mentoria zeroum

RESUMO COMPLETO CGU · P3 · AFFC TI, INFRAESTRUTURA DE TI

MODELOS E ARQUITETURA DE NUVEM

Computação em Nuvem, Virtualização e Automação · Tópico 1

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Sobre o seu exemplar

Este exemplar é seu. Ele sai com o seu nome e o seu CPF em todas as páginas, e é assim que eu mantenho o material fora dos grupos de rateio. É por isso que ele não tem senha nem bloqueio: imprima, destaque, anote à mão, leve para onde você estuda.

O Resumo Completo CGU é obra protegida pela Lei 9.610 de 1998, e a licença é individual, vinculada ao seu CPF. Ela não cobre revenda, rateio, nem publicação em grupo ou nuvem compartilhada.

Se você encontrar este arquivo circulando com o nome de outra pessoa, me avise em contato@mentoriazeroum.com.br.

Se encontrar um erro, use o botão abaixo. O relato chega direto a mim, com o nome deste resumo já preenchido, e cada correção que proceder entra na próxima versão do arquivo.

Reportar um erro

VERSÃO 1 · PRIMEIRA VERSÃO EM OUTUBRO DE 2026

Esta é a primeira versão do Resumo Completo CGU. Cada relato de erro é conferido na fonte e, quando procede, a correção sai numa versão nova deste arquivo, registrada abaixo.

ATUALIZAÇÕES DESTE RESUMO

- Nenhuma até agora. Quando houver correção, ela entra aqui, com a data e o que mudou.

Bons estudos.

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

RESUMO COMPLETO CGU · P3 · AFFC TI, INFRAESTRUTURA DE TI

Modelos e arquitetura de nuvem

Computação em Nuvem, Virtualização e Automação · Tópico 1. 1.1 IaaS, PaaS e SaaS. 1.2 Modelos de implantação e responsabilidade compartilhada. 1.3 Redes virtuais, integração com ambiente local, elasticidade, escalabilidade e portabilidade. 1.4 Dependência entre serviços e requisitos de segurança.

COMO ESTE MATERIAL ESTÁ ORGANIZADO

1. **O trecho do edital**, logo acima, e o **mapa do tópico**, com cada item do edital, a seção deste material que o cobre, o curso para aprofundar e a fonte oficial.
2. **O texto**, no recorte exato do edital, na ordem dos itens.
3. **Os exemplos comentados**, com a consulta, o código ou o cálculo e a leitura do resultado. **As citações literais**, conferidas no texto oficial, com o artigo ou a página de onde saíram.
4. **Os quadros Como o Cebraspe pode cobrar e Pontos importantes**, com as pegadinhas da banca no tema e o essencial do tópico.
5. **As caixas pretas do Estratégia**, com as páginas de cada aula sobre o assunto.
6. **As questões abertas**, com as respostas na página seguinte, e **as questões de certo ou errado**, com o gabarito comentado.
7. **A documentação oficial e as normas** do tópico, com os links.
8. **Os cadernos do TEC** do tópico, com os assuntos que cada um cobra.

SUMÁRIO

Mapa do tópico	4
1. O que é a nuvem e os modelos de serviço: IaaS, PaaS e SaaS	5
2. Modelos de implantação e responsabilidade compartilhada	9
3. Redes virtuais e integração com o ambiente local	12
4. Elasticidade, escalabilidade e portabilidade	15
5. Dependência entre serviços e requisitos de segurança	18
Questões abertas de fixação	21
Respostas das questões abertas	24
Questões de certo ou errado	25
Gabarito comentado	27
Documentação oficial, normas e fontes	29
Atividades sugeridas do curso e do TEC neste tópico	30

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Para situar este tópico: Este tópico trata do que é a nuvem e de como ela se organiza: os modelos de serviço e de implantação, quem responde por cada camada, a rede virtual e a ligação com o ambiente local, a elasticidade e a portabilidade, as dependências e os requisitos de segurança. As máquinas virtuais e os contêineres estão no tópico 2; o balanceamento, o serverless, as filas e a escolha entre operar e contratar, no tópico 3; a infraestrutura como código, no tópico 4; a migração, no tópico 5. Os protocolos da ligação entre nuvem e ambiente local (VPN IPsec, roteamento) são da matéria Redes, Sistemas e Plataformas de Dados, tópico 1; os custos, as cotas e o FinOps, da matéria Operação, Governança e Gestão de Serviços Digitais, tópico 2. Todos os preços dos exemplos são hipotéticos, só para mostrar a conta.

