# Legislação de GSI (Multibancas)
# Questões Atualização 2020

Prof. Walter Cunha

falecomigo@waltercunha.com

gabaritou <TI>

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

# [ Professor ]

Natural: Fortaleza – CE

Cargo: AFFC-CGU TI (2009)

Graduação: Engenharia Eletrônica
ITA 2000

Pós: Ger. Projetos FGV 2007

Emerging Leaders: Harvard
Kennedy School Nov/2018

# [ Professor ]

**Outros Cursos no Provas de TI:**
http://bit.ly/2RsnuhF

**TImasters:**
https://br.groups.yahoo.com/neo/groups/timasters/info

**Outros:**
https://about.me/waltercunha

# [ Questão 01]

(CESPE/ABIN 2010) Acerca da Política de Segurança da Informação (PSI) nos órgãos e entidades da administração pública federal, instituída pelo Decreto n.º 3.505/2000, julgue o seguinte item.

Os membros do Comitê Gestor da Segurança da Informação só podem participar de processos, no âmbito da segurança da informação, de iniciativa do setor privado, caso essa participação seja julgada imprescindível para atender aos interesses da defesa nacional, a critério do Comitê Gestor e após aprovação do Gabinete de Segurança Institucional da Presidência da República.

# [ Questão 01] – Comentários...

Artigo 7º, §2º do Decreto 3505/00, a seguir:

*"Art. 7o  O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados:*
*(...)*
*§ 2o  Os membros do Comitê Gestor não poderão participar de processos similares (no âmbito da segurança da informação) de iniciativa do setor privado, exceto nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República"*

# [ Questão 01]

(CESPE/ABIN 2010) Acerca da Política de Segurança da Informação (PSI) nos órgãos e entidades da administração pública federal, instituída pelo Decreto n.º 3.505/2000, julgue o seguinte item.

Os membros do Comitê Gestor da Segurança da Informação só podem participar de processos, no âmbito da segurança da informação, de iniciativa do setor privado, caso essa participação seja julgada imprescindível para atender aos interesses da defesa nacional, a critério do Comitê Gestor e após aprovação do Gabinete de Segurança Institucional da Presidência da República. (CERTA)

# [ Questão 02]

(CESPE/MEC 2015) Julgue o próximo item, que tratam da Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (IN-GSIPR) n.º 1/2009 e de normas complementares (NC), estabelecidas na mesma norma IN.

A criação de equipes de tratamento e respostas a incidentes em redes computacionais nos órgãos e nas entidades da administração pública federal figura em norma complementar.

# [ Questão 02] – Comentários...

*A Norma Complementar a qual a questão faz referência é a NC05.*

***Norma Complementar nº 05/IN01/DSIC/GSIPR**, e seu Anexo, **disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR** nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1)*

*Já os serviços prestados pelos CSIRTs definidos NC05 por meio do gerenciamento de incidentes constam na NC08.*

***Norma Complementar nº 08/IN01/DSIC/GSIPR, estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais** nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1)*

# [ Questão 02]

(CESPE/MEC 2015) Julgue o próximo item, que tratam da Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (IN-GSIPR) n.º 1/2009 e de normas complementares (NC), estabelecidas na mesma norma IN.

A criação de equipes de tratamento e respostas a incidentes em redes computacionais nos órgãos e nas entidades da administração pública federal figura em norma complementar. (CERTA)

# [ Questão 03]

(CESPE/PF 2014) A elaboração de uma política de segurança institucional deve refletir, sobretudo, o know-how de segurança dos profissionais envolvidos com a sua elaboração e não a cultura da organização.

# [ Questão 03] – Comentários...

*Para que a cultura da empresa seja mudada em relação à segurança da informação, é fundamental que os funcionários estejam preparados para a mudança, por meio de avisos, palestras de conscientização, elaboração de guias rápidos de consulta e treinamento direcionado. (FREITAS E ARAUJO, 2008, P. 47).*

*A política deve ser escrita de forma clara, não gerando qualquer dúvida entre os usuários. Todos os funcionários da organização, incluindo aqueles que são terciários e prestadores de serviço, deverão receber um treinamento adequado para que se adequem às mudanças. De acordo com a NBR ISO IEC 27002 (2005), os usuários devem estar clientes das ameaças e das vulnerabilidades de segurança da informação e estejam equipados para apoiar a política de segurança da informação da organização durante a execução normal do trabalho.*

# [ Questão 03]

(CESPE/PF 2014) A elaboração de uma política de segurança institucional deve refletir, sobretudo, o know-how de segurança dos profissionais envolvidos com a sua elaboração e não a cultura da organização. (ERRADA)

# [ Questão 04]

(ESAF/ESAF 2015) A Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008, que “Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal...”, estabelece as competências de diversos órgãos e entidades da Administração Pública Federal. O planejamento e a coordenação das atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, competem ao

A Comitê Gestor de Segurança da Informação.

