ES 2009) Considere que, em uma organização, os auditores observaram que algumas das atividades de identificação de riscos foram efetuadas parcialmente, na seguinte sequência: inventário dos ativos; identificação de ameaças; e identificação de vulnerabilidades. Nesse caso, a sequência de levantamento de dados realizada está coerente com o indicado na Norma 27.005.*
2. *(CESPE/TRT-21 2010) Os processos que fazem parte da análise/avaliação de riscos são identificação de riscos, estimativa de riscos e avaliação de riscos.*
3. *(CESPE/ANTT 2013) Na estimativa de risco, atribuem-se valores às probabilidades e também às consequências de um risco.*
4. *(CESPE/TJ-AL 2012) De acordo com a NBR ISO/IEC n.º 27.005/2011, as quatro possíveis ações para o tratamento do risco de segurança da informação correspondem a*
  - a) planejamento, identificação, mitigação e eliminação do risco.*
  - b) redução, retenção, prevenção e transferência do risco.*
  - c) identificação, redução, mitigação e eliminação do risco.*
  - d) retenção, redução, mitigação e transferência do risco.*
  - e) prevenção, identificação, redução e eliminação do risco.*
5. *(CESPE/TJ-SE 20014) Entre as formas de abordagem do risco inclui-se a transferência do risco, atividade que não se confunde com a abstenção do tratamento do risco.*
6. *(CESPE/MEC 2015) O tratamento de risco geralmente aumenta as despesas organizacionais. As opções para o tratamento do risco não podem ser usadas em conjunto.*
7. *(CESPE/MEC 2015) Entre as formas de abordagem do risco inclui-se a transferência do risco, atividade que não se confunde com a abstenção do tratamento do risco.*
8. *(CESPE/TRE-MS 2013) De acordo com a norma ABNT NBR ISO/IEC 27.005, os processos da análise de riscos incluem*

- a) a identificação de consequências.*
  - b) a definição e mensuração da efetividade de controles.*
  - c) a detecção de erros no resultado de processamento de informações.*
  - d) o contato com autoridades.*
  - e) os acordos de confidencialidade.*
9. *(CESPE/PREVIC 2011) Uma ameaça pode causar impacto em vários ativos ou apenas em parte de um deles, podendo ter efeitos imediatos (operacionais) ou futuros (negócios).*
10. *(CESPE/TER-PI 2016) Considere que a equipe composta por quatro analistas de sistemas de um órgão do judiciário federal brasileiro deva desenvolver um plano de implantação da gerência de riscos de segurança da informação nesse órgão. Acerca das atividades que podem ser realizadas pela equipe, e considerando os conceitos de gerência de riscos, de classificação e controle dos ativos de informação, e a norma ISO/IEC 27005, é correto afirmar que essa equipe*
- a) deve produzir ou obter a lista de processos de negócios aos quais estarão vinculados os demais ativos de informação a serem identificados na atividade de identificação de riscos.*
  - b) deve particionar entre os quatro membros a responsabilidade pelo desempenho dos seguintes papéis, entre outros: identificação e análise das partes interessadas, estabelecimento de ligações com as funções de gerência de riscos de alto nível, especificação dos critérios para a avaliação dos riscos, estimativa de impactos e aceitação do risco para a organização.*
  - c) deve aplicar uma metodologia de análise quantitativa de riscos, excluindo a aplicação de uma metodologia qualitativa.*
  - d) deve implantar o sistema de gestão de segurança da informação, antes de desenvolver o plano de gestão de riscos.*
  - e) deve particionar entre seus quatro membros a responsabilidade da execução simultânea das seguintes atividades: definição do escopo, identificação dos riscos, tratamento dos riscos e comunicação do risco.*

11. ***(CESPE/MEC 2015) O processo para a gestão de riscos de segurança da informação descrito pela referida norma pode ser usado para avaliações de riscos em um projeto; porém, não pode ser aplicado à operação cotidiana de um SGSI.***
12. ***(CESPE/MEC 2015) Conforme descreve a norma em questão, a metodologia para estimativa de riscos qualitativa pode ser utilizada: como uma verificação inicial a fim de identificar riscos que exigirão uma análise mais detalhada; quando esse tipo de análise é suficiente para a tomada de decisões; e quando os dados numéricos ou recursos são insuficientes para uma estimativa quantitativa.***
13. ***(CESPE/ANATEL 2014) Como o processo de gestão de riscos de segurança da informação contribui para a identificação de riscos, para a análise de riscos e para o estabelecimento da ordem prioritária para tratamento de riscos, ele deve ser aplicado à organização como um todo, e não apenas a uma área específica.***
14. ***(CESPE/ANATEL 2014) A referida norma prevê quatro opções para o tratamento de um risco identificado: redução do risco por meio de controles, para que o risco residual seja considerado aceitável; retenção do risco: que considera o risco como aceitável; transferência do risco: em que se transfere o risco para outra entidade que possa gerenciá-lo de forma eficaz; e reversão do risco, em que o risco é transformado em oportunidade de negócio.***
15. ***(CESPE/TRF-1 2017) A qualidade e a exatidão do processo de análise quantitativa de riscos estão relacionadas à disponibilidade de dados históricos e auditáveis.***
16. ***(CESPE/MEC 2015) Parte interessada é a pessoa ou a organização passível de ser afetada pela decisão sobre a forma de tratar do risco.***
17. ***(CESPE/MEC 2015) As organizações não devem definir o escopo e o limite da gestão de riscos, pois necessitam estar preparadas para atuarem quando da ocorrência de algum evento prejudicial aos negócios.***
18. ***(CESPE/MEC 2015) Os riscos que são integrantes do plano de gestão de risco devem ser identificados, mas não convém que sejam priorizados devido à incerteza do seu acontecimento.***



- 19. (CESPE/BASA 2012) *A conscientização dos gestores a respeito dos riscos, da natureza dos controles aplicados para mitigá-los e das áreas definidas como de interesse pela organização auxilia a organização na gestão dos incidentes e eventos previstos, porém não influencia no tratamento dos incidentes não previstos.***
- 20. (CESPE/TRF-1 2017) *Entre os ativos de suporte e infraestrutura incluem-se os recursos humanos, as instalações físicas e a estrutura da organização.***

### **Gabarito das Questões Abordadas nessa aula**

- 1. CERTA (mas a questão é polêmica)**
- 2. CERTA (com ressalvas)**
- 3. CERTA (com ressalvas)**
- 4. CERTA (com ressalvas)**
- 5. ERRADA**
- 6. ERRADA**
- 7. CERTA**
- 8. A**
- 9. CERTA**
- 10. A**
- 11. ERRADA**
- 12. CERTA**
- 13. ERRADA**
- 14. ERRADA**
- 15. CERTA**
- 16. CERTA**
- 17. ERRADA**
- 18. ERRADA**
- 19. ERRADA**
- 20. CERTA**

## **Aula 2: Banca CESPE Parte III**

Salve, salve, Galera! Prof. Walter Cunha novamente na área...

Como está o curso? Espero que estejam apreciando.

Hoje vamos abordar a última bateria do CESPE sobre Gestão de Riscos de Segurança da Informação (27.005).

Não deixem de enviar suas solicitações, dúvidas e sugestões no fórum do curso!

Simbora...

- 1. (CESPE/PREVIC 2011) De acordo com a norma NBR/ISO/IEC 27005, a comunicação de riscos visa assegurar que as informações sobre os riscos sejam compartilhadas entre os tomadores de decisão e outros stakeholders, buscando-se, assim, alcançar um entendimento de todos sobre como os riscos serão gerenciados.**

Comentários:

A assertiva faz todo o sentido, mas antes de fecharmos a nossa resposta, não vamos nos furtar de consultar a Norma:

*A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.*

*A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões que devem ser tomadas. A comunicação assegurará que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito, tenham um bom entendimento do por que as decisões são tomadas e dos motivos que tornam certas ações necessárias. A comunicação é bidirecional.*

Gabarito Oficial: CERTA.

**2. (CESPE/MEC 2015) As restrições organizacionais devem ser levadas em conta durante o tratamento de risco.**

Comentários:

De que adianta um plano de tratamento de riscos lindo e maravilhoso, mas inexecutável, seja porque não temos dinheiro suficiente, seja porque não temos capacidade de execução disponível?

Segundo a Norma:

Convém que todas as restrições - organizacionais, técnicas, estruturais etc.- identificadas durante a atividade de definição do contexto, sejam levadas em conta durante o tratamento do risco.

Gabarito Oficial: CERTA.

**3. (CESPE/MEC 2015) À luz da norma ISO/IEC 27005, julgue o item subsequente, acerca de gestão de riscos. No que diz respeito aos riscos de segurança da informação, essa norma não se aplica a qualquer tipo de organização.**

Comentários:

Essa é clássica. Perguntar se a norma depende do tipo de organização (privada, pública, terceiro setor...) ou do setor para ser aplicada. Grave aí, **NÃO DEPENDE!**

Segundo a Norma:

1 Escopo

(...)

*Esta Norma se aplica a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização.*

Gabarito Oficial: ERRADA.

**4. (CESPE/TJDF 2015) A ISO 27005, que estabelece guias de referência para gerenciamento de risco em segurança da informação, é aplicável**

***na maior parte das organizações, com exceção das agências de governo.***

Comentários:

Como na questão anterior, a adaptabilidade da Norma é mais uma vez questionada.

Sendo mais claro, não existe exceção para agências de governo na Norma.

Gabarito Oficial: ERRADA.

**5. (CESPE/TRT 2016) De acordo com a norma NBR ISO/IEC 27005, a etapa em que se identifica qualquer mecanismo administrativo, físico ou operacional capaz de tratar os riscos da ocorrência de um incidente de segurança é a identificação**

- a) das ameaças.***
- b) dos controles existentes.***
- c) das vulnerabilidades.***
- d) das consequências.***
- e) dos ativos.***

Comentários:

Segundo a Norma, primeiro vamos buscar a definição de Controles:

### **3.2 controle**

***medida que está modificando o risco (3.9)***

*[ABNT ISO GUIA 73:2009]*

*NOTA 1 Os controles da segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, que pode ser de natureza administrativa, técnica, gerencial ou legal que modificam o risco da segurança da informação.*

*NOTA 2 Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.*

*NOTA 3 Controle também é usado como um sinônimo de salvaguarda ou contramedida.*

Agora, vamos compor com o significado de controle existente para concluir a formulação do nosso parecer:

#### **8.2.4 Identificação dos controles existentes**

*Entrada: Documentação dos controles, planos de implementação do tratamento do risco.*

***Ação: Convém que os controles existentes e os planejados sejam identificados.***

*Diretrizes para implementação:*

*Convém que a identificação dos controles existentes seja realizada para evitar custos e trabalho desnecessários, por exemplo, na duplicação de controles. Além disso, enquanto os controles existentes estão sendo identificados, convém que seja feita uma verificação para assegurar que eles estão funcionando corretamente - uma referência aos relatórios já existentes de auditoria do SGSI pode reduzir o tempo gasto nesta tarefa. (...)*

Gabarito Oficial: B

#### **6. (CESPE/MEC 2015) Após ser realizado o tratamento de um risco poderá existir riscos não identificados.**

Comentários:

Embora a afirmação causa desconforto aos neófitos do gerenciamento de riscos, ela é quase que um mantra dos gestores mais experientes. A realidade é que por mais que você se esforce, você não conseguirá prever tudo, nem hoje tampouco no futuro.

Então para que serve isso tudo, Walter? Hora, a ideia é fazermos o nosso melhor por meio da aplicação das técnicas mais efetivas e dentro das nossas possibilidades. E o resto? “Bota na conta do Papa”!

Segunda a Norma:

#### **3.8 risco residual**

*risco (3.9) remanescente após o tratamento do risco (3.17)*

*[ABNT ISO GUIA 73:2009]*

*NOTA 1 O risco residual pode conter riscos não identificados.*

*NOTA 2 O risco residual também pode ser conhecido como "risco retido".*

Gabarito Oficial: CERTA

**7. (CESPE/TJ-SE 2014) Na definição da metodologia de avaliação dos riscos, devem ser identificadas as ameaças que podem afetar os ativos de informação que serão avaliados.**

Comentários:

Segundo a norma 27.005, temos a seguinte ordem:

*8.2 Identificação de riscos*

*8.2.1 Introdução à identificação de riscos*

*8.2.2 Identificação dos ativos*

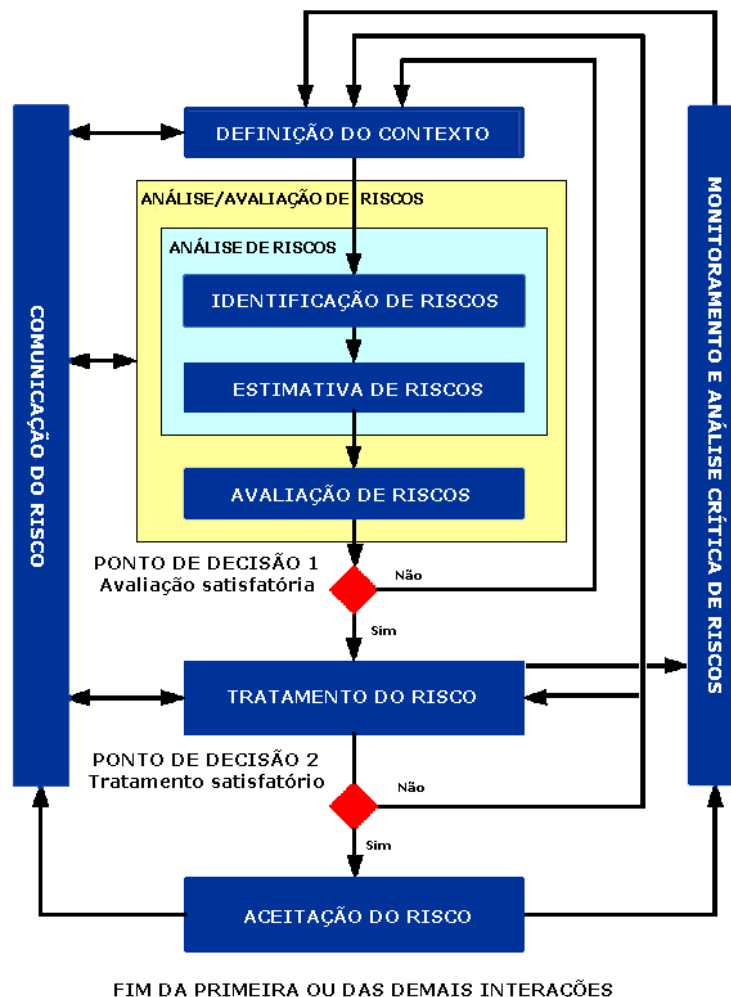
*8.2.3 Identificação das ameaças*

*8.2.4 Identificação dos controles existentes*

*8.2.5 Identificação das vulnerabilidades*

*8.2.6 Identificação das consequências*

Vamos agora revisitar o frame da 27.005:



Note a “Avaliação de Riscos” aparece simultaneamente com o Gênero e Par de Identificação de riscos, o que, dependendo da interpretação, influencia na resposta.