Mapa do tópico

Item do edital	Neste material	Curso para aprofundar	Fonte oficial
1.1 IaaS, PaaS e SaaS	Seção 1	Redes de Computadores e Segurança da Informação (Infraestrutura de TI), cap. 10: capítulo previsto para 01/11/2026. Enquanto isso: Sistemas Operacionais (Infraestrutura de TI), cap. 5, p. 5 a 7 (data center próprio, hospedagem e nuvem)	Portaria SGD/MGI 5.950/2023, art. 4º, II, e Anexo I, item 2.1, alíneas f, x, y, z, at e au; SGD, Guia Complementar de Segurança para Computação em Nuvem, p. 12 a 14; Portaria Normativa SE-CGU 223/2025, art. 2º; NIST SP 800-145
1.2 Modelos de implantação e responsabilidade compartilhada	Seção 2	Capítulo 10 previsto para 01/11/2026. A responsabilidade compartilhada: só neste material	IN GSI/PR 5/2021, arts. 3º, 11 e 16; Portaria 5.950/2023, Anexo I, itens 5.4 e 25; Guia Complementar de Segurança para Computação em Nuvem, p. 16 e 17
1.3 Redes virtuais e integração com ambiente local	Seção 3	Capítulo 10 previsto para 01/11/2026. Redes virtuais na nuvem: só neste material	Guia Complementar de Segurança para Computação em Nuvem, controle 12, p. 36 e 37; Portaria 5.950/2023, Anexo I, item 10.2, alínea h
1.3 Elasticidade, escalabilidade e portabilidade	Seção 4	Capítulo 10 previsto para 01/11/2026. Enquanto isso: Sistemas Operacionais (Infraestrutura de TI), cap. 5, p. 7 e 8 (escalabilidade vertical e horizontal)	Enap, curso O papel do DevOps na Transformação Digital dos Serviços Públicos (EVG), módulo 3, p. 14 e 15; Portaria 5.950/2023, Anexo I, item 8; Portaria SE-CGU 223/2025, art. 3º, § 6º; SGD, Boas práticas para minimizar o aprisionamento em nuvem
1.4 Dependência entre serviços e requisitos de segurança	Seção 5	Capítulo 10 previsto para 01/11/2026. Só neste material	IN GSI/PR 5/2021, arts. 13 a 20; SGD, relatório sobre aprisionamento em nuvem, p. 1; Portaria 5.950/2023, Anexo I, item 10.2

Páginas das fontes e dos cursos: as do PDF, como aparecem no leitor de PDF.

SÓ NESTE MATERIAL

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

O capítulo do Estratégia sobre computação em nuvem (Redes de Computadores e Segurança da Informação, capítulo 10) está previsto para 01/11/2026. Até lá, este material cobre o tópico inteiro; as caixas do Estratégia abaixo apontam só as páginas de outro curso que tratam de parte do assunto.

1 O que é a nuvem e os modelos de serviço: IaaS, PaaS e SaaS

Computação em nuvem é o modelo em que o órgão obtém processamento, armazenamento, rede e software como serviço, pela rede, quando precisa, e paga pelo que usa, em vez de comprar e operar o equipamento. A norma federal de contratação define o objeto assim:

CITAÇÃO LITERAL

"Serviços de computação em nuvem: disponibilização de grupo escalável e elástico de recursos físicos ou virtuais, compartilháveis, acessados via rede, com provisionamento via autoatendimento e administração sob demanda"

Portaria SGD/MGI 5.950/2023, art. 4º, II · abrir a fonte

A definição mais cobrada é a do NIST (SP 800-145): a nuvem tem **cinco características essenciais**, **três modelos de serviço** e **quatro modelos de implantação**. O guia de segurança em nuvem do Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital repete as características:

CITAÇÃO LITERAL

"A computação em nuvem possui características consideradas essenciais que incluem autoatendimento sob demanda, amplo acesso a serviços de rede, compartilhamento otimizado de recursos, elasticidade rápida e serviços mensuráveis"

SGD, Guia Complementar de Segurança da Informação para Computação em Nuvem, PPSI 2.0 (versão 1.1, 2025), item 3.2, p. 12 · abrir a fonte

Característica	O que significa
Autoatendimento sob demanda	O cliente provisiona recursos sozinho, por portal ou API, sem interação humana com o provedor
Amplo acesso pela rede	Os recursos são acessados pela rede, por mecanismos padronizados, de vários tipos de dispositivo
Agrupamento de recursos (resource pooling)	O provedor atende vários clientes com os mesmos recursos físicos (multilocação), alocando-os dinamicamente; o cliente não controla a localização exata, mas pode escolher região ou país
Elasticidade rápida	Os recursos crescem e diminuem com a demanda, às vezes automaticamente, e parecem ilimitados ao cliente (seção 4)
Serviço medido	O uso é medido por unidade (hora de processamento, gigabyte, requisição) e cobrado, com transparência para o cliente e o provedor

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

A virtualização é a tecnologia que torna o agrupamento de recursos possível, mas não está entre as cinco características. Hospedagem (hosting) e co-location não são nuvem: na hospedagem o cliente aluga recursos de um data center de terceiros sem compartilhamento entre clientes; no co-location aluga a infraestrutura do data center de terceiros para hospedar os próprios equipamentos (Portaria 5.950/2023, Anexo I, item 2.1, alíneas e e j).