B Gabinete de Segurança Institucional da Presidência da República – GSI.

C Ministério da Ciência e Tecnologia.

D Ministério da Defesa.

E Serviço Federal de Processamento de Dados – Serpro.

# [ Questão 04] – Comentários...

*IN GSI/PR n. 1/2008:*

*"Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:*

*I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;*

# [ Questão 04]

(ESAF/ESAF 2015) A Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008, que “Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal...”, estabelece as competências de diversos órgãos e entidades da Administração Pública Federal. O planejamento e a coordenação das atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, competem ao

A Comitê Gestor de Segurança da Informação.

***B Gabinete de Segurança Institucional da Presidência da República – GSI.***

C Ministério da Ciência e Tecnologia.

D Ministério da Defesa.

E Serviço Federal de Processamento de Dados – Serpro.

# [ Questão 05]

(CESGRANRIO/CHESF 2012) A autoridade Certificadora Raiz da ICP–Brasil é o

A Instituto Brasileiro de Segurança da Informação
B Instituto Nacional de Tecnologia da Informação
C Instituto Nacional de Pesos e Medidas
D Instituto Nacional de Metrologia, Normalização e Qualidade Industrial
E Gabinete de Segurança Institucional

# [ Questão 05] – Comentários...

*ICP, ou Infra-estrutura de Chaves Públicas, é a sigla no Brasil para PKI - Public Key Infrastructure -, um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais.*

*Desde julho de 2001, o Comitê Gestor da ICP-Brasil estabelece a política, os critérios e as normas para licenciamento de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da cadeia de certificação, credenciando as respectivas empresas na emissão de certificados no meio digital brasileiro. O ITI O Instituto Nacional de Tecnologia da Informação (ITI) é a Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil.*

# [ Questão 05]

(CESGRANRIO/CHESF 2012) A autoridade Certificadora Raiz da ICP–Brasil é o

A Instituto Brasileiro de Segurança da Informação

***B Instituto Nacional de Tecnologia da Informação***

C Instituto Nacional de Pesos e Medidas

D Instituto Nacional de Metrologia, Normalização e Qualidade Industrial

E Gabinete de Segurança Institucional

# [ Questão 06]

(ESAF/ESAF 2015) ADAP Em termos das questões relacionadas à política de segurança e auditoria é correto afirmar que

(...)

o Decreto n. 3.505, de 13.06.2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, tem como um de seus pressupostos garantir ao Estado o direito de acesso a qualquer informação que for de seu interesse.

# [ Questão 06] – Comentários...

*Exemplo de Limite:*

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

# [ Questão 06]

(ESAF/ESAF 2015) ADAP Em termos das questões relacionadas à política de segurança e auditoria é correto afirmar que

(...)

o Decreto n. 3.505, de 13.06.2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, tem como um de seus pressupostos garantir ao Estado o direito de acesso a qualquer informação que for de seu interesse (ERRADA).

# [ Questão 07]

(CESPE/MEC 2015) De acordo com a IN n.º 1/2009 do GSIPR, julgue o item que se segue.

O comitê de segurança da informação e comunicação deve propor normas relativas à segurança da informação, bem como alterações na Política de Segurança da Informação e Comunicação.

# [ Questão 07] – Comentários

*Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:*

*I - assessorar na implementação das ações de segurança da informação e comunicações;*

*II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;*

*III - propor alterações na Política de Segurança da Informação e Comunicações; e*

*IV - propor normas relativas à segurança da informação e comunicações.*

# [ Questão 07]

(CESPE/MEC 2015) De acordo com a IN n.º 1/2009 do GSIPR, julgue o item que se segue.

*O comitê de segurança da informação e comunicação deve propor normas relativas à segurança da informação, bem como alterações na Política de Segurança da Informação e Comunicação (CERTA).*

# [ Questão 08]

(CESPE/MEC 2015) De acordo com a IN GSIPR n.º 1, a atribuição de acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança em um órgão da administração pública federal é responsabilidade do Comitê de Segurança da Informação e Comunicações do órgão.