Outra hipótese para o Gabarito é que a Banca tenha utilizado a versão anterior da norma, mas acho esse cenário bem menos provável.

Gabarito Oficial: ERRADA (questão polêmica).

**8. (CESPE/TRE-BA 2017) O processo de gestão de risco, de acordo com a NBR ISO/IEC 27005, inicia-se com o(a).**

- a) identificação de riscos.**
- b) definição do contexto.**
- c) valiação de riscos.**
- d) tratamento do risco.**



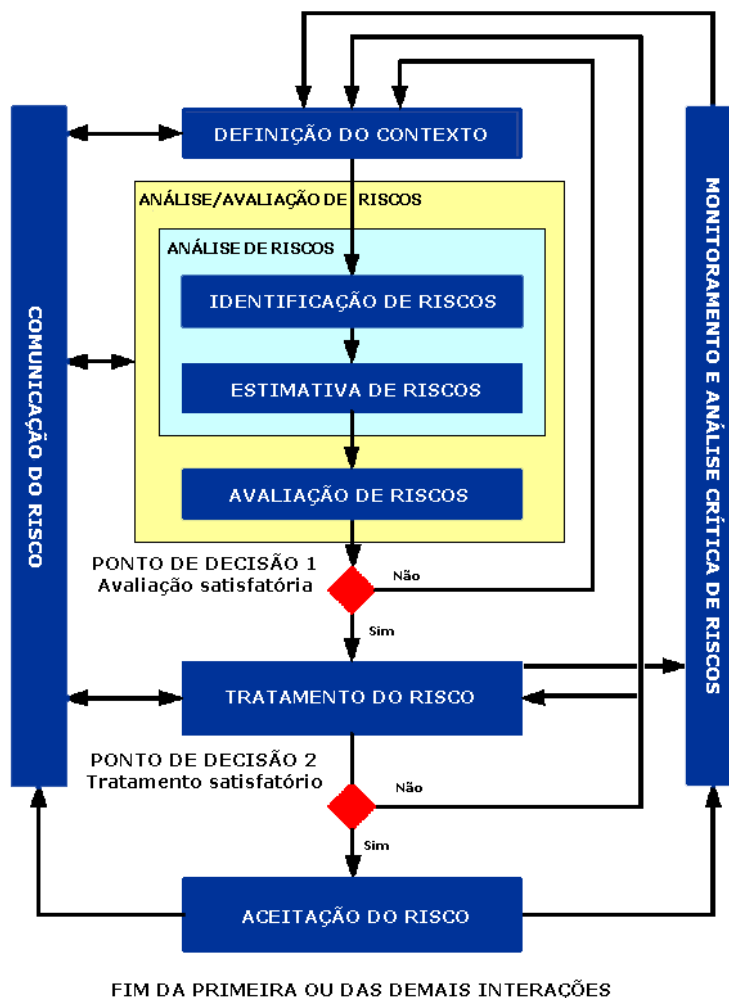
**e) monitoração dos riscos.**

Comentários:

Essa é “mel na chupeta”!

Caro aluno, não sei se você já notou, mas (praticamente) sempre que se perguntar como se inicia um processo, framework, metodologia, etc, e essa for uma das alternativas, pode marcar “<qualquer coisa> contexto”.

Revisitando o frame da 27.005, temos:



Gabarito Oficial: B

**9. (CESPE/TCE-RN 2015) É objeto da norma 27005 entender, desenvolver e implementar plano de continuidade de negócios em uma organização.**

Comentários:

É objeto da norma 27005 entender, desenvolver e implementar plano de continuidade de negócios em uma organização.

Apesar de a 27.005 fazer menção algumas vezes à “Continuidade do Negócio”, esta é tema da específico da 15.999, veja:

*Esta Norma estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN). O propósito desta Norma é fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização além de obter confiança nos negócios da organização com clientes e outras organizações. Ela permite também que a organização avalie sua capacidade de GCN de uma maneira consistente e reconhecida.*

*OBS: Apesar de ser ainda cobrada em concursos a ABNT NBR 15999-1:2007 foi cancelada em 05/10/2015 e substituída pela ABNT NBR ISO 22313:2015.*

Gabarito Oficial: ERRADA

**10. (CESPE/TCE-RN 2015) A norma 27005 contém a descrição do processo de gestão de riscos de segurança da informação e de suas atividades, mas a parte de comunicação e consulta do risco foi subdividida na norma 27005:CCR, que determina como deve ser o sistema de informação de gerenciamento do risco.**

Comentários:

Pesquisei e o único lugar onde encontrei o termo “27005:CCR” foi nessa questão.

Pudera, a Parte de comunicação e consulta do risco é tratada no próprio corpo da 27.005, diferente do que consta na assertiva.

Vejamos a Norma:

**4. Organização da Norma:**

(...)

*Todas as atividades de gestão de riscos de segurança da informação, apresentadas na Seção 6, são descritas nas seguintes seções:*

- *Definição do contexto na Seção 7,*
- *Processo de avaliação de riscos na Seção 8,*
- *Tratamento do risco na Seção 9,*
- *Aceitação do risco na Seção 10,*
- **Comunicação e consulta do risco na Seção 11.**
- *Monitoramento e análise crítica de riscos na Seção 12.*

Gabarito Oficial: ERRADA

**11. (CESPE/TRT - CE 2017) De acordo com a ABNT NBR ISO/IEC 27005, o propósito da gestão de riscos de segurança da informação pode ser**

- a) preparar um plano de resposta a incidentes.***
- b) monitorar controles de segurança da informação.***
- c) executar o processo de avaliação de riscos.***
- d) definir políticas.***

Comentários:

A despeito do aspecto formal para se chegar à resposta, o qual vamos apresentar logo a seguir, cabe uma observação aqui:

Embora seja muito comum a equipe encarregada se perder durante a implantação em discussões filosóficas - uma vez que o tema é rico e apaixonante -, a Gestão de Riscos serve na essência para isso mesmo “*preparar um plano de resposta a incidentes*”.

Ora, ao fim e ao caso, não adianta nada termos um lindo plano de gerenciamento de risco, com as melhores práticas, se eu não troco o extintor de incêndio vencido.

Depois do desabafo, vamos à Norma:

#### *7.1 Considerações Gerais*

*(...)*

**É essencial determinar o propósito da gestão de riscos de segurança da informação, pois ele afeta o processo em geral e a definição do contexto em particular. Esse propósito pode ser:**

- *Suporte a um SGSI*

- *Conformidade legal e evidência da devida diligência (“due diligence”)*
- *Preparação de um plano de continuidade de negócios*
- *Preparação de um plano de resposta a incidentes*
- *Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo*

Gabarito Oficial: A

**12. (CESPE/TJ-SE 2014) A perda de uma oportunidade de negócio devido a um evento de segurança da informação é considerada um critério de impacto.**

Comentários:

Apesar da sopa de definições misturadas, é praticamente o que diz a Norma, veja:

### **7.2.3 Critérios de impacto**

*Convém que os critérios de impacto sejam desenvolvidos e especificados em função do montante dos danos ou custos à organização causados por um evento relacionado com a segurança da informação, considerando o seguinte:*

- *Nível de classificação do ativo de informação afetado*
- *Ocorrências de violação da segurança da informação (por exemplo, perda da disponibilidade, da confidencialidade e/ou da integridade)*
- *Operações comprometidas (internas ou de terceiros)*
- *Perda de oportunidades de negócio e de valor financeiro*
- *Interrupção de planos e o não cumprimento de prazos*
- *Dano à reputação*
- *Violações de requisitos legais, regulatórios ou contratuais*

*NOTA Veja também a ABNT NBR ISO/IEC 27001:2006 [Seção 4.2.1 d) 4] com relação à identificação dos critérios de impacto, considerando a perda da confidencialidade, da integridade e/ou da disponibilidade.*

Gabarito Oficial: CERTA

**13. (CESPE/MEC 2015) Denomina-se avaliação de risco ao processo de busca, reconhecimento e descrição de riscos.**

Comentários:

Vamos à norma:

### **3.15 identificação de riscos**

processo de busca, reconhecimento e descrição de riscos (3.9)

[ABNT ISO GUIA 73:2009]

*NOTA 1 A identificação de riscos envolve a identificação das fontes de risco, eventos (3.3), suas causas e suas consequências (3.1) potenciais.*

*NOTA 2 A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas (3.18).*

Gabarito Oficial: ERRADA

### **14. (CESPE/MEC 2015) Uma consequência pode levar a um risco específico ou a uma série de riscos.**

Comentários:

Caros, para entender essa, é só lembra daquele velho pleonismo: “As consequências sempre vêm depois”.

Vamos à norma:

### **3.1 consequência**

*resultado de um evento (3.3) que afeta os objetivos*

[ABNT ISO GUIA 73:2009]

*NOTA 1 Um evento pode levar a uma série de consequências.*

*NOTA 2 Uma consequência pode ser certa ou incerta e, no contexto da segurança da informação, é, normalmente, negativa.*

*NOTA 3 As consequências podem ser expressas qualitativa ou quantitativamente.*

*NOTA 4 As consequências iniciais podem desencadear reações em cadeia.*

Gabarito Oficial: ERRADA

**15. (CESPE/MEC 2015) Através da utilização de formas adequadas de tratamento o risco deve deixar de existir.**

Comentários:

Note que a assertiva dá a entender (pelo menos na minha leitura) que o objetivo das formas de tratamento de riscos é a extinção do risco, o que não é fato por vários motivos. Por exemplo, o compartilhamento não visa à extinção dos riscos, mas a diluição entre as partes. De outro lado, tentar levar a modificação (redução) do risco para próximo de zero poder ser possível, mas rotineiramente inviável, quando consideramos disponibilidade e restrições de recursos.

Vamos à norma:

Em geral, convém que as consequências adversas do risco sejam reduzidas ao mínimo possível, independentemente de quaisquer critérios absolutos.

**Às vezes, a organização pode beneficiar-se substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais.**

Gabarito Oficial: ERRADA

**16. (CESPE/TJ-SE 2014) Deve ser recebida como entrada do processo de avaliação de riscos uma lista de cenários de incidentes identificados como relevantes, com as respectivas consequências para os processos de negócio.**

Comentários:

Vamos à norma..

Só existem dois processos que tem como:

Entrada: Uma lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos do negócio.

Um é:

### **8.3.2 Avaliação das consequências**

O outro é:

### **8.3.3 Avaliação da probabilidade dos incidentes**

Gabarito Oficial: ERRADA

**17. (CESPE/MEC 2015) Requisitos legais, regulatórios e contratuais estão entre os critérios para a escolha dos controles para tratamento do risco.**

Comentários:

Vejamos o que diz a Norma:

*Convém que controles apropriados e devidamente justificados sejam selecionados para satisfazer os requisitos identificados através do processo de avaliação de riscos e do tratamento dos mesmos.*

*Convém que essa escolha leve em conta os critérios para a aceitação do risco assim como requisitos legais, regulatórios e contratuais. Convém que essa seleção também leve em conta custos e prazos para a implementação de controles, além de aspectos técnicos, culturais e ambientais. Com frequência, é possível diminuir o custo total de propriedade de um sistema por meio de controles de segurança da informação apropriadamente selecionados.*

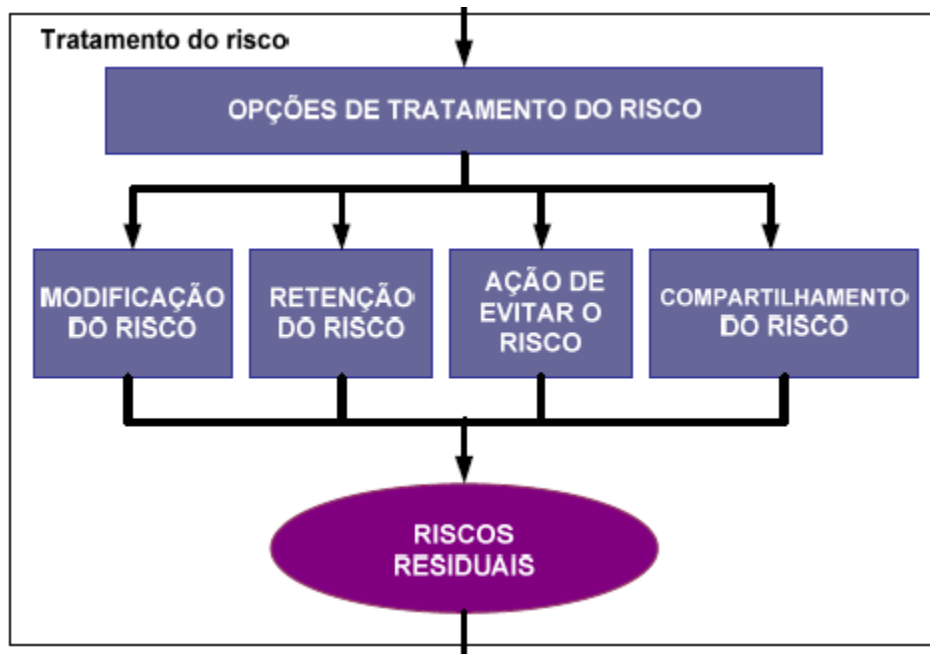
Gabarito Oficial: CERTA

**18. (CESPE/MEC 2015) Em um ambiente empresarial a retenção de um risco pode ser considerado como uma forma de tratá-lo.**

Comentários:

Resumindo, a Norma se aplica a qualquer organização.