Os **modelos de serviço** dizem até onde vai o controle do cliente. Na IaaS, ele recebe máquinas virtuais, discos e rede e cuida do sistema operacional para cima; no PaaS, recebe uma plataforma pronta e cuida só da aplicação e da sua configuração; no SaaS, usa o software pronto. As definições de IaaS e de PaaS da Portaria 5.950/2023 traduzem quase literalmente as do NIST SP 800-145; a de SaaS descreve o lado do provedor:

CITAÇÃO LITERAL

"x) Modelo de Serviços em nuvem IaaS (...) O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados e, possivelmente, um controle limitado de alguns componentes de rede; y) Modelo de Serviços em nuvem PaaS (...) O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente sobre as configurações do ambiente de hospedagem de aplicações; z) Modelo de Serviços em nuvem SaaS (...) O provedor de serviço gerencia hardware e software e garante a disponibilidade e a segurança do aplicativo e de seus dados;"

Portaria SGD/MGI 5.950/2023, Anexo I, item 2.1, alíneas x, y e z · abrir a fonte

Modelo	O cliente recebe	Exemplos	O cliente ainda cuida de
IaaS (infraestrutura como serviço)	Máquinas virtuais, discos, redes virtuais, balanceadores	Máquina virtual de qualquer provedor público; nuvem privada com OpenStack	Sistema operacional (atualizações), middleware, aplicação, dados, contas e regras de rede
PaaS (plataforma como serviço)	Ambiente de execução, banco gerenciado, filas, Kubernetes gerenciado	Banco de dados como serviço, plataforma de aplicações web	Aplicação, configuração do ambiente, dados e acessos
SaaS (software como serviço)	O software completo, acessado pela web ou por API	Correio eletrônico, suíte de escritório, sistema de chamados	Dados, usuários, permissões e configuração do uso
FaaS (função como serviço)	Execução de funções disparadas por eventos	Funções sem servidor (tópico 3)	Código da função, permissões e dados

A lista de "como serviço" cresce: a Portaria 5.950/2023 define também o banco de dados como serviço (DBaaS) e a função como serviço (FaaS), e o guia do PPSI trata o contêiner como serviço (CaaS) como subconjunto da IaaS, entre IaaS e PaaS. Na CGU, o provisionamento de nuvem pública abrange expressamente as variantes:

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

CITAÇÃO LITERAL

"I - provisionamento de recursos de computação em nuvem - processo de disponibilização de recursos computacionais em nuvem pública, conforme a demanda das unidades administrativas, abrangendo infraestrutura como serviço, plataforma como serviço, software como serviço, função como serviço e backend como serviço;"

Portaria Normativa SE-CGU 223/2025, art. 2º, I · abrir a fonte

EXEMPLO COMENTADO · O SERVIÇO MEDIDO VIRA FATURA

```
def brl(v):                                   # 1234.5 -> '1.234,50'
    return f'{v:,.2f}'.replace(',', '#').replace('.', ',').replace('#', '.')

# Preços hipotéticos, em R$, só para mostrar como o serviço medido vira fatura
# (a primeira linha são 4 vCPU ligadas o mês todo, 730 horas)
uso = [('vCPU-hora de máquina virtual (IaaS)',      4 * 730, 0.20),
       ('GB-mês de disco em bloco (IaaS)',            500, 0.45),
       ('GB-mês de banco de dados gerenciado (PaaS)', 200, 1.10),
       ('GB transferido para a internet',             300, 0.50),
       ('usuário-mês de correio eletrônico (SaaS)',    40, 18.00)]
total = 0
for item, qtd, preco in uso:
    custo = qtd * preco
    total += custo
    print(f'{item:44} {qtd:>5} un. a R$ {brl(preco):>5} = R$ {brl(custo):>8}')
print(f'{"total do mês":44} R$ {brl(total)}')
print(f'mesmo uso com as máquinas ligadas só 10 h por dia útil (22 dias): '
      f'R$ {brl(total - 4 * 730 * 0.20 + 4 * 220 * 0.20)}')
```

SAÍDA DA EXECUÇÃO

```
vCPU-hora de máquina virtual (IaaS)          2920 un. a R$  0,20 = R$   584,00
GB-mês de disco em bloco (IaaS)               500 un. a R$  0,45 = R$   225,00
GB-mês de banco de dados gerenciado (PaaS)    200 un. a R$  1,10 = R$   220,00
GB transferido para a internet                300 un. a R$  0,50 = R$   150,00
usuário-mês de correio eletrônico (SaaS)       40 un. a R$ 18,00 = R$   720,00
total do mês                                                    R$ 1.899,00
mesmo uso com as máquinas ligadas só 10 h por dia útil (22 dias): R$ 1.491,00
```

Cada modelo tem a sua unidade: vCPU-hora e gigabyte-mês na IaaS, gigabyte de banco no PaaS, usuário-mês no SaaS, e a transferência para fora do provedor é cobrada à parte. O total foi de R$ 1.899,00. Desligar as máquinas fora do expediente (10 horas em 22 dias úteis, 220 horas em vez de 730) derruba a fatura para R$ 1.491,00: é o serviço medido funcionando a favor do cliente, o que não acontece com o servidor comprado, que custa o mesmo ligado ou desligado.

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

ESTRATÉGIA · APROFUNDE AQUI · P. 5 A 7

Sistemas Operacionais para CGU (TI, Infraestrutura de TI) · Capítulo 5 (Armazenamento)

Foco: a decisão entre data center próprio e nuvem (p. 5), os data centers de provedor, o co-location e a hospedagem (p. 6 e 7) e os data centers de hiperescala, base da IaaS, do PaaS e do SaaS (p. 7).

https://concursos.estrategia.com/ldi/sistemas-operacionais-para-cgu-auditor-federal-de-financas-e-controle-ti-infraestrutura-de-ti-pos-edital

SE O SEU CURSO FOR OUTRO

Gran (PDF): disciplina "Computação em Nuvem, Virtualização e Automação", PDF "Computação na Nuvem" (63 p.)