# [ Questão 08] – Comentários

*Art. 7º da Instrução Normativa GSI/PR nº 01 o Gestor de Segurança da Informação e Comunicações deve:*

- *promover cultura de Segurança da Informação e Comunicações;*
- *acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;*
- *propor recursos necessários às ações de Segurança da Informação e Comunicações;*
- *coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;*
- *realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicações;*
- *manter contato direto com o DSIC para o trato de assuntos relativos à Segurança da Informação e Comunicações.*

# [ Questão 08]

(CESPE/MEC 2015) *De acordo com a IN GSIPR n.º 1, a atribuição de acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança em um órgão da administração pública federal é responsabilidade do Comitê de Segurança da Informação e Comunicações do órgão. (CERTA)*

# [ Questão 09]

(CESPE/MEC 2015) A Norma Complementar 02/IN01/DSIC/GSIPR prevê que, na fase Planejar do Ciclo de Gestão de Segurança da Informação, a atividade de análise de riscos deverá identificar a probabilidade real de ocorrência de falhas de segurança; para isso devem-se considerar as vulnerabilidades prevalecentes, os impactos associados a esses ativos e, por fim, as ações de segurança da informação e comunicações atualmente implementadas em determinado órgão ou entidade.

# [ Questão 09] – Comentários

Segundo a Norma Complementar 02/IN01/DSIC/GSIPR

***3.1 ("Plan – P") Planejar*** *- É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações planejará as ações de segurança da informação e comunicações que serão implementadas, considerando os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade*

***3.1.5 Analisar os riscos, sendo necessário:***
*a) identificar os impactos para a missão do órgão ou entidade que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de disponibilidade, integridade, confidencialidade ou autenticidade destes ativos;*

*b) identificar a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados a estes ativos e as ações de segurança da informação e comunicações atualmente implementadas no órgão ou entidade;*

# [ Questão 09]

(CESPE/MEC 2015) A Norma Complementar 02/IN01/DSIC/GSIPR prevê que, na fase Planejar do Ciclo de Gestão de Segurança da Informação, a atividade de análise de riscos deverá identificar a probabilidade real de ocorrência de falhas de segurança; para isso devem-se considerar as vulnerabilidades prevalecentes, os impactos associados a esses ativos e, por fim, as ações de segurança da informação e comunicações atualmente implementadas em determinado órgão ou entidade. (CERTA)

# [ Questão 10]

(CESPE/MEC 2015) De acordo com a Norma Complementar 08/IN01/DSIC/GSIPR, a prospecção ou a monitoração de novas tecnologias e o desenvolvimento de ferramentas de segurança são serviços adicionais que uma ETIR poderá oferecer à sua comunidade.

# [ Questão 10] – Comentários

**Norma Complementar 08/IN01/DSIC/GSIPR**

*7.2 Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores:*

*7.2.1 Tratamento de artefatos maliciosos;*

*7.2.2 Tratamento de vulnerabilidades;*

*7.2.3 Emissão de alertas e advertências;*

*7.2.4 Anúncios;*

*7.2.5 Prospecção ou monitoração de novas tecnologias;*

*7.2.6 Avaliação de segurança;*

*7.2.7 Desenvolvimento de ferramentas de segurança;*

*]7.2.8 Detecção de intrusão;*

*7.2.9 Disseminação de informações relacionadas à segurança;*

# [ Questão 10]

(CESPE/MEC 2015) De acordo com a Norma Complementar 08/IN01/DSIC/GSIPR, a prospecção ou a monitoração de novas tecnologias e o desenvolvimento de ferramentas de segurança são serviços adicionais que uma ETIR poderá oferecer à sua comunidade. (CERTA)

# [ Questão 11]

(CESPE/TJSE 2014) No que se refere à equipe de resposta e tratamento a incidentes (ETIR) e aos incidentes de segurança, julgue os itens que se seguem.

Entre os modelos de formação do time de resposta a incidentes previstos pela ISACA, Central, Distributed, Coordinating e Outsourced, apenas o último não foi incorporado ao regramento do DSIC (NC 05/IN01/DSIC/GSIPR) para a administração pública, haja vista que, no âmbito dessa administração, a escolha preferencial, na formação da equipe, deve recair sobre servidor público ocupante de cargo efetivo ou militares de carreira.

# [ Questão 11] – Comentários

**NC 05/IN01/DSIC/GSIPR**

*10.2 Preferencialmente a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos.*

# [ Questão 11]

(CESPE/TJSE 2014) No que se refere à equipe de resposta e tratamento a incidentes (ETIR) e aos incidentes de segurança, julgue os itens que se seguem.

Entre os modelos de formação do time de resposta a incidentes previstos pela ISACA, Central, Distributed, Coordinating e Outsourced, apenas o último não foi incorporado ao regramento do DSIC (NC 05/IN01/DSIC/GSIPR) para a administração pública, haja vista que, no âmbito dessa administração, a escolha preferencial, na formação da equipe, deve recair sobre servidor público ocupante de cargo efetivo ou militares de carreira

. (CERTA)

# [ Questão 12]

(CESPE/TJSE 2014) As diretrizes do trabalho da ETIR e o planejamento da estratégia de resposta a incidentes devem ser traçados pelo agente responsável e pelos membros da equipe, sem o envolvimento do gestor de segurança da informação, que tem a função de atuar como analista de conformidade do processo.