E a forma de tratamento:



Gabarito Oficial: CERTA

**19. (CESPE/MEC 2015) Ativos de suporte representam as informações, os processos e as atividades de negócio.**

Comentários:

Na verdade, segundo a Norma, eles são ativos PRIMÁRIOS. Vejamos:

*Anexo B*

*(...)*

*B.1 Exemplos de identificação de ativos*

*(...)*

*Para estabelecer o valor de seus ativos, uma organização precisa primeiro identificá-los (num nível de detalhamento adequado). Dois tipos de ativos podem ser distinguidos:*

**Ativos primários:**

- *Processos e atividades do negócio*
- *Informação*

**Ativos de suporte e infraestrutura** (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:

- *Hardware*
- *Software*



- *Rede*
- *Recursos humanos*
- *Instalações físicas*
- *A estrutura da organização*

Gabarito Oficial: ERRADA

**20. (CESPE/TRF-1 2017) Na fase executar são realizadas ações que incluem a reaplicação do processo de GRSI.**

Comentários:

Guarde essa comparação entre os processos do GRSI e do SGSI e não erre mais:

Processos de GRSI x SGSI

- Definição do contexto. (Planejar)
- Avaliação de riscos. (Planejar)
- Definição do plano de tratamento do risco. (Planejar)
- Aceitação do risco. (Planejar)
- Implementação do plano de tratamento do risco. (Executar)
- Monitoramento contínuo e análise crítica de riscos. (Verificar)
- Manter e melhorar o processo de GRSI. (Agir)

Gabarito Oficial: ERRADA

**21. (CESPE/TRF-1 2017) Quanto ao tratamento de riscos, conforme a norma NBR ISO/IEC 27005, assinale a opção correta.**

**a) A remoção da fonte do risco é forma de tratamento do risco conhecida como modificação do risco.**

**b) Os riscos residuais são aqueles classificados como impossíveis de ser tratados.**

**c) A retenção do risco consiste na ação de implementar controles que busquem reduzir os riscos a um nível aceitável pela organização.**

**d) O compartilhamento do risco envolve transferência ou compartilhamento do risco com entidades internas da organização com**

***vistas a balancear os prejuízos entre as unidades na ocorrência de perdas advindas de um incidente.***

***e) A escolha de controles para reduzir os riscos a um nível aceitável pela organização deve considerar os seus critérios para a aceitação do risco, a exemplo dos requisitos legais, culturais e ambientais.***

Comentários:

- a) FALSO: Modificar riscos é variar sua probabilidade e/ou seu impacto e não remover sua fonte;
- b) FALSO: Risco residual na verdade é o risco remanescente após o tratamento do risco;
- c) FALSO: A definição da assertiva é referente a forma de tratamento “MODIFICAR”;
- d) FALDO: Ficaria correto se ele tivesse usado o termo “ENTIDADES EXTERNAS”.
- e) CERTA.

Gabarito Oficial: E

Galerinha, por hoje é só! Espero sinceramente que vocês estejam apreciando o curso.

Na próxima aula, vamos ver com a FCC aborda o tema!

Abraços!

WC

### **Enunciado das Questões Abordadas nessa aula**

1. *(CESPE/PREVIC 2011) De acordo com a norma NBR/ISO/IEC 27005, a comunicação de riscos visa assegurar que as informações sobre os riscos sejam compartilhadas entre os tomadores de decisão e outros stakeholders, buscando-se, assim, alcançar um entendimento de todos sobre como os riscos serão gerenciados.*
2. *(CESPE/MEC 2015) As restrições organizacionais devem ser levadas em conta durante o tratamento de risco.*
3. *(CESPE/MEC 2015) À luz da norma ISO/IEC 27005, julgue o item subsequente, acerca de gestão de riscos. No que diz respeito aos riscos de segurança da informação, essa norma não se aplica a qualquer tipo de organização.*
4. *(CESPE/TJDF 2015) A ISO 27005, que estabelece guias de referência para gerenciamento de risco em segurança da informação, é aplicável na maior parte das organizações, com exceção das agências de governo.*
5. *(CESPE/TRT 2016) De acordo com a norma NBR ISO/IEC 27005, a etapa em que se identifica qualquer mecanismo administrativo, físico ou operacional capaz de tratar os riscos da ocorrência de um incidente de segurança é a identificação*
  - a) *das ameaças.*
  - b) *dos controles existentes.*
  - c) *das vulnerabilidades.*
  - d) *das consequências.*
  - e) *dos ativos.*
6. *(CESPE/MEC 2015) Após ser realizado o tratamento de um risco poderá existir riscos não identificados.*

7. **(CESPE/TJ-SE 2014)** Após ser realizado o tratamento de um risco poderá existir riscos não identificados.
8. **(CESPE/TRE-BA 2017)** O processo de gestão de risco, de acordo com a NBR ISO/IEC 27005, inicia-se com o(a).
- a) identificação de riscos.
  - b) definição do contexto.
  - c) valiação de riscos.
  - d) tratamento do risco.
  - e) monitoração dos riscos.
9. **(CESPE/TCE-RN 2015)** É objeto da norma 27005 entender, desenvolver e implementar plano de continuidade de negócios em uma organização.
10. **(CESPE/TCE-RN 2015)** A norma 27005 contém a descrição do processo de gestão de riscos de segurança da informação e de suas atividades, mas a parte de comunicação e consulta do risco foi subdividida na norma 27005:CCR, que determina como deve ser o sistema de informação de gerenciamento do risco.
11. **(CESPE/TRT - CE 2017)** De acordo com a ABNT NBR ISO/IEC 27005, o propósito da gestão de riscos de segurança da informação pode ser
- a) preparar um plano de resposta a incidentes.
  - b) monitorar controles de segurança da informação.
  - c) executar o processo de avaliação de riscos.
  - d) definir políticas.
12. **(CESPE/TJ-SE 2014)** A perda de uma oportunidade de negócio devido a um evento de segurança da informação é considerada um critério de impacto.

13. *(CESPE/MEC 2015) Denomina-se avaliação de risco ao processo de busca, reconhecimento e descrição de riscos.*
14. *(CESPE/MEC 2015) Uma consequência pode levar a um risco específico ou a uma série de riscos.*
15. *(CESPE/MEC 2015) Através da utilização de formas adequadas de tratamento o risco deve deixar de existir.*
16. *(CESPE/TJ-SE 2014) Deve ser recebida como entrada do processo de avaliação de riscos uma lista de cenários de incidentes identificados como relevantes, com as respectivas consequências para os processos de negócio.*
17. *(CESPE/MEC 2015) Requisitos legais, regulatórios e contratuais estão entre os critérios para a escolha dos controles para tratamento do risco.*
18. *(CESPE/MEC 2015) Em um ambiente empresarial a retenção de um risco pode ser considerado como uma forma de tratá-lo.*
19. *(CESPE/MEC 2015) Ativos de suporte representam as informações, os processos e as atividades de negócio.*
20. *(CESPE/TRF-1 2017) Na fase executar são realizadas ações que incluem a reaplicação do processo de GRSI.*
21. *(CESPE/TRF-1 2017) Quanto ao tratamento de riscos, conforme a norma NBR ISO/IEC 27005, assinale a opção correta.*

### **Gabarito das Questões Abordadas nessa aula**

- 1. CERTA**
- 2. CERTA**
- 3. ERRADA**
- 4. ERRADA**
- 5. B**
- 6. CERTA**
- 7. ERRADA**
- 8. B**
- 9. ERRADA**
- 10. ERRADA**
- 11. A**
- 12. CERTA**
- 13. ERRADA**
- 14. ERRADA**
- 15. ERRADA**
- 16. ERRADA**
- 17. CERTA**
- 18. CERTA**
- 19. ERRADA**
- 20. ERRADA**
- 21. E**

### **Aula 3: Banca FCC**

Salve, salve, Galera! Prof. Walter Cunha novamente na área...

E aí, curtindo as Questões? É como eu falo, Questão em Concurso é igual a Cerveja em Churrasco, nunca pode faltar...

Hoje vamos ter a oportunidade de entender com a FCC aborda a Gestão de Riscos de Segurança da Informação (27.005).

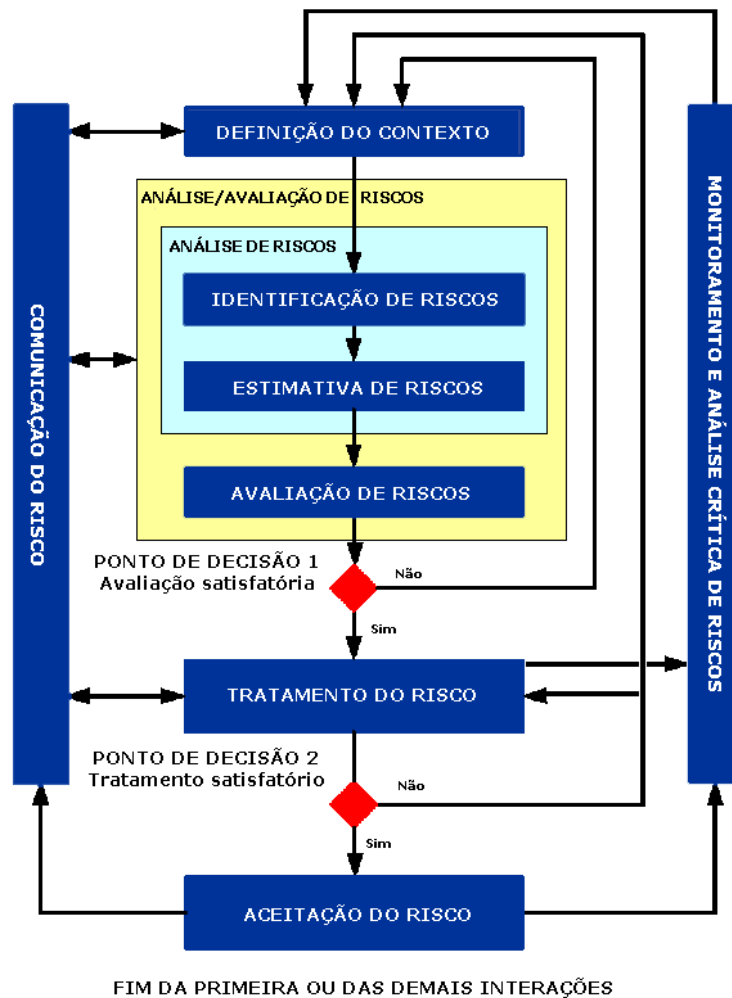
Não deixem de enviar suas solicitações, dúvidas e sugestões no fórum do curso ou para [falecomigo@waltercunha.com](mailto:falecomigo@waltercunha.com)!

**1. (FCC/SEFAZ-SP 2009) Segundo as normas ABNT sobre segurança da informação, o tratamento de risco está inserido no processo de**

- a) gestão de riscos.**
- b) aceitação do risco.**
- c) análise de riscos.**
- d) avaliação de riscos.**
- e) análise/avaliação de riscos.**

Comentários:

Basta olharmos o frame da Norma para ver que a única alternativa que engloba o “Tratamento” é o processo geral de Gestão de Riscos:



Gabarito Oficial: A

**2. (FCC/TRT-24 2017) Considere os processos abaixo.**

**Processos do SGSI**

- Planejar.
- Executar.
- Verificar.
- Agir.

**Processos de GRSI**

- Definição do contexto.



- Avaliação de riscos.**
- Definição do plano de tratamento do risco.**
- Aceitação do risco.**
- Implementação do plano de tratamento do risco.**
- Monitoramento contínuo e análise crítica de riscos.**
- Manter e melhorar o processo de GRSI.**

**A norma ABNT NBR ISO/IEC 27005:2011 apresenta o alinhamento do processo do Sistema de Gestão da Segurança da Informação – SGSI e do processo de Gestão de Riscos de Segurança da Informação – GRSI. Segundo a Norma, o processo de GRSI denominado**

- a) "Aceitação do risco" está alinhado com o processo do SGSI "Planejar".**
- b) "Avaliação de riscos" está alinhado com o processo do SGSI "Verificar".**
- c) "Manter e melhorar o processo de GRSI" está alinhado com o processo do SGSI "Verificar".**
- d) "Implementação do plano de tratamento do risco" está alinhado com o processo do SGSI "Agir".**
- e) "Aceitação do risco" está alinhado com o processo do SGSI "Verificar".**

Comentários:

Lembra da dica que eu dei na Aula 02? Não, então vamos lembrar...