Direção (livro digital): módulo "Computação em Nuvem, Virtualização e Automação", aula 4 (Arquiteturas de serviços, parte 2 de 2), capítulo "Computação em Nuvem"

PONTOS IMPORTANTES

- As cinco características essenciais do NIST são autoatendimento sob demanda, amplo acesso pela rede, agrupamento de recursos, elasticidade rápida e serviço medido.
- Na IaaS, o cliente controla o sistema operacional, o armazenamento e as aplicações; no PaaS, só as aplicações e a configuração do ambiente; no SaaS, usa o software pronto.
- Em qualquer modelo, os dados, os usuários e as permissões continuam sob responsabilidade do cliente.
- Hospedagem e co-location são serviços de data center, sem as características da nuvem.

COMO O CEBRASPE PODE COBRAR

- Afirmar que, no autoatendimento sob demanda, o cliente depende de interação humana com o provedor para obter recursos.
- Dizer que, na IaaS, o sistema operacional das máquinas virtuais é atualizado pelo provedor, ou que, no PaaS, o cliente administra o sistema operacional.
- Incluir a virtualização, a alta disponibilidade ou o baixo custo entre as cinco características essenciais do NIST.
- Afirmar que, no SaaS, o cliente gerencia o middleware e a infraestrutura de execução do aplicativo.
- Tratar o co-location como modelo de serviço em nuvem.
- Dizer que o armazenamento em nuvem exige equipamento do provedor instalado no órgão, só serve a cópias de segurança ou impede controles como a criptografia e a autenticação multifator: ele é acessado pela rede, escala sob demanda e é pago pelo uso, com os controles de segurança do cliente.

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

2 Modelos de implantação e responsabilidade compartilhada

Os **modelos de implantação** dizem a quem a infraestrutura de nuvem se destina. A instrução do Gabinete de Segurança Institucional (GSI) que fixa os requisitos de segurança para o uso de nuvem pelos órgãos federais os define:

CITAÇÃO LITERAL

"I - nuvem privada (ou interna) - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos; II - nuvem comunitária - infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações (...) III - nuvem pública (ou externa) - infraestrutura de nuvem dedicada para uso aberto de qualquer organização (...) IV - nuvem híbrida - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações."

IN GSI/PR 5/2021, art. 3º · abrir a fonte

Dois detalhes caem em prova. A nuvem privada não precisa ficar dentro do órgão: pode ser operada por terceiros e ficar fora das suas instalações; o que a define é o uso exclusivo. E a nuvem híbrida não é a soma de duas nuvens quaisquer: as partes continuam distintas e se ligam por tecnologia padrão que permite mover dados e aplicações entre elas. A Portaria 5.950/2023 acrescenta a **nuvem de governo** (privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas) e a **multinuvem** (dois ou mais provedores de nuvem pública), e liga a escolha do modelo ao sigilo da informação de cada carga de trabalho: a informação sem restrição de acesso pode ir para qualquer modelo (item 5.4.2), a classificada em grau de sigilo não pode ir para a nuvem pública (item 5.4.4), e a protegida por sigilo legal fica na nuvem de governo:

CITAÇÃO LITERAL

"5.4.3. Devem ser mantidas em ambiente de nuvem de governo, exceto se expressamente determinado pelo Comitê de Governança Digital ou instância equivalente do órgão ou entidade, cargas de trabalho que tratem informação com restrição de acesso prevista na legislação, a exemplo de: sigilo fiscal, bancário, comercial, empresarial, contábil, de segredo industrial, de direito autoral, de propriedade intelectual, industrial, policial, processual civil, processual penal e disciplinar administrativa."

Portaria SGD/MGI 5.950/2023, Anexo I, item 5.4.3 · abrir a fonte

Os sistemas estruturantes (os que sustentam as atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, serviços gerais e outras atividades auxiliares comuns que necessitem de coordenação central, na definição da Portaria 5.950/2023, Anexo I, item 2.1, alínea am) têm regra própria: só nuvem privada ou comunitária restrita às infraestruturas de órgãos ou entidades (IN GSI/PR 5/2021, art. 11, IV).

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

EXEMPLO COMENTADO · ONDE CADA CARGA DE TRABALHO PODE RODAR

```
# sistemas fictícios de um órgão: (nome, estruturante?, informação tratada)
cargas = [
    ('Portal de dados abertos',              False, 'sem restrição'),
    ('Painel de compras públicas',           False, 'sem restrição'),
    ('Apuração de denúncias',                False, 'restrição legal'),
    ('Folha de pagamento de pessoal',        True,  'restrição legal'),
    ('Relatório reservado de inteligência',  False, 'classificada'),
]   # as denúncias têm sigilo processual
def onde(estruturante, info):
    if estruturante:                    # IN GSI/PR 5, art. 11, IV
        return 'nuvem privada ou comunitária restrita a órgãos'
    if info == 'classificada':          # Portaria 5.950, item 5.4.4
        return 'nunca em nuvem pública'
    if info == 'restrição legal':       # Portaria 5.950, item 5.4.3
        return 'nuvem de governo, salvo decisão do comitê'
    # Portaria 5.950, item 5.4.2
    return 'qualquer modelo (pública, privada, híbrida ou comunitária)'
for nome, estr, info in cargas:
    print(f'{nome}\n    -> {onde(estr, info)}')
```