# [ Questão 12] – Comentários

**NC 05/IN01/DSIC/GSIPR**

*5 RESPONSABILIDADE*

***Os Gestores de Segurança da Informação e Comunicações são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais**, nos órgãos e entidades da Administração Pública Federal, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.*

# [ Questão 12]

(CESPE/TJSE 2014) As diretrizes do trabalho da ETIR e o planejamento da estratégia de resposta a incidentes devem ser traçados pelo agente responsável e pelos membros da equipe, sem o envolvimento do gestor de segurança da informação, que tem a função de atuar como analista de conformidade do processo. (ERRADA)

# [ Questão 13]

(ESAF/MF 2013) Segundo a Norma Complementar n. 08/IN01/DSIC/ GSIPR, durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar n. 05/IN01/DSIC/GSIPR:

A manter as operações do ambiente de TI.

B disponibilizar os recursos materiais, tecnológicos e humanos para tratar o incidente.

C informar a alta administração do incidente.

D contratar capacitação para evitar a repetição do incidente.

E acionar as autoridades policiais competentes para a adoção dos procedimentos legais necessários.

# [ Questão 13] – Comentários

**NC 08/IN01/DSIC/GSIPR**

*8.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar no 05/IN01/DSIC/GSIPR:*

*8.5.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;*

*8.5.2 Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;*

*8.5.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 8.5.2.*

# [ Questão 13]

(ESAF/MF 2013) Segundo a Norma Complementar n. 08/IN01/DSIC/ GSIPR, durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar n. 05/IN01/DSIC/GSIPR:

A manter as operações do ambiente de TI.

B disponibilizar os recursos materiais, tecnológicos e humanos para tratar o incidente.

C informar a alta administração do incidente.

D contratar capacitação para evitar a repetição do incidente.

*E acionar as autoridades policiais competentes para a adoção dos procedimentos legais necessários.*

# [ Questão 14]

(CESPE/ABIN 2010) Acerca da Política de Segurança da Informação (PSI) nos órgãos e entidades da administração pública federal, instituída pelo Decreto n.º 3.505/2000, julgue o seguinte item.

Entre os objetivos da PSI, insere-se o estímulo à participação competitiva do setor produtivo no mercado de bens e de serviços relacionados com a segurança da informação, incluindo-se a fabricação de produtos que incorporem recursos criptográficos.

# [ Questão 14] – Comentários

**Decreto n.º 3.505/2000**

*"Art. 3o  São objetivos da Política da Informação:*
*(...)*
*VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação"*

# [ Questão 14]

(CESPE/ABIN 2010) Acerca da Política de Segurança da Informação (PSI) nos órgãos e entidades da administração pública federal, instituída pelo Decreto n.º 3.505/2000, julgue o seguinte item.

Entre os objetivos da PSI, insere-se o estímulo à participação competitiva do setor produtivo no mercado de bens e de serviços relacionados com a segurança da informação, incluindo-se a fabricação de produtos que incorporem recursos criptográficos. (CERTA)

# [ Questão 15]

(CESPE/BACEN 2013) Julgue os itens subsecutivos, com base no disposto na Lei n.º 12.527/2011.

O órgão público não pode exigir do particular que ele apresente os motivos determinantes da solicitação de informações de interesse público por ele realizada.

# [ Questão 15] – Comentários

**Lei nº 12.527/2011**

*Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.*
*(...)*
*§ 3o São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público.*

# [ Questão 15]

(CESPE/BACEN 2013) Julgue os itens subsecutivos, com base no disposto na Lei n.º 12.527/2011.

O órgão público não pode exigir do particular que ele apresente os motivos determinantes da solicitação de informações de interesse público por ele realizada.(CERTA)

# [ Questão 16]

(CESPE/BACEN 2013) Julgue os itens subsecutivos, com base no disposto na Lei n.º 12.527/2011.

Sendo pessoas jurídicas de direito privado, as empresas públicas não estão sujeitas às regras previstas na referida lei.

# [ Questão 16] – Comentários

**Lei n.º 12.527/2011**

*Parágrafo único. Subordinam-se ao regime desta Lei:*

*I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;*

*II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.*

# [ Questão 16]

(CESPE/BACEN 2013) Julgue os itens subsecutivos, com base no disposto na Lei n.º 12.527/2011.

Sendo pessoas jurídicas de direito privado, *as empresas públicas não estão sujeitas às regras previstas na referida lei*.