*Guarde essa comparação entre os processos do GRSI e do SGSI e não erre mais:*

*Processos de GRSI x SGSI*

- Definição do contexto. (Planejar)*
- Avaliação de riscos. (Planejar)*
- Definição do plano de tratamento do risco. (Planejar)*
- Aceitação do risco. (Planejar)*
- Implementação do plano de tratamento do risco. (Executar)*
- Monitoramento contínuo e análise crítica de riscos. (Verificar)*

– *Manter e melhorar o processo de GRSI. (Agir)*

Gabarito Oficial: A

**3. (FCC/TRT-20 2016) Considere que o Tribunal Regional do Trabalho esteja seguindo orientações da norma ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de segurança da informação. Seguindo esta norma, a implantação do processo de gestão de riscos deve passar pelas etapas: definição do contexto, processo de avaliação de riscos, tratamento do risco,**

***a) análise de impacto do risco, monitoramento do risco e comunicação do risco.***

***b) aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos.***

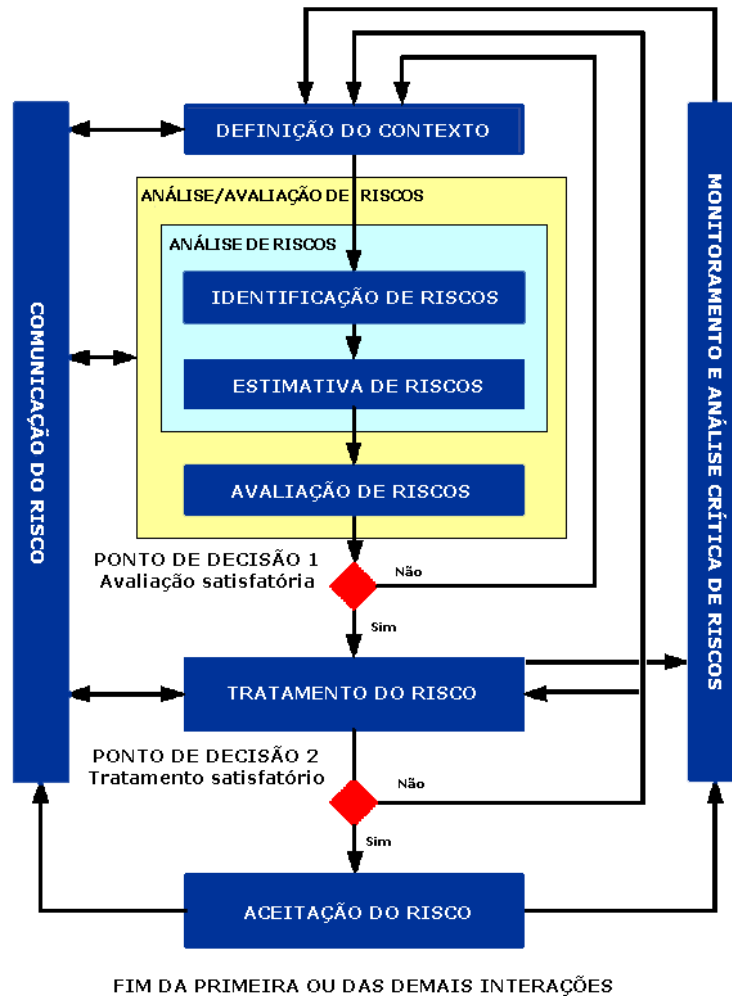
***c) mitigação do impacto do risco e análise crítica sobre o risco.***

***d) análise de impacto do risco, comunicação do risco e definição de ações de contenção do risco.***

***e) tomada de decisão sobre o risco, divulgação do risco na organização e monitoramento e controle de riscos.***

Comentários:

Basta olharmos o frame da Norma para ver que a única alternativa que engloba o “Tratamento” é o processo geral de Gestão de Riscos:



Os mais desavisados poderiam cair facilmente na letra A, a qual até poderia ser a resposta SE a B não fosse mais completa.

Gabarito Oficial: B

**4. (FCC/PGE-MT 2016) Considere, hipoteticamente, que a PGE-MT está diante de um risco de segurança da informação e o Analista de Sistemas terá que decidir que ação tomar. Resolve se guiar pela seção da norma ABNT NBR ISO/IEC 27005:2011 que discorre sobre o tratamento do risco de segurança da informação. Esta seção indica como ações para o tratamento do risco:**

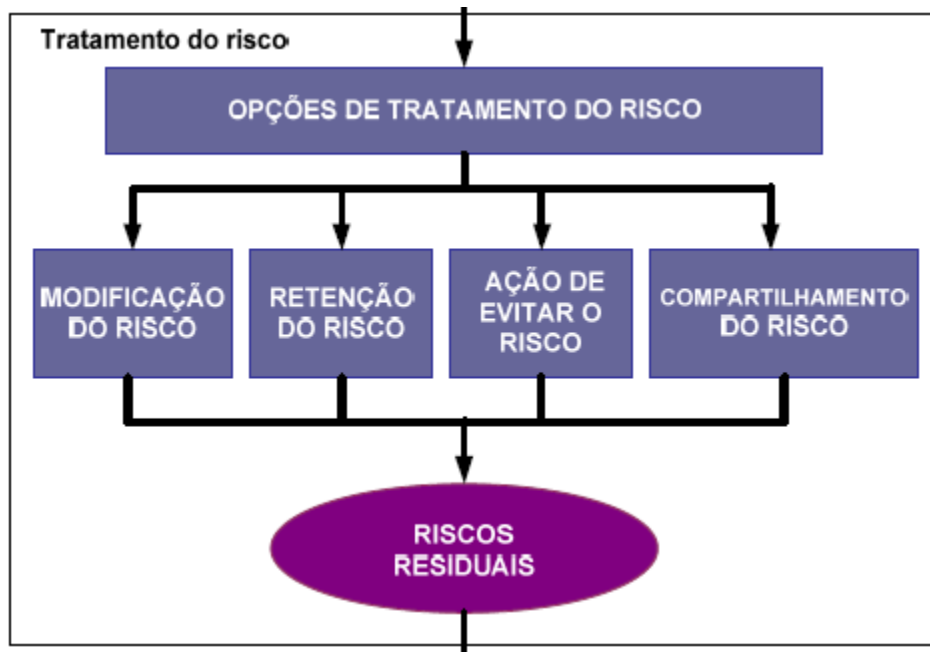
- a) modificar, reter, evitar e compartilhar.**
- b) evitar, monitorar, conter e terceirizar.**
- c) eliminar, aceitar, evitar e mitigar.**

**d) modificar, aceitar, ignorar, terceirizar.**

**e) identificar, monitorar, eliminar, divulgar.**

Comentários:

Recapitulando as formas de tratamento:



Então vamos destacar o que está COMPLETAMENTE errado em cada questão:

a) modificar, reter, evitar e compartilhar. CERTA

b) evitar, monitorar, conter e terceirizar.

c) eliminar, aceitar, evitar e mitigar.

d) modificar, aceitar, ignorar, terceirizar.

e) identificar, monitorar, eliminar, divulgar.

Outros itens como “terceirizar”, apesar de canonicamente errados, poderiam até ser aceito dependendo da rigidez da banca, por isso não foram destacados, ok?

Gabarito Oficial: A

**5. (FCC/ARTESP 2017) Segundo a Norma ABNT NBR ISO/IEC 27005:2011, a análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Uma metodologia para análise de riscos pode ser quantitativa, qualitativa ou uma combinação de ambas. A análise quantitativa**

**a) é utilizada em primeiro lugar, na prática, para obter uma indicação geral do nível de risco e para revelar os grandes riscos.**

**b) é normalmente menos complexa e menos onerosa que a análise qualitativa, já que a análise qualitativa é focada somente nos grandes riscos.**

**c) de riscos utiliza uma escala com atributos quantificadores que descrevem a magnitude das consequências potenciais (pequena, média ou grande) e a probabilidade dessas consequências ocorrerem.**

**d) de riscos tem como vantagem a facilidade de compreensão por todas as pessoas envolvidas, enquanto sua desvantagem é a dependência da escolha subjetiva da escala.**

**e) utiliza dados históricos dos incidentes, na maioria dos casos, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização.**

Comentários:

- a) ERRADA. Quando usadas em conjunto, a análise QUANTITATIVA deve vir depois da análise QUALITATIVA;
- b) ERRADA. É MAIS complexa e onerosa do que a QUALITATIVA, e não é só foca em grandes riscos;
- c) ERRADA. Característica referente à análise QUALITATIVA;
- d) ERRADA. Característica referente à análise QUALITATIVA;
- e) CERTA.

Gabarito Oficial: E

**6. (FCC/INFRAERO 2011) A norma ISO/IEC 27005:2008 adota o modelo “Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar os processos do ISMS (Information Security Management System). Na**

***fase “Do” do ISMS é representado o processo de gerenciamento de risco:***

- a) Risk acceptance.***
- b) Continual monitoring and reviewing of risks.***
- c) Implementation of risk treatment plan.***
- d) Maintain and improve the Information Security Risk Management Process.***
- e) Developing risk treatment plan..***

Comentários:

Recapitulando mais uma vez...

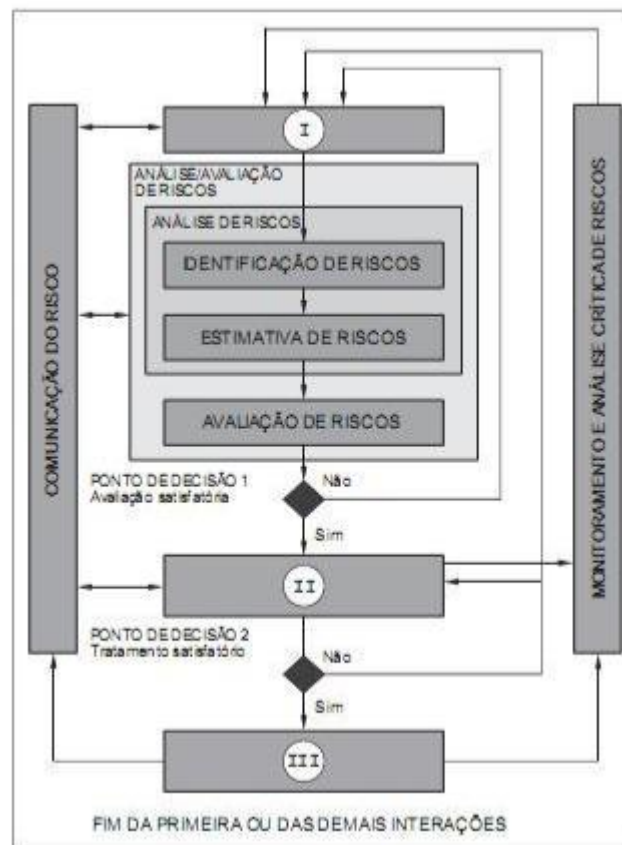
*Guarde essa comparação entre os processos do GRSI e do SGSI e não erre mais:*

*Processos de GRSI x SGSI*

- Definição do contexto. (Planejar)*
- Avaliação de riscos. (Planejar)*
- Definição do plano de tratamento do risco. (Planejar)*
- Aceitação do risco. (Planejar)*
- Implementação do plano de tratamento do risco. (Executar)*
- Monitoramento contínuo e análise crítica de riscos. (Verificar)*
- Manter e melhorar o processo de GRSI. (Agir)*

Gabarito Oficial: C

- 7. (FCC/SABESP 2014) De acordo com a Norma NBR ISO/IEC 27005, o processo de Gestão de Riscos da Segurança da Informação é composto pelas atividades mostradas na figura abaixo:**

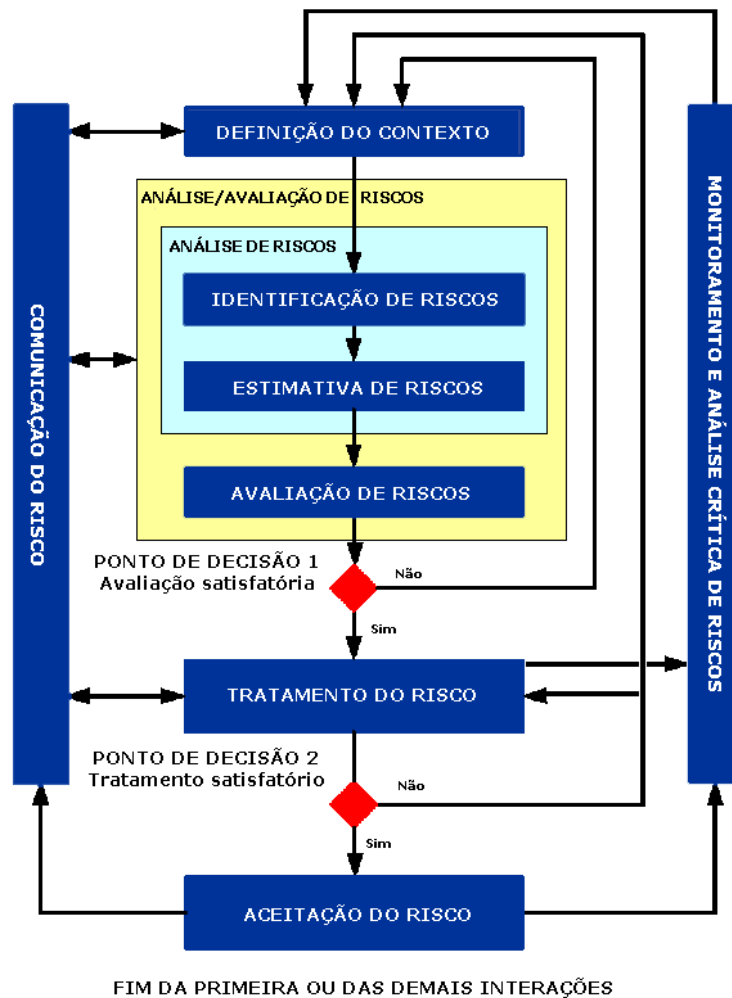


**As atividades I, II e III da figura acima correspondem, respectivamente, a:**

- a) Definição das ameaças; Categorização do risco; Tratamento do risco.**
- b) Avaliação das ameaças; Tratamento das ameaças; Aceitação dos riscos e ameaças.**
- c) Avaliação do contexto; Categorização das ameaças; Tratamento das ameaças.**
- d) Contextualização dos riscos; Tratamento dos riscos e das ameaças; Aceitação dos riscos e das ameaças.**
- e) Definição do contexto; Tratamento do risco; Aceitação do risco.**

Comentários:

Você não precisa ser nenhum gênio para perceber que os conceitos requeridos nas questões costumam se repetir ao longo do tempo. E esse é o “grande segredo dos concursos”.



Então, comparando as duas figuras, termos:

Gabarito Oficial: E

8. (FCC/Pref. Teresina-PI 2016) De acordo com a Norma NBR ISO/IEC 27005:2011, dentre as classes de ameaças conhecidas como ações não autorizadas, o único tipo de ameaça que é considerado acidental é

- a) o uso não autorizado de equipamento.
- b) a cópia ilegal de software.
- c) o comprometimento dos dados.
- d) o processamento ilegal de dados.



***e) o uso de cópias de software falsificadas ou ilegais.***

Comentários:

Essa foi mais puxada, pois tirou do Anexo.

Anexo C, NBR ISO/IEC 27005:2011

Para cada tipo de ameaça, ela pode ser considerada:

- I (intencional)
- A (acidental) ou
- N (natural).