SAÍDA DA EXECUÇÃO

```
Portal de dados abertos
    -> qualquer modelo (pública, privada, híbrida ou comunitária)
Painel de compras públicas
    -> qualquer modelo (pública, privada, híbrida ou comunitária)
Apuração de denúncias
    -> nuvem de governo, salvo decisão do comitê
Folha de pagamento de pessoal
    -> nuvem privada ou comunitária restrita a órgãos
Relatório reservado de inteligência
    -> nunca em nuvem pública
```

A ordem dos testes importa: a regra do sistema estruturante vale qualquer que seja a informação, e a da informação classificada vem antes da do sigilo legal, porque é a mais restritiva. O resultado é uma arquitetura híbrida: o mesmo órgão usa nuvem pública para o portal e o painel, nuvem de governo para as denúncias e infraestrutura própria ou comunitária para a folha e para o relatório classificado.

A **responsabilidade compartilhada** divide a segurança e a operação entre o provedor e o cliente, camada por camada. O provedor sempre responde pelo que o cliente não vê (instalações, servidores físicos, rede física, hipervisor); o cliente sempre responde pelos seus dados, pelas identidades e pelas permissões que concede. O que fica no meio muda com o modelo de serviço. O guia do PPSI descreve a divisão em cada controle:

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

CITAÇÃO LITERAL

"Privado (on-premises) - A organização é responsável pela segurança de tudo (servidores físicos, sala, rede, armazenamento, hipervisor, sistemas operacionais, etc.). (...) IaaS - A organização implanta, opera e mantém as redes virtuais e máquinas virtuais dentro desse modelo de serviço, mas não gerencia a infraestrutura de nuvem subjacente (servidores físicos, rede física, armazenamento físico, hipervisor, etc.), pois essa é uma responsabilidade do Provedor de Serviços em Nuvem (CSP - em inglês). (...) SaaS - Não se aplica à organização, pois SaaS e FaaS estão categorizados como soluções de software. O CSP é responsável por tudo, exceto pelos dados."

SGD, Guia Complementar de Segurança da Informação para Computação em Nuvem (2025), controle 1, p. 16 e 17 · abrir a fonte

Camada	Local (on-premises)	IaaS	PaaS	SaaS
Dados, contas, identidades e permissões	Órgão	Órgão	Órgão	Órgão
Aplicação e sua configuração	Órgão	Órgão	Órgão	Provedor (o órgão configura o uso)
Middleware, ambiente de execução e sistema operacional	Órgão	Órgão	Provedor	Provedor
Redes virtuais, regras de firewall virtual e máquinas virtuais	Órgão	Órgão	Provedor, com algumas configurações do órgão	Provedor
Hipervisor, servidores, armazenamento e rede físicos, instalações	Órgão	Provedor	Provedor	Provedor

A divisão exata vem no contrato. A IN GSI/PR 5/2021 obriga o órgão a exigir que o provedor documente as suas responsabilidades e a elaborar a própria matriz:

CITAÇÃO LITERAL

"II - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem; III - elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias;"

IN GSI/PR 5/2021, art. 16, II e III · abrir a fonte

Quando a contratação é feita por um **integrador** (cloud broker), que integra dois ou mais provedores, a matriz ganha um terceiro ator. A Portaria 5.950/2023 prevê o modelo totalmente gerenciado pelo integrador e o parcialmente gerenciado (o órgão opera os recursos pela plataforma do integrador), exige matriz de responsabilidades no termo de referência (item 25.4) e um termo de compartilhamento de responsabilidades entre o integrador e o provedor (item 25.6). O TCU apontou justamente a falta de clareza dessa divisão como risco na contratação centralizada de nuvem pelo Ministério da Gestão (Acórdão 292/2025-Plenário).

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

PONTOS IMPORTANTES

- Nuvem privada é de uso exclusivo de um órgão, mesmo quando operada por terceiros ou fora das suas instalações; a pública é aberta a qualquer organização.
- Na nuvem híbrida, as infraestruturas continuam distintas e se ligam por tecnologia padrão que permite a portabilidade.
- Informação com sigilo legal fica na nuvem de governo, a classificada não vai para a nuvem pública e os sistemas estruturantes só usam nuvem privada ou comunitária de órgãos.
- Na responsabilidade compartilhada, o provedor responde pelo físico e pelo hipervisor, e o cliente sempre responde pelos dados, pelas identidades e pelas permissões.

COMO O CEBRASPE PODE COBRAR

- Afirmar que a nuvem privada precisa estar fisicamente instalada nas dependências do órgão.
- Definir nuvem híbrida como qualquer uso simultâneo de dois provedores, sem a interoperabilidade e a portabilidade entre as infraestruturas.
- Dizer que, ao contratar SaaS, o órgão transfere ao provedor a responsabilidade pelos dados e pelos acessos dos usuários.
- Afirmar que sistemas estruturantes podem ser hospedados em nuvem pública desde que haja cópia de segurança no Brasil.
- Inverter os modelos, chamando de comunitária a nuvem aberta ao público em geral.