# [ Questão 17]

(CETRO/ANVISA 2013) Em relação ao Decreto nº 7.724/2012, a pessoa natural ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o Poder Público e agir com dolo ou má-fé na análise dos pedidos de acesso à informação estará sujeita, entre outras sanções, à .

A advertência.

B notificação.

C suspensão de 6 (seis) meses.

D demissão

E exoneração

# [ Questão 17] – Comentários

**Decreto nº 7.724/2012**

*Art. 66. A pessoa natural ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o Poder Público e praticar conduta prevista no art. 65, estará sujeita às seguintes sanções:*
*I - advertência;*
*II - multa;*
*III - rescisão do vínculo com o Poder Público;*
*IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a dois anos; e*
*V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade.*

# [ Questão 17]

(CETRO/ANVISA 2013) Em relação ao Decreto nº 7.724/2012, a pessoa natural ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o Poder Público e agir com dolo ou má-fé na análise dos pedidos de acesso à informação estará sujeita, entre outras sanções, à .

*A advertência.*

B notificação.

C suspensão de 6 (seis) meses.

D demissão

E exoneração

# [ Questão 18]

(CETRO/ANVISA 2013) A gestão de processos de TI, incluindo a gestão de segurança da informação, não pode ser objeto de contratação.

# [ Questão 18] – Comentários

***IN4/2014***

*Art. 5º Não poderão ser objeto de contratação:*

*I - mais de uma Solução de Tecnologia da Informação em um único contrato; e*

*II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação.*

# [ Questão 18]

(CETRO/ANVISA 2013) A gestão de processos de TI, incluindo a gestão de segurança da informação, não pode ser objeto de contratação. (CERTA)

# [ Questão 19]

(CESPE/ANAC 2012) Acerca das normas do Gabinete de Segurança Institucional (GSIPR), julgue os próximos itens.

Em conformidade com a Norma Complementar n.º 04/IN01/DSIC/GSIPR, cabe ao diretor de tecnologia da informação dos órgãos da administração pública federal direta e indireta aprovar as diretrizes gerais e o processo de gestão de riscos de segurança da informação e comunicações, observada a respectiva política de segurança da informação e comunicações.

# [ Questão 19] – Comentários

**04/IN01/DSIC/GSI/PR**

*7.1 Cabe à Alta Administração do órgão ou entidade da APF, direta e indireta, aprovar as diretrizes gerais e o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC observada, dentre outras, a respectiva Política de Segurança da Informação e Comunicações;*

# [ Questão 19]

(CESPE/ANAC 2012) Acerca das normas do Gabinete de Segurança Institucional (GSIPR), julgue os próximos itens.

Em conformidade com a Norma Complementar n.º 04/IN01/DSIC/GSIPR, cabe ao diretor de tecnologia da informação dos órgãos da administração pública federal direta e indireta aprovar as diretrizes gerais e o processo de gestão de riscos de segurança da informação e comunicações, observada a respectiva política de segurança da informação e comunicações. (ERRADA)

# [ Questão 20]

(ESAF/MF 2013) Segundo a Norma Complementar n. 04/IN01/DSIC/GSIPR, na fase de análise/avaliação dos riscos, deve-se identificar os riscos associados ao escopo definido, considerando:

A as ameaças envolvidas, as vulnerabilidades existentes nos ativos de informação e as ações de Segurança da Informação e Comunicações já adotadas.

B as ameaças bloqueadas, as vulnerabilidades ainda existentes nos ativos de informação e a Política de Segurança da Informação e Comunicações.

C as ameaças envolvidas, as vulnerabilidades sanadas nos ativos de informação e o histórico de incidentes de Segurança da Informação e Comunicações.

D as ameaças mais críticas, as vulnerabilidades Web existentes nos ativos de informação e os controles de Segurança da Informação e Comunicações já adotados.

E as ameaças na DMZ, as vulnerabilidades Web existentes e os controles contra malware implantados.

# [ Questão 20] – Comentários

**04/IN01/DSIC/GSIPR**

*6.2 Análise/avaliação dos riscos: nesta fase, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados.*

*6.2.2 Identificar os riscos associados ao escopo definido, considerando:*
a) as ameaças envolvidas;
b) as vulnerabilidades existentes nos ativos de informação; e
c) as ações de Segurança da Informação e Comunicações – SIC já adotadas.

# [ Questão 20]

(ESAF/MF 2013) Segundo a Norma Complementar n. 04/IN01/DSIC/GSIPR, na fase de análise/avaliação dos riscos, deve-se identificar os riscos associados ao escopo definido, considerando:

*A as ameaças envolvidas, as vulnerabilidades existentes nos ativos de informação e as ações de Segurança da Informação e Comunicações já adotadas.*

B as ameaças bloqueadas, as vulnerabilidades ainda existentes nos ativos de informação e a Política de Segurança da Informação e Comunicações.