Voltando ao enunciado:

- a) Uso não autorizado de equipamento I
- b) Cópia ilegal de software I
- c) Comprometimento dos dados I
- d) Processamento ilegal de dados I
- e) Uso de cópias de software falsificadas ou ilegais A, I

Gabarito Oficial: E

**9. (FCC/TRT-20 2016) No processo de tratamento do risco de segurança da informação, segundo a norma ABNT NBR ISO/IEC 27005:2011,**

***a) compartilha-se a responsabilidade de gerenciar riscos e também a responsabilidade legal por um impacto.***

***b) se o risco atender aos critérios legais para a aceitação do risco, devem ser implementados controles adicionais para que o risco possa ser aceito.***

***c) riscos considerados de impacto mediano ou alto, mesmo que os custos do tratamento não excedam os benefícios, devem ser evitados completamente.***

***d) o nível de risco pode ser gerenciado através da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.***

***e) determinar se o risco residual está ou não abaixo ou acima de um limite bem definido deve ser o único critério para aceitar ou não o risco.***

Comentários:

Vamos comentar cada item usando um trecho da Norma:

- a) ERRADA. *"Convém notar que é possível compartilhar a responsabilidade de gerenciar riscos, entretanto não é normalmente possível compartilhar a responsabilidade legal por um impacto."*
- b) ERRADA. *"Se o nível de risco atende aos critérios para a aceitação do risco, não há necessidade de se implementar controles adicionais e pode haver a retenção do risco."*
- c) ERRADA. *"Quando os riscos identificados são considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja através da eliminação de uma atividade planejada ou existente (ou de um conjunto de atividades), seja através de mudanças nas condições em que a operação da atividade ocorre."*
- d) CERTA;
- e) ERRADA. Existem outros critérios como descrito na seção 7.2.4 *Critérios para a aceitação do risco da norma.*

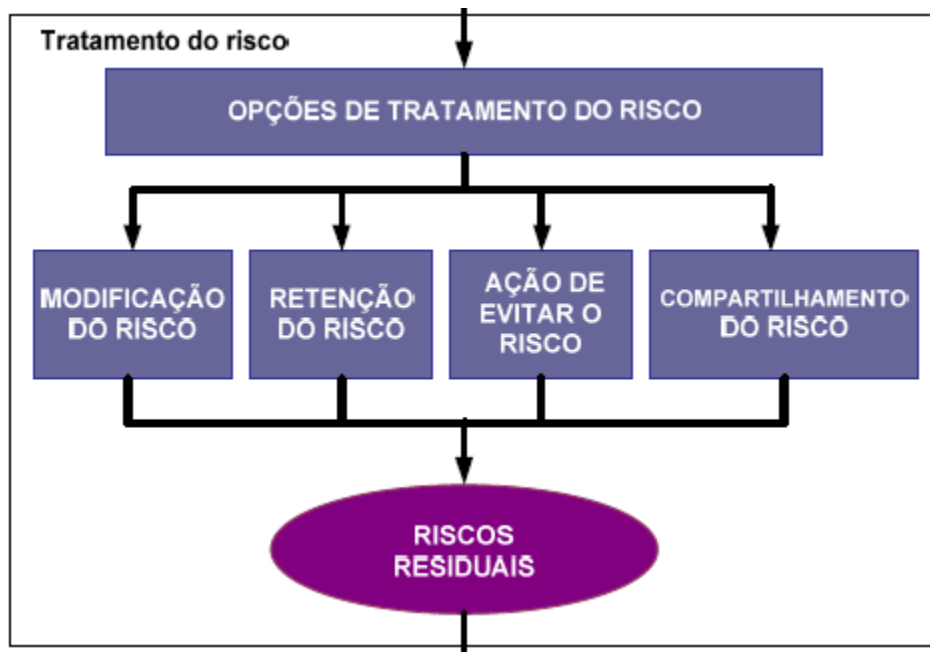
Gabarito Oficial: D

**10. (FCC/Perf. Teresina-PI 2016) A NBR ISO/IEC 27005:2011 NÃO considera como opção para o tratamento do risco de segurança da informação:**

- a) a retenção do risco.**
- b) a modificação do risco.**
- c) o compartilhamento do risco.**
- d) a eliminação do risco.**
- e) a ação de evitar o risco.**

Comentários:

Recapitulando as formas de tratamento:



Gabarito Oficial: D

**11. (FCC/Perf. Teresina-PI 2016) De acordo com a Norma NBR ISO/IEC 27005:2011, no processo de identificação de ativos da organização, um dos ativos do tipo primário é**

- a) a instalação física.**
- b) o recurso humano.**
- c) a informação.**
- d) a estrutura da organização.**
- e) a rede de comunicação.**

Comentários:

Mais uma questão de Anexo.

*Para estabelecer o valor de seus ativos, uma organização precisa primeiro identificá-los (num nível de detalhamento adequado). Dois tipos de ativos podem ser distinguidos:*

Ativos primários:

- *Processos e atividades do negócio*
- *Informação*

Ativos de suporte e infraestrutura (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:

- *Hardware*
- *Software*
- *Rede*
- *Recursos humanos*
- *Instalações físicas*
- *A estrutura da organização*

Gabarito Oficial: C

**12.(FCC/INFRAERO 2011) De acordo com a ISO/IEC 27005:2008, as opções completas para tratamento do risco são: mitigar (risk reduction),**

**a) ignorar (risk ignore), evitar (risk avoidance) e transferir (risk transfer).**

**b) aceitar (risk retention), evitar (risk avoidance) e transferir (risk transfer).**

**c) ignorar (risk ignore), aceitar (risk retention), evitar (risk avoidance) e transferir (risk transfer).**

**d) aceitar (risk retention), evitar (risk avoidance), transferir (risk transfer) e ocultar (risk hide).**

**e) evitar (risk avoidance) e transferir (risk transfer).**

Comentários:

Duas coisas que você tem que ficar ligado: (i) a terminologia em inglês; e (ii) a versão anterior da norma.

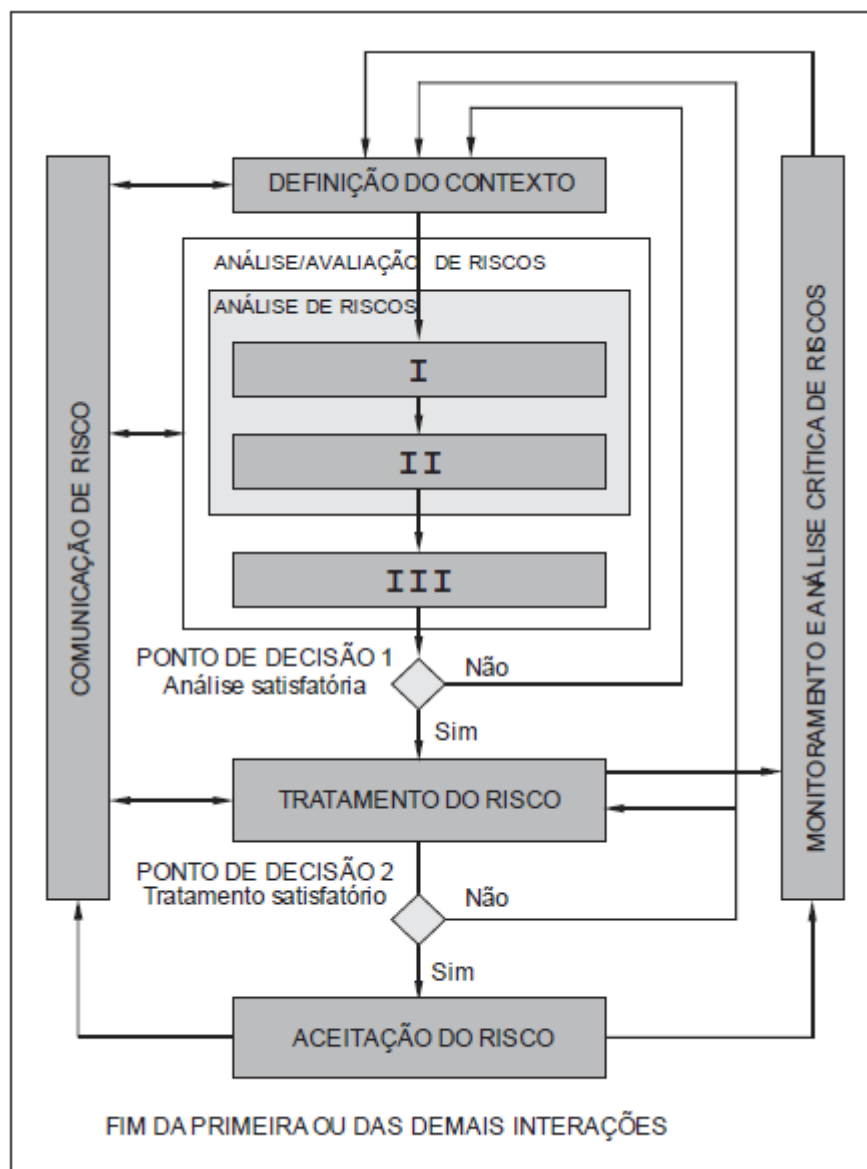
Como ele usou a versão anterior não vou usar figura, como é a nossa praxe, mas sim o texto da norma:

9.1 Descrição geral do processo de tratamento do risco

*Há quatro opções disponíveis para o tratamento do risco: modificação do risco (ver 9.2), retenção do risco (ver 9.3), ação de evitar o risco (ver 9.4) e compartilhamento do risco (ver 9.5).*

Gabarito Oficial: B

**13. (FCC/TRT-18 2013) Considere a figura abaixo que mostra o Sistema de Gestão de Riscos da Norma NBR ISO/IEC 27005: 2008**

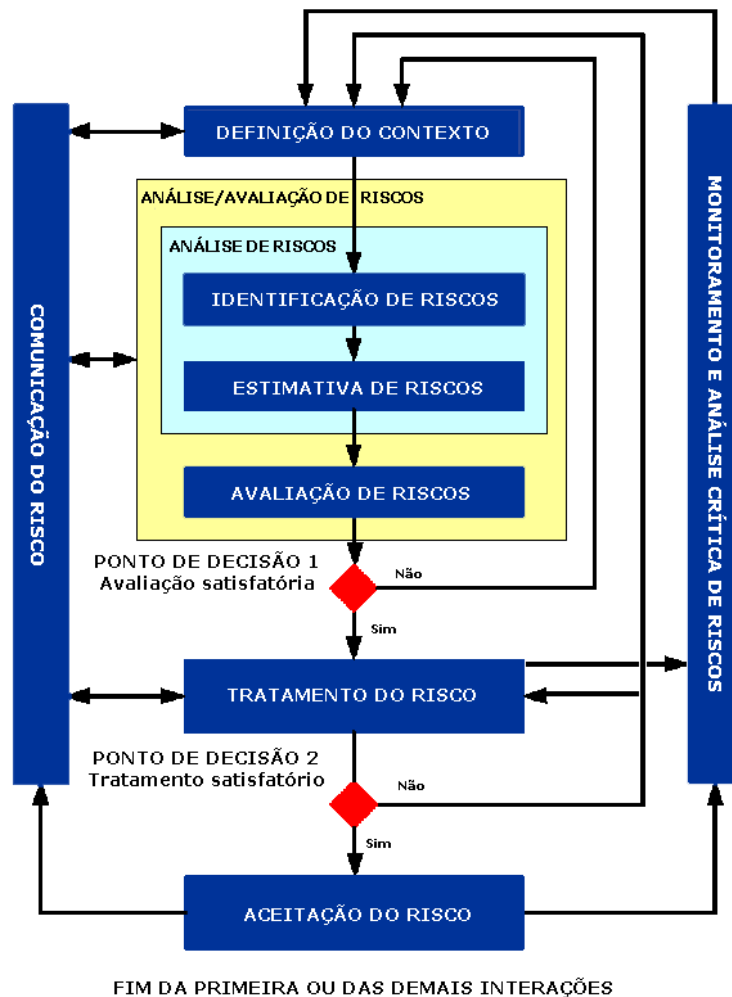


**A Análise/Avaliação de Riscos é composta das etapas I, II e III mostradas na figura acima, que se referem, respectivamente, a:**

- a) **Classificação de Riscos – Priorização de Riscos – Encaminhamento de Riscos.**
- b) **Identificação de Riscos – Estimativa de Riscos – Avaliação de Riscos.**
- c) **Reter o Risco – Evitar o Risco – Transferir o Risco.**
- d) **Identificação do Risco – Análise de Vulnerabilidade – Definição de Ações de Mitigação do Risco.**
- e) **Classificar o Risco – Priorizar o Risco – Mitigar o Risco.**

Comentários:

Recapitulando...



Então, comparando as duas figuras, termos:

Gabarito Oficial: B

**14. (FCC/TJ-AP 2014) Segundo Norma ABNT NBR ISO/IEC 27005:2011, convém que a organização defina sua própria escala de níveis de aceitação de risco e que critérios para a aceitação do risco**

**a) possam ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado.**

**b) possam incluir apenas um limite, representando um nível desejável de risco.**

**c) dependam das políticas, metas e objetivos da organização e nunca dos interesses das partes interessadas.**

**d) não sejam diferenciados de acordo com o tempo de existência previsto do risco.**

**e) não incluam requisitos para um tratamento adicional futuro do risco.**

Comentários:

Vejamos o que diz a Norma ABNT NBR ISO/IEC 27005:2011:

*"7.2.4 Critérios para a aceitação do risco*

*Convém que os critérios para a aceitação do risco sejam desenvolvidos e especificados. Os critérios de aceitação do risco dependem frequentemente das políticas, metas e objetivos da organização, assim como dos interesses das partes interessadas.*

*Convém que a organização defina sua própria escala de níveis de aceitação do risco. Convém que os seguintes tópicos sejam considerados durante o desenvolvimento:*

*Critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas por gestores seniores para aceitar riscos acima desse nível desde que sob circunstâncias definidas*

*Critérios para a aceitação do risco podem ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado*

*Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, por exemplo: riscos que podem resultar em não conformidade com regulamentações ou leis podem não ser aceitos, enquanto riscos de alto impacto poderão ser aceitos se isto for especificado como um requisito contratual".*

Gabarito Oficial: A

**15. (FCC/TJ-AP 2014) Segundo Norma ABNT NBR ISO/IEC 27005:2011, o processo de avaliação de riscos de segurança da informação consiste nas atividades de identificação de riscos, análise de riscos e avaliação de riscos. Segundo a Norma, a entrada da atividade de avaliação de riscos é uma lista de riscos**

**a) priorizada de acordo com os objetivos do negócio e com os cenários de incidentes.**

**b) associada a cada ativo, processo de negócio ou processo de TI.**

**c) categorizada e priorizada a partir da análise crítica dos incidentes ocorridos.**

**d) com níveis de valores designados e critérios para a avaliação de riscos.**

**e) e cenários de incidentes com suas consequências associadas aos ativos e processos de negócio.**

Comentários:

Vejamos o que diz a Norma ABNT NBR ISO/IEC 27005:2011:

**"8.4 Avaliação de riscos**

**Entrada:** Uma lista de riscos com níveis de valores designados e critérios para a avaliação de riscos.

**Ação:** Convém que o nível dos riscos seja comparado com os critérios de avaliação de riscos e com os critérios para a aceitação do risco (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 e 4)).