3 Redes virtuais e integração com o ambiente local

Na IaaS, o órgão monta a própria **rede virtual** dentro do provedor (VPC, na AWS e no Google Cloud; VNet, no Azure): um espaço de endereços privado, isolado logicamente das redes dos outros clientes, dividido em sub-redes e controlado por tabelas de rotas e regras de filtragem. Os elementos se repetem nos provedores, com nomes diferentes:

Elemento	Função
Bloco de endereços (CIDR)	Faixa privada da rede virtual, como 10.20.0.0/16; não pode repetir faixas do ambiente local com que vai se comunicar
Sub-rede pública	Tem rota para o gateway de internet; recebe o balanceador de carga e o que precisa ser alcançado de fora
Sub-rede privada	Sem rota de entrada pela internet; recebe aplicações e bancos. Sai para a internet, quando precisa, por um gateway de tradução de endereços (NAT)
Zona de disponibilidade	Data center ou grupo de data centers isolado dentro de uma região; sub-redes em zonas diferentes resistem à falha de uma zona
Grupo de segurança	Firewall virtual ligado à interface da máquina; nos grandes provedores, guarda o estado da conexão (a resposta de uma conexão permitida volta sem regra própria)

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Lista de controle de acesso da sub-rede	Filtro na fronteira da sub-rede; na AWS, não guarda estado, e por isso exige regras nos dois sentidos
Emparelhamento (peering)	Liga duas redes virtuais pela rede do provedor; não é transitivo: se A fala com B e B com C, A não fala com C por B
Ponto de acesso privado (private endpoint)	Acesso a um serviço gerenciado (banco, armazenamento de objetos) por endereço privado, sem passar pela internet

No modelo de responsabilidade compartilhada, essa rede é do cliente. O guia do PPSI, no controle de gestão da infraestrutura de rede:

> **CITAÇÃO LITERAL**
>
> *"IaaS - A organização implanta, opera e mantém redes virtuais e firewalls de aplicações web dentro deste modelo de serviço, mas não gerencia a infraestrutura física subjacente, como servidores físicos, rede física, armazenamento, hipervisor etc., pois isso é responsabilidade do CSP. (...) Garantir que todos os firewalls virtuais estejam configurados com política de negação por padrão (deny by default)."*
>
> SGD, Guia Complementar de Segurança da Informação para Computação em Nuvem (2025), controle 12, p. 37 · abrir a fonte

A **integração com o ambiente local** liga a rede virtual ao data center do órgão. As formas, da mais simples à mais robusta: a **VPN site a site**, um túnel IPsec cifrado sobre a internet, rápido de montar, com banda e latência que variam com a internet; o **enlace dedicado** (Direct Connect, ExpressRoute, Cloud Interconnect), circuito privado com banda contratada e latência estável, que não passa pela internet e, por isso, não é cifrado por padrão; e a topologia **hub-and-spoke**, em que um centro de trânsito concentra as conexões das várias redes virtuais e do ambiente local. Na prática, usam-se o enlace dedicado como caminho principal e a VPN como contingência. Completam a integração o DNS híbrido (nomes resolvidos dos dois lados), a identidade federada (seção 5) e o plano de endereços sem sobreposição. A Portaria 5.950/2023 pede controles de transferência de dados, como criptografia e VPN adequada (Anexo I, item 10.2, alínea h).

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

EXEMPLO COMENTADO · O PLANO DE ENDEREÇOS DA REDE VIRTUAL

```
import ipaddress as ip

vpc = ip.ip_network('10.20.0.0/16')                    # rede virtual na nuvem
# redes do órgão
local = [ip.ip_network('10.0.0.0/14'), ip.ip_network('192.168.10.0/24')]
for r in local:
    print(f'{vpc} sobrepõe {r}? {vpc.overlaps(r)}')

# Quatro sub-redes /24 em duas zonas: uma pública e uma privada em cada
nomes = ['pública, zona A', 'privada, zona A',
         'pública, zona B', 'privada, zona B']
for nome, sub in zip(nomes, vpc.subnets(new_prefix=24)):
    uteis = sub.num_addresses - 5
    print(f'{nome:16} {str(sub):14} {uteis} endereços utilizáveis')
n24 = len(list(vpc.subnets(new_prefix=24)))
print('sub-redes /24 que cabem na rede /16:', n24)

# Erro comum: rede virtual que repete a faixa do ambiente local
nova = ip.ip_network('10.2.0.0/16')
print(f'{nova} sobrepõe {local[0]}? {nova.overlaps(local[0])}')
```

SAÍDA DA EXECUÇÃO

```
10.20.0.0/16 sobrepõe 10.0.0.0/14? False
10.20.0.0/16 sobrepõe 192.168.10.0/24? False
pública, zona A  10.20.0.0/24   251 endereços utilizáveis
privada, zona A  10.20.1.0/24   251 endereços utilizáveis
pública, zona B  10.20.2.0/24   251 endereços utilizáveis
privada, zona B  10.20.3.0/24   251 endereços utilizáveis
sub-redes /24 que cabem na rede /16: 256
10.2.0.0/16 sobrepõe 10.0.0.0/14? True
```

A rede 10.20.0.0/16 não colide com as do órgão (10.0.0.0/14 vai de 10.0.0.0 a 10.3.255.255) e comporta 256 sub-redes /24. Cada /24 tem 256 endereços, mas o provedor reserva alguns: na AWS são cinco por sub-rede (rede, roteador, DNS, um reservado e difusão), o que deixa 251. Já 10.2.0.0/16 cai dentro de 10.0.0.0/14: com a VPN ou o enlace dedicado ligados, os roteadores não saberiam para que lado mandar um pacote para 10.2.1.10, e a integração falha. O plano de endereços se faz antes de criar a primeira rede virtual.