C as ameaças envolvidas, as vulnerabilidades sanadas nos ativos de informação e o histórico de incidentes de Segurança da Informação e Comunicações.

D as ameaças mais críticas, as vulnerabilidades Web existentes nos ativos de informação e os controles de Segurança da Informação e Comunicações já adotados.

E as ameaças na DMZ, as vulnerabilidades Web existentes e os controles contra malware implantados.

# [ Questão 21]

(ESAF/MF 2013) *Segundo a Norma Complementar n. 04/IN01/DSIC/ GSIPR, a Gestão de Riscos de Segurança da Informação e Comunicações deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e o(a):*

*A Plano Estratégico de TI.*

*B Plano de Risco de Negócios.*

*C Gestão de Respostas a Incidentes.*

*D Plano Tático de Segurança da Informação.*

*E Gestão de Continuidade de Negócios.*

# [ Questão 21] – Comentários

**04/IN01/DSIC/GSIPR**

*4 PRINCÍPIOS E DIRETRIZES*

*4.4 A Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócio.*

# [ Questão 21]

(ESAF/MF 2013) *Segundo a Norma Complementar n. 04/IN01/DSIC/ GSIPR, a Gestão de Riscos de Segurança da Informação e Comunicações deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e o(a):*

*A Plano Estratégico de TI.*

*B Plano de Risco de Negócios.*

*C Gestão de Respostas a Incidentes.*

*D Plano Tático de Segurança da Informação.*

*E Gestão de Continuidade de Negócios.*

# [ Questão 22]

(ESAF/MF 2013) Segundo a Norma Complementar n. 03/IN01/DSIC/GSIPR, na elaboração da Política de Segurança da Informação e Comunicações, recomenda-se estabelecer diretrizes sobre o tema:

a) Proteção da DMZ.

b) Backup e restauração.

c) Uso de email.

d) Balanceamento de carga.

e) Acesso à Intranet

# [ Questão 22] – Comentários

**03/IN01/DSIC/GSIPR**

*5.3 Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens:*
*5.3.5 Diretrizes Gerais: neste item recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as Normas específicas vigentes no ordenamento jurídico:*
*a) Tratamento da Informação;*
*b) Tratamento de Incidentes de Rede;*
*c) Gestão de Risco;*
*d) Gestão de Continuidade;*
*e) Auditoria e Conformidade;*
*f) Controles de Acesso;*
*g) Uso de e-mail; e*
*h) Acesso a Internet.*

# [ Questão 22]

(ESAF/MF 2013) Segundo a Norma Complementar n. 03/IN01/DSIC/GSIPR, na elaboração da Política de Segurança da Informação e Comunicações, recomenda-se estabelecer diretrizes sobre o tema:

a) Proteção da DMZ.

b) Backup e restauração.

***c) Uso de email.***

d) Balanceamento de carga.

e) Acesso à Intranet

# [ Questão 23]

(ESAF/MF 2013) *Segundo a Norma Complementar n. 03/IN01/DSIC/GSIPR, todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicações (POSIC), incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de:*

*A 6 meses.*

*B 1 ano.*

*C 2 anos.*

*D 3 anos.*

*E 4 anos.*

# [ Questão 23] – Comentários

**03/IN01/DSIC/GSIPR**

*8 ATUALIZAÇÃO DA POSIC*

*Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03(três) anos.*

# [ Questão 23]

(ESAF/MF 2013) *Segundo a Norma Complementar n. 03/IN01/DSIC/GSIPR, todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicações (POSIC), incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de:*

*A 6 meses.*

*B 1 ano.*

*C 2 anos.*

***D 3 anos.***

*E 4 anos.*

# [ Questão 24]

(CESPE/TCE-TO 2009) ADAP Assinale a opção correta, acerca da legislação relativa à segurança dos sistemas de informação.

(...)

A política de segurança da informação nos órgãos e entidades da administração pública, nos âmbitos federal, estadual e municipal, dos poderes Executivo, Legislativo e Judiciário, foi instituída por meio do Decreto n.º 3.505/2000.

# [ Questão 24] – Comentários

***DECRETO No 3.505, DE 13 DE JUNHO DE 2000, Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.***

# [ Questão 24]

(CESPE/TCE-TO 2009) ADAP Assinale a opção correta, acerca da legislação relativa à segurança dos sistemas de informação.

(...)

A política de segurança da informação nos órgãos e entidades da administração pública, nos âmbitos federal, ***estadual e municipal***, dos poderes Executivo, ***Legislativo e Judiciário***, foi instituída por meio do Decreto n.º 3.505/2000.