Gabarito Oficial: D



**16. (FCC/TRT-3 2015) Um analista de TI está utilizando as recomendações da norma ABNT NBR ISO/IEC 27005:2011 para realizar o tratamento de riscos dentro do processo de gestão de riscos de segurança da informação. Nesse contexto, a norma recomenda que**

- a) um plano de tratamento de riscos seja definido identificando os riscos mais prováveis, as formas de tratar estes riscos, independente das prioridades, e os prazos de execução das ações de tratamento de risco indicadas.**
- b) as opções de tratamento do risco sejam selecionadas apenas com base no resultado do processo de avaliação de riscos e no custo esperado para implementações dessas opções.**
- c) as quatro opções para tratamento do risco sejam aplicadas de forma mutuamente exclusiva, ou seja, não combinadas.**
- d) as opções de tratamento do risco sejam consideradas levando-se em conta como o risco é percebido pelas partes afetadas e as formas mais apropriadas de comunicação com estas partes.**
- e) as consequências adversas do risco sejam reduzidas ao mínimo possível de acordo com critérios absolutos, como a probabilidade do risco, pois riscos mais prováveis devem ser os primeiros a serem considerados.**

Comentários:

Com base na Norma ABNT NBR ISO/IEC 27005:2011:

- a) **ERRADA.** “Convém que um plano de tratamento do risco seja definido, identificando claramente a ordem de prioridade em que as formas específicas de tratamento do risco convém ser implementadas, assim como os seus prazos de execução”.
- b) **ERRADA.** “Convém que as opções do tratamento do risco sejam selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos”.
- c) **ERRADA.** As quatro opções para o tratamento do risco não são mutuamente exclusivas.
- d) **CERTA**

e) *ERRADA. “Em geral, convém que as consequências adversas do risco sejam reduzidas ao mínimo possível, independentemente de quaisquer critérios absolutos”.*

Gabarito Oficial: D

**17. (FCC/TCE-CE 2015) Segundo a norma NBR ISO/IEC 27005:2011, que trata da Gestão de Riscos de Segurança da Informação,**

**a) atividades de tratamento de riscos só podem ser realizadas uma vez no processo de Gestão de Riscos.**

**b) a atividade de análise/avaliação de riscos é composta pelas sub-atividades: identificar os riscos, estimar os riscos, classificar os riscos e responder aos riscos.**

**c) atividades de análise/avaliação de riscos só podem ser realizadas uma vez no processo de Gestão de Riscos.**

**d) as opções de tratamento do risco são: reduzir o risco, reter o risco, evitar o risco e ignorar o risco.**

**e) a atividade de tratamento do risco será iniciada somente se a avaliação do risco for satisfatória.**

Comentários:

Com base na Norma ABNT NBR ISO/IEC 27005:2011:

a) *ERRADA. O processo é cíclico.*

b) *ERRADA. As subatividades são identificar, estimar e avaliar;*

c) *CERTA.*

d) *ERRADA. Tratamento: Modificar, Reter, Compartilhar e Evitar;*

e) *ERRADA. O processo é cíclico.*

Gabarito Oficial: C

Galerinha, por hoje é só! Por favor, revisem todas as questões de modo a fixar o conhecimento adquirido até aqui.

E para fechar, na próxima aula vamos ver com a outras Bancas, menos expressivas abordam o tema!

Bons Estudos!

WC

**Enunciado das Questões Abordadas na Aula 3: Banca FCC (27.005)**

**1. (FCC/SEFAZ-SP 2009) Segundo as normas ABNT sobre segurança da informação, o tratamento de risco está inserido no processo de**

- a) gestão de riscos.**
- b) aceitação do risco.**
- c) análise de riscos.**
- d) avaliação de riscos.**
- e) análise/avaliação de riscos.**

**2. (FCC/TRT-24 2017) Considere os processos abaixo.**

**Processos do SGSI**

- Planejar.**
- Executar.**
- Verificar.**
- Agir.**

**Processos de GRSI**

- Definição do contexto.**
- Avaliação de riscos.**
- Definição do plano de tratamento do risco.**
- Aceitação do risco.**
- Implementação do plano de tratamento do risco.**
- Monitoramento contínuo e análise crítica de riscos.**
- Manter e melhorar o processo de GRSI.**

**A norma ABNT NBR ISO/IEC 27005:2011 apresenta o alinhamento do processo do Sistema de Gestão da Segurança da Informação – SGSI e do**

***processo de Gestão de Riscos de Segurança da Informação – GRSI. Segundo a Norma, o processo de GRSI denominado***

- a) "Aceitação do risco" está alinhado com o processo do SGSI "Planejar".***
- b) "Avaliação de riscos" está alinhado com o processo do SGSI "Verificar".***
- c) "Manter e melhorar o processo de GRSI" está alinhado com o processo do SGSI "Verificar".***
- d) "Implementação do plano de tratamento do risco" está alinhado com o processo do SGSI "Agir".***
- e) "Aceitação do risco" está alinhado com o processo do SGSI "Verificar".***

***3. (FCC/TRT-20 2016) Considere que o Tribunal Regional do Trabalho esteja seguindo orientações da norma ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de segurança da informação. Seguindo esta norma, a implantação do processo de gestão de riscos deve passar pelas etapas: definição do contexto, processo de avaliação de riscos, tratamento do risco,***

***a) análise de impacto do risco, monitoramento do risco e comunicação do risco.***

***b) aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos.***

***c) mitigação do impacto do risco e análise crítica sobre o risco.***

***d) análise de impacto do risco, comunicação do risco e definição de ações de contenção do risco.***

***e) tomada de decisão sobre o risco, divulgação do risco na organização e monitoramento e controle de riscos.***

***4. (FCC/PGE-MT 2016) Considere, hipoteticamente, que a PGE-MT está diante de um risco de segurança da informação e o Analista de Sistemas terá que decidir que ação tomar. Resolve se guiar pela seção da norma ABNT NBR ISO/IEC 27005:2011 que discorre sobre o***

***tratamento do risco de segurança da informação. Esta seção indica como ações para o tratamento do risco:***

- a) modificar, reter, evitar e compartilhar.***
- b) evitar, monitorar, conter e terceirizar.***
- c) eliminar, aceitar, evitar e mitigar.***
- d) modificar, aceitar, ignorar, terceirizar.***
- e) identificar, monitorar, eliminar, divulgar.***

- 5. (FCC/ARTESP 2017) Segundo a Norma ABNT NBR ISO/IEC 27005:2011, a análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Uma metodologia para análise de riscos pode ser quantitativa, qualitativa ou uma combinação de ambas. A análise quantitativa**

***a) é utilizada em primeiro lugar, na prática, para obter uma indicação geral do nível de risco e para revelar os grandes riscos.***

***b) é normalmente menos complexa e menos onerosa que a análise qualitativa, já que a análise qualitativa é focada somente nos grandes riscos.***

***c) de riscos utiliza uma escala com atributos quantificadores que descrevem a magnitude das consequências potenciais (pequena, média ou grande) e a probabilidade dessas consequências ocorrerem.***

***d) de riscos tem como vantagem a facilidade de compreensão por todas as pessoas envolvidas, enquanto sua desvantagem é a dependência da escolha subjetiva da escala.***

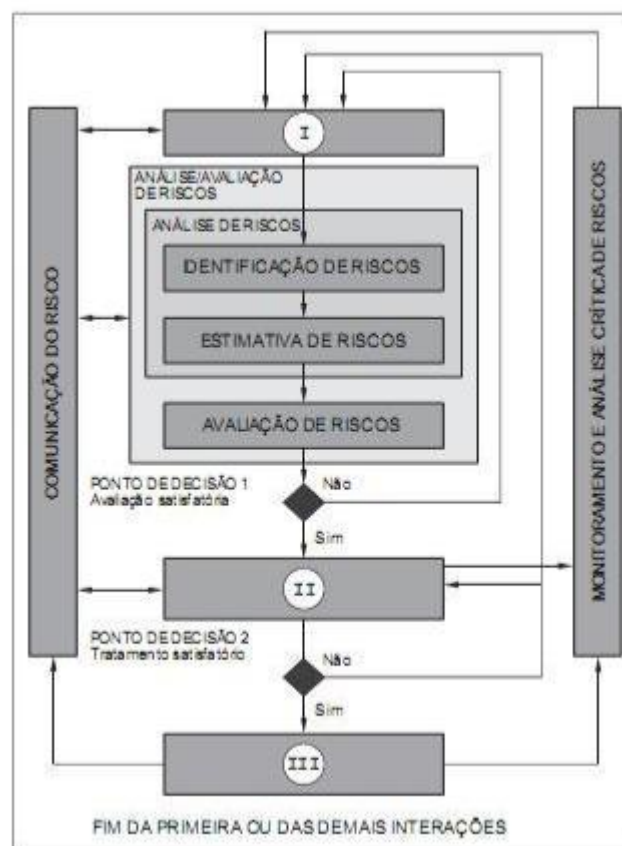
***e) utiliza dados históricos dos incidentes, na maioria dos casos, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização.***

- 6. (FCC/SABESP 2014) A norma ISO/IEC 27005:2008 adota o modelo “Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar os processos do ISMS (Information Security Management System). Na**

**fase “Do” do ISMS é representado o processo de gerenciamento de risco:**

- a) Risk acceptance.**
- b) Continual monitoring and reviewing of risks.**
- c) Implementation of risk treatment plan.**
- d) Maintain and improve the Information Security Risk Management Process.**
- e) Developing risk treatment plan..**

**7. (FCC/INFRAERO 2011) De acordo com a Norma NBR ISO/IEC 27005, o processo de Gestão de Riscos da Segurança da Informação é composto pelas atividades mostradas na figura abaixo:**



**As atividades I, II e III da figura acima correspondem, respectivamente, a:**

- a) *Definição das ameaças; Categorização do risco; Tratamento do risco.*
  - b) *Avaliação das ameaças; Tratamento das ameaças; Aceitação dos riscos e ameaças.*
  - c) *Avaliação do contexto; Categorização das ameaças; Tratamento das ameaças.*
  - d) *Contextualização dos riscos; Tratamento dos riscos e das ameaças; Aceitação dos riscos e das ameaças.*
  - e) *Definição do contexto; Tratamento do risco; Aceitação do risco.*
8. (FCC/Pref. Teresina-PI 2016) *De acordo com a Norma NBR ISO/IEC 27005:2011, dentre as classes de ameaças conhecidas como ações não autorizadas, o único tipo de ameaça que é considerado acidental é*
- a) *o uso não autorizado de equipamento.*
  - b) *a cópia ilegal de software.*
  - c) *o comprometimento dos dados.*
  - d) *o processamento ilegal de dados.*
  - e) *o uso de cópias de software falsificadas ou ilegais.*
9. (FCC/TRT-20 2016) *No processo de tratamento do risco de segurança da informação, segundo a norma ABNT NBR ISO/IEC 27005:2011,*
- a) *compartilha-se a responsabilidade de gerenciar riscos e também a responsabilidade legal por um impacto.*
  - b) *se o risco atender aos critérios legais para a aceitação do risco, devem ser implementados controles adicionais para que o risco possa ser aceito.*
  - c) *riscos considerados de impacto mediano ou alto, mesmo que os custos do tratamento não excedam os benefícios, devem ser evitados completamente.*
  - d) *o nível de risco pode ser gerenciado através da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.*



***e) determinar se o risco residual está ou não abaixo ou acima de um limite bem definido deve ser o único critério para aceitar ou não o risco.***

**10. (FCC/Perf. Teresina-PI 2016) A NBR ISO/IEC 27005:2011 NÃO considera como opção para o tratamento do risco de segurança da informação:**

- a) a retenção do risco.***
- b) a modificação do risco.***
- c) o compartilhamento do risco.***
- d) a eliminação do risco.***
- e) a ação de evitar o risco.***

**11. (FCC/Perf. Teresina-PI 2016) De acordo com a Norma NBR ISO/IEC 27005:2011, no processo de identificação de ativos da organização, um dos ativos do tipo primário é**

- a) a instalação física.***
- b) o recurso humano.***
- c) a informação.***
- d) a estrutura da organização.***
- e) a rede de comunicação.***