SÓ NESTE MATERIAL

As redes virtuais na nuvem (sub-redes, grupos de segurança, emparelhamento, pontos de acesso privado) e as formas de ligação com o ambiente local não estão nos capítulos já liberados do Estratégia. Para esses pontos, este material é a fonte de estudo.

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

PONTOS IMPORTANTES

- A rede virtual é responsabilidade do cliente na IaaS: sub-redes, rotas e regras de filtragem são configuradas por ele.
- Sub-rede pública tem rota para o gateway de internet; a privada não recebe conexões da internet e sai, quando precisa, por NAT.
- O emparelhamento entre redes virtuais não é transitivo, e as faixas de endereços não podem se sobrepor.
- VPN site a site cifra o tráfego sobre a internet; o enlace dedicado dá banda e latência estáveis, sem passar pela internet.

COMO O CEBRASPE PODE COBRAR

- Afirmar que o emparelhamento entre redes virtuais é transitivo.
- Dizer que o enlace dedicado entre o data center e o provedor trafega pela internet pública.
- Afirmar que, na IaaS, a configuração das redes virtuais e dos firewalls virtuais é responsabilidade exclusiva do provedor.
- Considerar adequado que a rede virtual repita a faixa de endereços do ambiente local com que vai se comunicar.

4 Elasticidade, escalabilidade e portabilidade

Escalabilidade é a capacidade de atender a uma carga maior acrescentando recursos. **Elasticidade** é escalar automaticamente nos dois sentidos, acompanhando a demanda, e devolver o que sobra: toda solução elástica é escalável, mas nem toda escalável é elástica (um servidor que só cresce com compra e instalação é escalável e não é elástico). O curso de DevOps da Enap, na Escola Virtual de Governo (EVG), define a escalabilidade e as suas duas direções:

CITAÇÃO LITERAL

"Escalabilidade é a capacidade de um ambiente de se ajustar a demanda no momento, provisionando ou liberando recursos para o serviço de uma forma transparente para o usuário. (...) A escalabilidade vertical consiste em crescer o ambiente já disponibilizado, aumentando o número de processadores, disco ou memória RAM, por exemplo. Trata-se de um crescimento limitado, pois existe um limite para a quantidade de recursos que podem ser adicionados a uma máquina. (...) A escalabilidade horizontal vem da ideia de aumentarmos os números de instâncias da aplicação, permitindo o crescimento constante e virtualmente ilimitado da quantidade de recursos disponibilizados para a aplicação."

Enap, O papel do DevOps na Transformação Digital dos Serviços Públicos (EVG), módulo 3, item 1.5, p. 14 e 15 · abrir a fonte

	Vertical (scale up)	Horizontal (scale out)
Como cresce	Máquina maior: mais vCPU, memória, disco	Mais instâncias iguais atrás de um balanceador

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Limite	O maior tipo de máquina disponível	Na prática, as cotas e o custo
Interrupção	Em geral exige reiniciar a máquina	Não: instâncias entram e saem com o serviço no ar
Exige da aplicação	Nada em particular	Que não guarde estado na instância (sessão, arquivos locais), ou que o estado fique num serviço compartilhado
Alta disponibilidade	Não traz: continua sendo uma máquina	Traz, se as instâncias ficarem em zonas diferentes

O escalonamento automático (autoscaling) usa uma política: por meta (manter o uso médio de CPU em 70%, por exemplo), por degraus, por agenda (mais instâncias às 8h dos dias úteis) ou preditiva. Tem sempre mínimo, máximo e um intervalo de espera entre ajustes, para não oscilar. A elasticidade parece ilimitada ao cliente, mas existem cotas por conta e por região.

EXEMPLO COMENTADO · ELASTICIDADE CONTRA CAPACIDADE FIXA DIMENSIONADA PARA O PICO

```
import math
import numpy as np

# Demanda fictícia de um serviço público (requisições por segundo, por hora)
demanda = np.array([
    40, 30, 25, 25, 30, 60, 150, 400, 900, 1200, 1300, 1250,
    1100, 1150, 1250, 1300, 1100, 800, 500, 300, 200, 120, 80, 50])
# capacidade de cada instância e uso-alvo de CPU
POR_INSTANCIA, ALVO = 200, 0.70
por_inst = POR_INSTANCIA * ALVO
inst = np.array([max(2, math.ceil(d / por_inst)) for d in demanda])
fixo = inst.max()        # dimensionado para o pico, ligado o dia todo
print('instâncias por hora:', ' '.join(str(i) for i in inst))
print(f'pico: {fixo} instâncias | instância-hora no dia: '
      f'elástico {inst.sum()}, fixo {fixo * 24}')
print(f'economia da elasticidade: {1 - inst.sum() / (fixo * 24):.0%}')
capacidade = fixo * POR_INSTANCIA * 24
print(f'uso médio da capacidade fixa: {demanda.sum() / capacidade:.0%}')
```

SAÍDA DA EXECUÇÃO

```
instâncias por hora: 2 2 2 2 2 2 2 3 7 9 10 9 8 9 9 10 8 6 4 3 2 2 2 2
pico: 10 instâncias | instância-hora no dia: elástico 117, fixo 240
economia da elasticidade: 51%
uso médio da capacidade fixa: 28%
```

Com 200 requisições por segundo por instância e meta de 70% de uso, cada instância atende 140 requisições por segundo, e o mínimo de duas mantém a redundância de madrugada. O pico pede 10 instâncias. A elasticidade consome 117 instâncias-hora no dia, contra 240 da capacidade fixa: 51% a menos. A capacidade fixa ficaria, na média do dia, com só 28% de uso. Na nuvem, a economia vira fatura menor; no data center próprio, o equipamento do pico já foi comprado.