# [ Questão 25]

(CESGRANRIO/BNDES 2010) O Decreto nº 3.505, de 13/06/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, define, dentre as diretrizes a serem adotadas, o desenvolvimento do sistema de classificação de dados e informação, com vistas à garantia dos níveis de segurança desejados e à normatização

A do uso de chaves públicas.

B do acesso às informações.

C dos recursos criptográficos.

D dos graus de sigilo.

E da preservação dos documentos.

# [ Questão 25] – Comentários

**Decreto Federal nº 3.505**

*Art. 4o  Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6o, adotar as seguintes diretrizes:*

*XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;*

# [ Questão 25]

(CESGRANRIO/BNDES 2010) O Decreto nº 3.505, de 13/06/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, define, dentre as diretrizes a serem adotadas, o desenvolvimento do sistema de classificação de dados e informação, com vistas à garantia dos níveis de segurança desejados e à normatização

A do uso de chaves públicas.

***B do acesso às informações.***

C dos recursos criptográficos.

D dos graus de sigilo.

E da preservação dos documentos.

# [ Questão 26]

(CESGRANRIO/BNDES 2010) Para que a informação documental seja protegida, é necessário que as organizações implantem uma política de segurança, objetivando o gerenciamento da mesma. No âmbito dos órgãos e entidades da Administração Pública Federal foi instituída a Política de Segurança da Informação por meio do Decreto Federal nº 3.505, de 13 de junho de 2000. É parte dos objetivos dessa política:

A assegurar a interoperabilidade entre os sistemas de segurança da informação e ampliar a dependência externa em relação a sistemas e equipamentos.

B assegurar a interoperabilidade entre os sistemas de segurança da informação e ampliar a dependência externa em relação à segurança da informação.

C instrumentalizar a Administração Pública Federal para assegurar a indisponibilidade dos dados, com a promoção da capacitação de recursos humanos.

D capacitar recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação e estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação.

E promover o intercâmbio científico-tecnológico restrito aos órgãos e entidades da Administração Pública Federal, excluindo as instituições privadas, sobre as atividades de segurança da informação.

# [ Questão 26] – Comentários

**Decreto Federal nº 3.505**

*(...)*

*II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação*

*III* - promover a capacitação *de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação*

*VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;*

*(...)*

*VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação;*

# [ Questão 26]

(CESGRANRIO/BNDES 2010) Para que a informação documental seja protegida, é necessário que as organizações implantem uma política de segurança, objetivando o gerenciamento da mesma. No âmbito dos órgãos e entidades da Administração Pública Federal foi instituída a Política de Segurança da Informação por meio do Decreto Federal nº 3.505, de 13 de junho de 2000. É parte dos objetivos dessa política:

A assegurar a interoperabilidade entre os sistemas de segurança da informação e *ampliar a dependência externa em relação a sistemas e equipamentos*.

B assegurar a interoperabilidade entre os sistemas de segurança da informação e *ampliar a dependência externa em relação à segurança da informação.*

C instrumentalizar a Administração Pública Federal para *assegurar a indisponibilidade dos dados*, com a promoção da capacitação de recursos humanos.

***D capacitar recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação e estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação.***

E promover o intercâmbio científico-tecnológico *restrito aos órgãos e entidades da Administração Pública Federal, excluindo as instituições privadas, sobre as atividades de segurança da informação*.

# [ Questão 27]

(CESPE/ABIN 2010) De acordo com as normas da Secretaria Executiva do Conselho de Defesa Nacional, para o uso e a comercialização de recursos criptográficos pelas entidades e órgãos da administração pública federal, deve-se dar preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional.

# [ Questão 27] – Comentários

**Decreto Federal nº 3.505**

*Art. 4o Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6o, adotar as seguintes diretrizes:*
*(...)*
*IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;*

# [ Questão 27]

(CESPE/ABIN 2010) *De acordo com as normas da Secretaria Executiva do Conselho de Defesa Nacional, para o uso e a comercialização de recursos criptográficos pelas entidades e órgãos da administração pública federal, deve-se dar preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional.* (CERTA)

# [ Questão 28]

(IF SUL- MG/IF SUL- MG 2016 ADAP) A obediência ao regramento trazido pela IN 4/2014 é mandatória. E sim, existem previsões de contratações em que essa Instrução Normativa pode ser ignorada, conforme rol taxativo previsto na mesma. Contudo, não se verifica o enquadramento de tal situação quando:

(...)

Quando se tratar de contratação de Solução de Tecnologia da Informação que possa comprometer a segurança nacional. Caso seja este o caso, deverá ser observado o disposto no Decreto nº 8.135, de 4 de novembro de 2013, e suas regulamentações específicas.