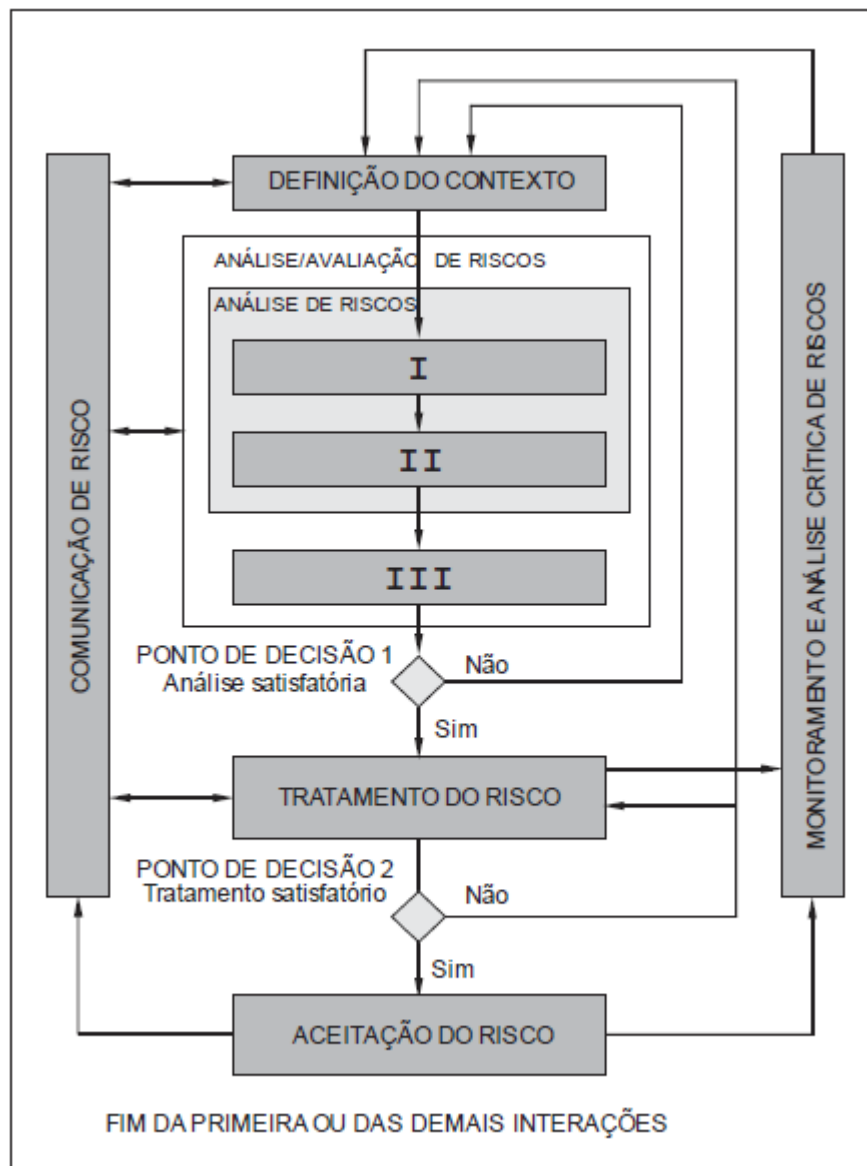
**12. (FCC/INFRAERO 2011) De acordo com a ISO/IEC 27005:2008, as opções completas para tratamento do risco são: mitigar (risk reduction),**

- a) ignorar (risk ignore), evitar (risk avoidance) e transferir (risk transfer).***
- b) aceitar (risk retention), evitar (risk avoidance) e transferir (risk transfer).***
- c) ignorar (risk ignore), aceitar (risk retention), evitar (risk avoidance) e transferir (risk transfer).***

**d) aceitar (risk retention), evitar (risk avoidance), transferir (risk transfer) e ocultar (risk hide).**

**e) evitar (risk avoidance) e transferir (risk transfer).**

**13. (FCC/TRT-18 2013) Considere a figura abaixo que mostra o Sistema de Gestão de Riscos da Norma NBR ISO/IEC 27005: 2008**



**A Análise/Avaliação de Riscos é composta das etapas I, II e III mostradas na figura acima, que se referem, respectivamente, a:**

***A Classificação de Riscos – Priorização de Riscos – Encaminhamento de Riscos.***

***B Identificação de Riscos – Estimativa de Riscos – Avaliação de Riscos.***

***C Reter o Risco – Evitar o Risco – Transferir o Risco.***

***D Identificação do Risco – Análise de Vulnerabilidade – Definição de Ações de Mitigação do Risco.***

***E Classificar o Risco – Priorizar o Risco – Mitigar o Risco.***

**14. (FCC/TJ-AP 2014) Segundo Norma ABNT NBR ISO/IEC 27005:2011, convém que a organização defina sua própria escala de níveis de aceitação de risco e que critérios para a aceitação do risco**

***A possam ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado.***

***B possam incluir apenas um limite, representando um nível desejável de risco.***

***C dependam das políticas, metas e objetivos da organização e nunca dos interesses das partes interessadas.***

***D não sejam diferenciados de acordo com o tempo de existência previsto do risco.***

***E não incluam requisitos para um tratamento adicional futuro do risco.***

**15. (FCC/TJ-AP 2014) Segundo Norma ABNT NBR ISO/IEC 27005:2011, o processo de avaliação de riscos de segurança da informação consiste nas atividades de identificação de riscos, análise de riscos e avaliação de riscos. Segundo a Norma, a entrada da atividade de avaliação de riscos é uma lista de riscos**

***A priorizada de acordo com os objetivos do negócio e com os cenários de incidentes.***

***B associada a cada ativo, processo de negócio ou processo de TI.***

***C categorizada e priorizada a partir da análise crítica dos incidentes ocorridos.***

***D com níveis de valores designados e critérios para a avaliação de riscos.***

***E e cenários de incidentes com suas consequências associadas aos ativos e processos de negócio.***

**16. (FCC/TRT-3 2015) Um analista de TI está utilizando as recomendações da norma ABNT NBR ISO/IEC 27005:2011 para realizar o tratamento de riscos dentro do processo de gestão de riscos de segurança da informação. Nesse contexto, a norma recomenda que**

***A um plano de tratamento de riscos seja definido identificando os riscos mais prováveis, as formas de tratar estes riscos, independente das prioridades, e os prazos de execução das ações de tratamento de risco indicadas.***

***B as opções de tratamento do risco sejam selecionadas apenas com base no resultado do processo de avaliação de riscos e no custo esperado para implementações dessas opções.***

***C as quatro opções para tratamento do risco sejam aplicadas de forma mutuamente exclusiva, ou seja, não combinadas.***

***D as opções de tratamento do risco sejam consideradas levando-se em conta como o risco é percebido pelas partes afetadas e as formas mais apropriadas de comunicação com estas partes.***

***E as consequências adversas do risco sejam reduzidas ao mínimo possível de acordo com critérios absolutos, como a probabilidade do risco, pois riscos mais prováveis devem ser os primeiros a serem considerados.***

**17. (FCC/TCE-CE 2015) Segundo a norma NBR ISO/IEC 27005:2011, que trata da Gestão de Riscos de Segurança da Informação,**

***A atividades de tratamento de riscos só podem ser realizadas uma vez no processo de Gestão de Riscos.***

***B a atividade de análise/avaliação de riscos é composta pelas sub-atividades: identificar os riscos, estimar os riscos, classificar os riscos e responder aos riscos.***

***C atividades de análise/avaliação de riscos só podem ser realizadas uma vez no processo de Gestão de Riscos.***

***D as opções de tratamento do risco são: reduzir o risco, reter o risco, evitar o risco e ignorar o risco.***

***E a atividade de tratamento do risco será iniciada somente se a avaliação do risco for satisfatória.***

### **Gabarito das Questões Abordadas na Aula 3: Banca FCC (27.005)**

1. ***(FCC/SEFAZ-SP 2009)*** - Gabarito Oficial: A
2. ***(FCC/TRT-24 2017)*** - Gabarito Oficial: A
3. ***(FCC/TRT-20 2016)*** - Gabarito Oficial: B
4. ***(FCC/PGE-MT 2016)*** - Gabarito Oficial: A
5. ***(FCC/ARTESP 2017)*** - Gabarito Oficial: E
6. ***(FCC/SABESP 2014)*** - Gabarito Oficial: C
7. ***(FCC/INFRAERO 2011)*** - Gabarito Oficial: E
8. ***(FCC/Pref. Teresina-PI 2016)*** - Gabarito Oficial: E
9. ***(FCC/TRT-20 2016)*** - Gabarito Oficial: D
10. ***(FCC/Perf. Teresina-PI 2016)*** - Gabarito Oficial: D
11. ***(FCC/Perf. Teresina-PI 2016)*** - Gabarito Oficial: C
12. ***(FCC/INFRAERO 2011)*** - Gabarito Oficial: B
13. ***(FCC/TRT-18 2013)*** - Gabarito Oficial: B
14. ***(FCC/TJ-AP 2014)*** - Gabarito Oficial: A
15. ***(FCC/TJ-AP 2014)*** - Gabarito Oficial: D
16. ***(FCC/TRT-3 2015)*** - Gabarito Oficial: D
17. ***(FCC/TCE-CE 2015)*** - Gabarito Oficial: C

## **Aula 4: Outras Bancas**

Salve, salve, Galera! Prof. Walter Cunha novamente na área...

Estamos chegando ao fim do curso. Espero sinceramente que ele esteja agregando valor à sua preparação.

Hoje vamos ter a oportunidade de entender como a Gestão de Riscos de Segurança da Informação (27.005) é abordada pelas OUTRAS BANCAS de menor expressão nacional.

Não deixem de enviar suas solicitações, dúvidas e sugestões no fórum do curso ou para [falecomigo@waltercunha.com](mailto:falecomigo@waltercunha.com)!

**1. (FGV/FIOCRUZ 2010) Com relação à análise de risco em segurança da informação, considere os tipos de risco a seguir.**

***I. Dano físico, como fogo, vandalismo e desastres naturais.***

***II. Perda de dados, seja intencional ou não.***

***III. Falha de equipamento.***

***IV. Risco de mercado e perda de investimento.***

***Assinale:***

***a) se uma empresa deve estar atenta, em sua análise, somente aos riscos I, II e III.***

***b) se uma empresa deve estar atenta, em sua análise, a todos esses tipos de riscos.***

***c) se uma empresa deve estar atenta, em sua análise, somente aos riscos I e II.***

***d) se uma empresa deve estar atenta, em sua análise, somente aos riscos II e III.***

***e) se uma empresa deve estar atenta, em sua análise, somente aos riscos I e IV.***

Comentários:

A “sacada” dessa questão é saber distinguir Riscos (intrínsecos) de Segurança da Informação de Riscos de (exógenos) de Mercado. Se você for um profissional atuante de Tecnologia da Informação, vai perceber que os riscos

de I a III fazem parte do seu dia-a-dia (Riscos de SI). Já o IV é risco corporativo típico do Nível Estratégico.

Gabarito Oficial: A

**2. (CONSULPLAN/TRT-2 2017) A Norma Brasileira ABNT NBR ISO/IEC 27005:2011 é responsável pela Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de Segurança da Informação, fornecendo diretrizes para o processo de gestão de riscos de segurança da informação, de acordo com os padrões do Sistema de Gestão de Segurança da Informação (SGSI). Os gestores, além do pessoal envolvido com a gestão de riscos de segurança da informação em uma organização, são as pessoas que têm maior interesse nesta norma, ou também entidades externas que dão suporte a essas atividades. Esta norma apresenta diversas atividades que possuem: Entrada; Ação; Diretrizes para implementação; e, Saída. “Trata-se da comunicação que é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas.” A afirmativa anterior trata-se de:**

- a) Avaliação do risco.**
- b) Percepção do risco.**
- c) Comunicação do risco.**
- d) Monitoramento do risco.**

Comentários:

Segundo a ABNT NBR ISO/IEC 27005:

**Comunicação e consulta do risco de segurança da informação**

**Entrada:** Todas as informações sobre os riscos obtidas através das atividades de gestão de riscos (ver Figura 2).

**Ação:** Convém que as informações sobre riscos sejam trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas.

Diretrizes para implementação:

*A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.*

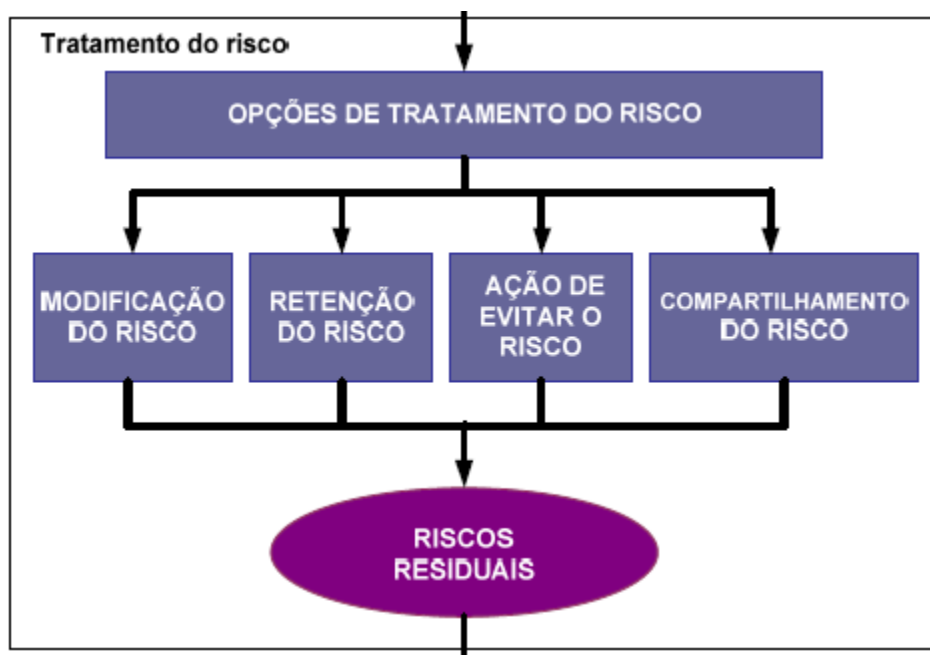
Gabarito Oficial: C

**3. (VUNESP/SAEG 2015) A norma NBR ISO/IEC 27005 apresenta 4 opções para o tratamento de riscos relacionados à segurança da informação. Uma dessas opções é**

- a) Retenção do Risco.**
- b) Transição do Risco.**
- c) Serialização do Risco.**
- d) Congelamento do Risco.**
- e) Empacotamento do Risco.**

Comentários:

Recapitulando as formas de tratamento:





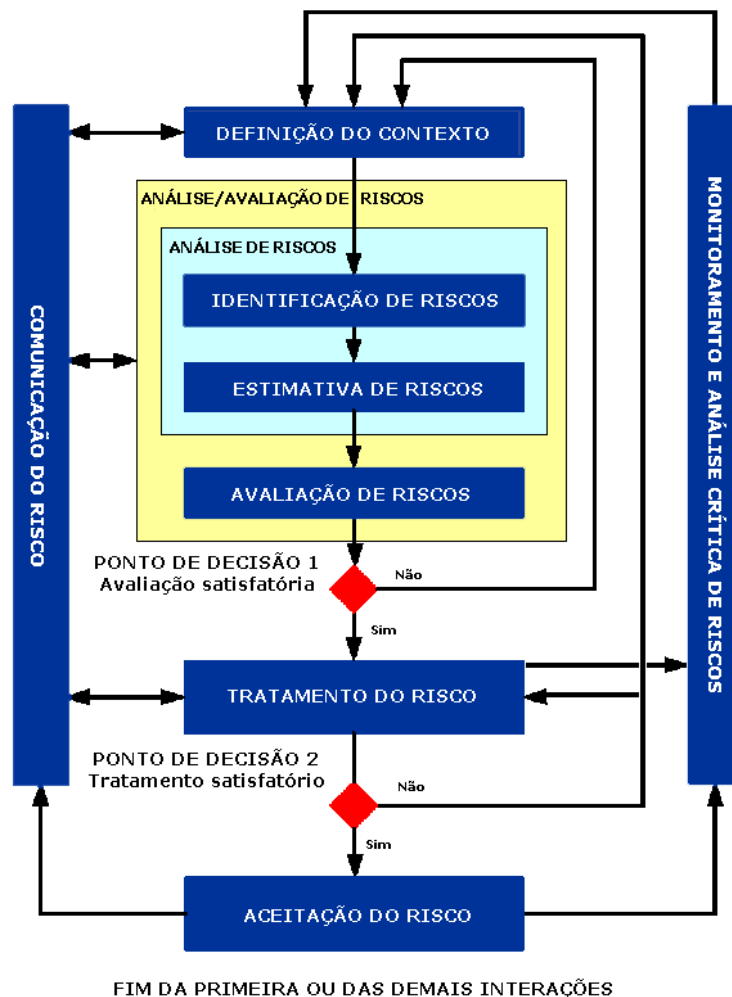
Gabarito Oficial: A

4. (FEMERJ/TCE-RJ 2012) A gestão de riscos envolve diversas atividades. Segundo a norma ISO 27005, faz parte da atividade chamada análise/ avaliação de riscos:

- a) a definição de contexto;
- b) a estimativa de riscos;
- c) o tratamento do risco;
- d) a comunicação do risco;
- e) a aceitação do risco.