# [ Questão 28] – Comentários

*§ 1º - Esta IN não se aplica:*

*III - às contratações de Soluções de Tecnologia da Informação que possam comprometer a segurança nacional, em que deverá ser observado o disposto no Decreto nº 8.135, de 4 de novembro de 2013, e suas regulamentações específicas.*

# [ Questão 28]

(IF SUL- MG/IF SUL- MG 2016 ADAP) A obediência ao regramento trazido pela IN 4/2014 é mandatória. E sim, existem previsões de contratações em que essa Instrução Normativa pode ser ignorada, conforme rol taxativo previsto na mesma. Contudo, não se verifica o enquadramento de tal situação quando:

(...)

Quando se tratar de contratação de Solução de Tecnologia da Informação que possa comprometer a segurança nacional. Caso seja este o caso, deverá ser observado o disposto no Decreto nº 8.135, de 4 de novembro de 2013, e suas regulamentações específicas. (CERTA, a IN PODE SER IGNORADA)

# [ Questão 29]

(CESPE/TELEBRÁS 2015) A respeito das comunicações de dados da administração pública federal, objeto do Decreto n.º 8.135/2013, julgue o item subsequente.

As comunicações da administração pública federal fundacional devem ser realizadas por serviços providos por órgãos ou entidades da própria administração, inclusive no que se refere ao serviço telefônico fixo comutado.

# [ Questão 29] – Comentários

**Decreto Federal nº 8.135/2013**

*Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.*

*§ 1º O disposto no caput não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.*

# [ Questão 29]

(CESPE/TELEBRÁS 2015) A respeito das comunicações de dados da administração pública federal, objeto do Decreto n.º 8.135/2013, julgue o item subsequente.

*As comunicações da administração pública federal fundacional devem ser realizadas por serviços providos por órgãos ou entidades da própria administração, inclusive no que se refere ao serviço telefônico fixo comutado*. (ERRADA)

# [ Questão 30]

(CESPE/TELEBRÁS 2015) A respeito das comunicações de dados da administração pública federal, objeto do Decreto n.º 8.135/2013, julgue o item subsequente.

A comunicação entre a presidência da República e a TELEBRAS deve ser realizada com equipamentos que permitam eventual auditoria para fins de garantia da confidencialidade e autenticidade das informações trocadas, entre outros propósitos.

# [ Questão 30] – Comentários

**Decreto Federal nº 8.135**

*Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.*

*(...)*

*§ 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.*

# [ Questão 30]

(CESPE/TELEBRÁS 2015) A respeito das comunicações de dados da administração pública federal, objeto do Decreto n.º 8.135/2013, julgue o item subsequente.

*A comunicação entre a presidência da República e a TELEBRAS deve ser realizada com equipamentos que permitam eventual auditoria para fins de garantia da confidencialidade e autenticidade das informações trocadas, entre outros propósitos.* (CERTA)

# [ Questão 31]

(FGV/TJ-RO 2015) Em relação à legislação em TI, aplicáveis às informações digitais, analise as afirmativas a seguir:

I. O Marco Civil da Internet procura regular o uso das informações digitais, definindo sanções penais a serem aplicadas em caso de abuso.

II. Em respostas às denúncias de espionagem dos EUA, o governo brasileiro publicou o Decreto nº 8135/2013, com o objetivo de proteger suas comunicações de dados.

III. O tempo mínimo de armazenamento de registros de acesso a aplicações na Internet, por provedores de aplicações de internet, está atualmente definido na legislação.

Está correto somente o que se afirma em:

A I; B II; C III; D I e II; E II e III.

# [ Questão 31]

(FGV/TJ-RO 2015) Em relação à legislação em TI, aplicáveis às informações digitais, analise as afirmativas a seguir:

I. O Marco Civil da Internet procura regular o uso das informações digitais, definindo sanções penais a serem aplicadas em caso de abuso.

II. ***Em respostas às denúncias de espionagem dos EUA, o governo brasileiro publicou o Decreto nº 8135/2013, com o objetivo de proteger suas comunicações de dados***.

III. ***O tempo mínimo de armazenamento de registros de acesso a aplicações na Internet, por provedores de aplicações de internet, está atualmente definido na legislação***.

Está correto somente o que se afirma em:

A I;  B II;  C III; D I e II; ***E II e III***.

# Dúvidas

Prof. Walter Cunha
falecomigo@waltercunha.com

https://www.patreon.com/timasters
https://www.facebook.com/walter.cunha.7
https://www.instagram.com/walter.cunha.7/
https://twitter.com/timasters
https://www.linkedin.com/in/walter-cunha-19a90721