Comentários:

Recapitulando o frame da Norma:



Gabarito Oficial: B

**5. (FEMERJ/TCE-RJ 2012) De acordo com a norma ISO 27005, a retenção de riscos:**

**a) analisa apenas atos intencionais que possam produzir violações de segurança;**

**b) trata apenas fragilidades em ativos de informação, as chamadas ameaças;**

**c) considera somente consequências negativas (perdas);**

**d) procura eliminar uma atividade ou processo através da mudança na forma de sua ocorrência;**

**e) compara o risco estimado com critérios de risco predefinidos para determinar a sua importância.**

Comentários:

Segundo a ABNT NBR ISO/IEC 27005:

**3 Termos e definições**

*3.8 retenção do risco: aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco*

Cabe ressaltar que essa é uma característica dos Riscos de Segurança da Informação. Diferente dos Riscos Corporativos e de Projetos, aqui sempre o foco é negativo, e não nas oportunidades.

Gabarito Oficial: C

**6. (AOCP/TCE-PA 2012) A norma técnica NBR 27005 trata**

**a) da gestão de riscos de segurança da Informação.**

**b) das normas do código de práticas para a gestão da Tecnologia de Informação.**

**c) dos requisitos de sistemas de gestão de segurança da informação.**

**d) da especificação do gerenciamento de serviços.**

**e) do código de prática do gerenciamento de serviços.**

Comentário:

Esta é a famosa questão “Melzinho na Chupeta”. Como temos poucas questões de outras bancas sobre GSI, resolvi mantê-la.

*Introdução*

*Esta Norma fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001.*

Gabarito Oficial: A

**7. (FEPESE/MPE-SC 2014) Assinale a alternativa que apresenta corretamente as etapas do processo de Gestão de Riscos de acordo com a NBR ISO/IEC 27005.**

***A Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco; Comunicação do risco; e Monitoramento e análise crítica de riscos.***

***B Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco e Comunicação do risco.***

***C Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Contenção do risco; Aceitação do risco; Comunicação do risco***

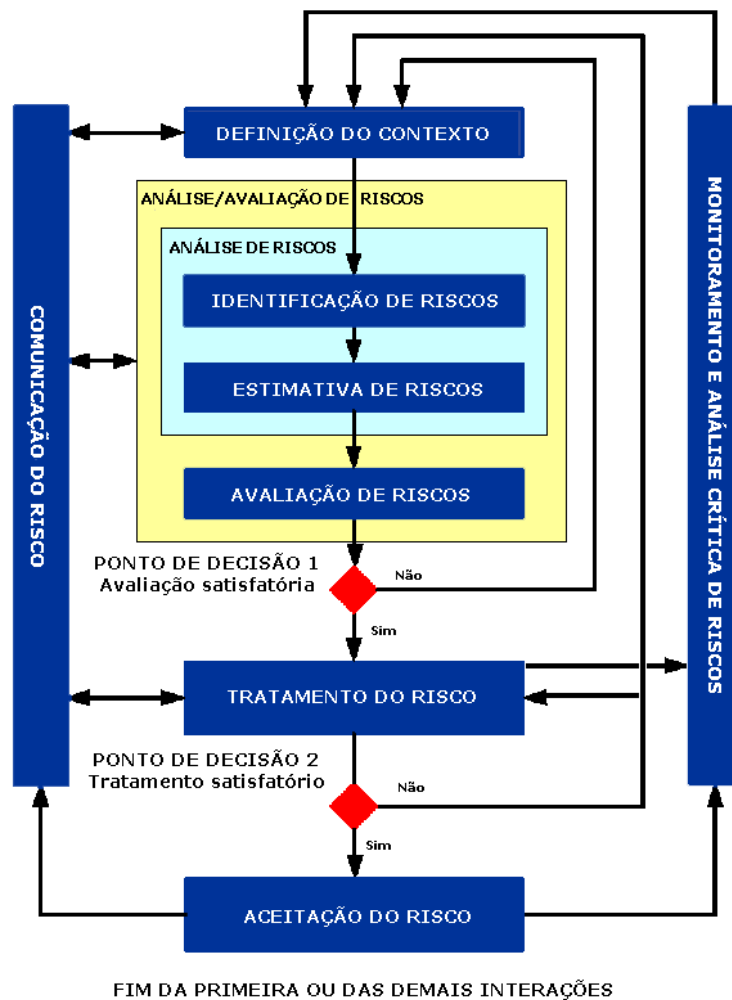
***D Definição de contexto; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco; Comunicação do risco; e Monitoramento e análise crítica de riscos.***

***E Definição de contexto; Análise de riscos; Eliminação/Aceitação do risco; Monitoramento de riscos.***

Comentários:

A uma altura dessas você deve saber responder a esse tipo de questão com o pé nas costas.

Recapitulando o frame da Norma:



Gabarito Oficial: D

8. (FEPESE/MPE-SC 2014) Com relação à Gestão da Segurança da Informação, assinale a alternativa que indica a norma especificamente destinada a fornecer orientação para o gerenciamento de risco da segurança da informação.

- A ISO/IEC 27001
- B ISO/IEC 27002
- C ISO/IEC 27005
- D ISO/IEC 27006
- E ISO/IEC 27010

Comentários:

Mais uma Questão imediata:

*Introdução*

*Esta Norma fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001.*

Gabarito Oficial: C

- 9. (VUNESP/TCE-SP 2014) A norma NBR ISO/IEC 27005:2011 estabelece a correspondência entre processos de um Sistema de Gestão de Segurança da Informação (SGSI) e processos de gestão de riscos da segurança da informação. Assinale a alternativa que contém uma correspondência correta entre os dois tipos de processos.**

**A Agir – implementação do plano de tratamento de risco.**

**B Executar – aceitação do risco.**

**C Executar – análise/avaliação de riscos.**

**D Planejar – plano de tratamento de risco.**

**E Verificar – definição do contexto.**

Comentários:

Relembrando...

*Guarde essa comparação entre os processos do GRSI e do SGSI e não erre mais:*

*Processos de GRSI x SGSI*

- Definição do contexto. (Planejar)*
- Avaliação de riscos. (Planejar)*
- Definição do plano de tratamento do risco. (Planejar)*
- Aceitação do risco. (Planejar)*
- Implementação do plano de tratamento do risco. (Executar)*
- Monitoramento contínuo e análise crítica de riscos. (Verificar)*
- Manter e melhorar o processo de GRSI. (Agir)*

Gabarito Oficial: D

Galerinha, então é isso! Revisamos praticamente TODAS as questões de 27.005 dos últimos tempos, agora é só chegar na prova e gabaritar.

Espero vocês no próximo curso!

Bons Estudos!

WC

**Enunciado das Questões Abordadas na Aula 4: Outras Bancas (27.005)**

**1. (FGV/FIOCRUZ 2010) Com relação à análise de risco em segurança da informação, considere os tipos de risco a seguir.**

***I. Dano físico, como fogo, vandalismo e desastres naturais.***

***II. Perda de dados, seja intencional ou não.***

***III. Falha de equipamento.***

***IV. Risco de mercado e perda de investimento.***

***Assinale:***

***a) se uma empresa deve estar atenta, em sua análise, somente aos riscos I, II e III.***

***b) se uma empresa deve estar atenta, em sua análise, a todos esses tipos de riscos.***

***c) se uma empresa deve estar atenta, em sua análise, somente aos riscos I e II.***

***d) se uma empresa deve estar atenta, em sua análise, somente aos riscos II e III.***

***e) se uma empresa deve estar atenta, em sua análise, somente aos riscos I e IV.***

**2. (CONSULPLAN/TRT-2 2017) A Norma Brasileira ABNT NBR ISO/IEC 27005:2011 é responsável pela Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de Segurança da Informação, fornecendo diretrizes para o processo de gestão de riscos de segurança da informação, de acordo com os padrões do Sistema de Gestão de Segurança da Informação (SGSI). Os gestores, além do pessoal envolvido com a gestão de riscos de segurança da informação em uma organização, são as pessoas que têm maior interesse nesta norma, ou também entidades externas que dão suporte a essas atividades. Esta norma apresenta diversas atividades que possuem: Entrada; Ação; Diretrizes para implementação; e, Saída. “Trata-se da comunicação que é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas.” A afirmativa anterior trata-se de:**

- a) *Avaliação do risco.*
  - b) *Percepção do risco.*
  - c) *Comunicação do risco.*
  - d) *Monitoramento do risco.*
3. (VUNESP/SAEG 2015) A norma NBR ISO/IEC 27005 apresenta 4 opções para o tratamento de riscos relacionados à segurança da informação. Uma dessas opções é
- a) *Retenção do Risco.*
  - b) *Transição do Risco.*
  - c) *Serialização do Risco.*
  - d) *Congelamento do Risco.*
  - e) *Empacotamento do Risco.*
4. (FEMERJ/TCE-RJ 2012) A gestão de riscos envolve diversas atividades. Segundo a norma ISO 27005, faz parte da atividade chamada análise/ avaliação de riscos:
- a) *a definição de contexto;*
  - b) *a estimativa de riscos;*
  - c) *o tratamento do risco;*
  - d) *a comunicação do risco;*
  - e) *a aceitação do risco.*
5. (FEMERJ/TCE-RJ 2012) De acordo com a norma ISO 27005, a retenção de riscos:
- a) *analisa apenas atos intencionais que possam produzir violações de segurança;*
  - b) *trata apenas fragilidades em ativos de informação, as chamadas ameaças;*
  - c) *considera somente consequências negativas (perdas);*



**d) procura eliminar uma atividade ou processo através da mudança na forma de sua ocorrência;**

**e) compara o risco estimado com critérios de risco predefinidos para determinar a sua importância.**

**6. (AOCP/TCE-PA 2012) A norma técnica NBR 27005 trata**

**a) da gestão de riscos de segurança da Informação.**

**b) das normas do código de práticas para a gestão da Tecnologia de Informação.**

**c) dos requisitos de sistemas de gestão de segurança da informação.**

**d) da especificação do gerenciamento de serviços.**

**e) do código de prática do gerenciamento de serviços.**

**7. (FEPESE/MPE-SC 2014) Assinale a alternativa que apresenta corretamente as etapas do processo de Gestão de Riscos de acordo com a NBR ISO/IEC 27005.**

**A Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco; Comunicação do risco; e Monitoramento e análise crítica de riscos.**

**B Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco e Comunicação do risco.**

**C Identificação de Risco; Análise/avaliação de riscos; Tratamento do risco; Contenção do risco; Aceitação do risco; Comunicação do risco**

**D Definição de contexto; Análise/avaliação de riscos; Tratamento do risco; Aceitação do risco; Comunicação do risco; e Monitoramento e análise crítica de riscos.**

**E Definição de contexto; Análise de riscos; Eliminação/Aceitação do risco; Monitoramento de riscos.**

**8. (FEPESE/MPE-SC 2014) Com relação à Gestão da Segurança da Informação, assinale a alternativa que indica a norma especificamente destinada a fornecer orientação para o gerenciamento de risco da segurança da informação.**

**A ISO/IEC 27001**

**B ISO/IEC 27002**

**C ISO/IEC 27005**

**D ISO/IEC 27006**

**E ISO/IEC 27010**

- 9. (VUNESP/TCE-SP 2014) A norma NBR ISO/IEC 27005:2011 estabelece a correspondência entre processos de um Sistema de Gestão de Segurança da Informação (SGSI) e processos de gestão de riscos da segurança da informação. Assinale a alternativa que contém uma correspondência correta entre os dois tipos de processos.**

**A Agir – implementação do plano de tratamento de risco.**

**B Executar – aceitação do risco.**

**C Executar – análise/avaliação de riscos.**

**D Planejar – plano de tratamento de risco.**

**E Verificar – definição do contexto.**

**Gabarito das Questões Abordadas na Aula 4: Outras Bancas (27.005)**

1. *(FGV/FIOCRUZ 2010) Gabarito Oficial: A*
2. *(CONSULPLAN/TRT-2 2017) Gabarito Oficial: C*
3. *(VUNESP/SAEG 2015) Gabarito Oficial: A*
4. *(FEMERJ/TCE-RJ 2012) Gabarito Oficial: B*
5. *(FEMERJ/TCE-RJ 2012) Gabarito Oficial: C*
6. *(AOCP/TCE-PA 2012) Gabarito Oficial: A*
7. *(FEPESE/MPE-SC 2014) Gabarito Oficial: D*
8. *(FEPESE/MPE-SC 2014) Gabarito Oficial: C*
9. *(VUNESP/TCE-SP 2014) Gabarito Oficial: D*