Portabilidade é a possibilidade de levar dados e aplicações para outro provedor ou de volta ao ambiente local, com custo e prazo aceitáveis. O contrário é o **aprisionamento** (lock-in): a solução fica presa ao provedor por serviços proprietários, formatos fechados, custo de saída de dados ou falta de

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

documentação. A Portaria 5.950/2023 lista as ações preventivas:

CITAÇÃO LITERAL

"8.2. Como forma de mitigar os riscos de dependência tecnológica ou aprisionamento (lock-in), sempre que possível, devem ser realizadas ações preventivas antes ou durante a adoção de software ou da execução dos serviços em nuvem, a exemplo de: a) utilizar padrões tecnológicos interoperáveis; b) considerar o uso de tecnologia de contêineres, de forma a facilitar a implantação padronizada de soluções; c) evitar o uso de tecnologias e ferramentas proprietárias que possam dificultar a portabilidade de aplicações e de dados entre nuvens de diferentes provedores; d) evitar o uso de bancos de dados proprietário de um provedor de nuvem específico; e) considerar a contratação de mais de um provedor de nuvem como contingência; e f) considerar a alternativa de utilizar a própria infraestrutura de TIC como contingência."

Portaria SGD/MGI 5.950/2023, Anexo I, item 8.2 · abrir a fonte

O mesmo item 8 exige que o termo de referência assegure a portabilidade de dados e aplicativos sem custo adicional (item 8.5) e manda avaliar abordagens híbridas e multinuvem (item 8.3). Na CGU, a multinuvem é princípio do provisionamento:

CITAÇÃO LITERAL

"§ 6º O princípio da multinuvem estabelece a adoção de um modelo que utilize múltiplos provedores de serviços de nuvem, com o objetivo de reduzir o risco de dependência de um único fornecedor, devendo a estratégia de multinuvem garantir flexibilidade e resiliência nos serviços de computação em nuvem"

Portaria Normativa SE-CGU 223/2025, art. 3º, § 6º · abrir a fonte

Portabilidade tem custo: usar só o denominador comum dos provedores abre mão de serviços gerenciados que economizam operação. O relatório da Secretaria de Governo Digital sobre aprisionamento recomenda contêineres Docker, Kubernetes conforme a versão padrão do projeto (upstream), infraestrutura como código com Terraform, bancos de código aberto e mensageria com protocolos abertos.

ESTRATÉGIA · APROFUNDE AQUI · P. 7 E 8

Sistemas Operacionais para CGU (TI, Infraestrutura de TI) · Capítulo 5 (Armazenamento)

Foco: escalabilidade como requisito do data center e a diferença entre a horizontal (scale-out) e a vertical (scale-up).

https://concursos.estrategia.com/ldi/sistemas-operacionais-para-cgu-auditor-federal-de-financas-e-controle-ti-infraestrutura-de-ti-pos-edital

SE O SEU CURSO FOR OUTRO

Gran (PDF): disciplina "Computação em Nuvem, Virtualização e Automação", PDF "Computação na Nuvem" (63 p.)

Direção (livro digital): módulo "Computação em Nuvem, Virtualização e Automação", aula 4 (Arquiteturas de serviços, parte 2 de 2), capítulo "Computação em Nuvem"

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

PONTOS IMPORTANTES

- Escalabilidade é crescer acrescentando recursos; elasticidade é crescer e encolher automaticamente com a demanda.
- Escalar na vertical aumenta a máquina e tem teto; escalar na horizontal acrescenta instâncias e pede aplicação sem estado local.
- Portabilidade se garante com padrões abertos, contêineres, bancos não proprietários, cláusula de devolução dos dados e plano de saída.
- A multinuvem reduz a dependência de um fornecedor, e a CGU a adota como princípio do provisionamento.

COMO O CEBRASPE PODE COBRAR

- Tratar escalabilidade e elasticidade como sinônimos, ou afirmar que a elasticidade só permite aumentar recursos.
- Dizer que a escalabilidade vertical consiste em acrescentar novas máquinas ao conjunto.
- Afirmar que a nuvem oferece recursos efetivamente ilimitados, sem cotas.
- Dizer que o uso de serviços proprietários do provedor aumenta a portabilidade da solução.

5 Dependência entre serviços e requisitos de segurança

Uma aplicação em nuvem raramente é uma máquina só: ela depende de banco gerenciado, fila, cofre de chaves, serviço de identidade, DNS, armazenamento de objetos, cada um com a sua disponibilidade, a sua região e o seu contrato. Três cuidados decorrem disso. O primeiro é **mapear as dependências**, inclusive as invisíveis (o serviço de identidade do provedor, o DNS, um software de terceiros comprado no marketplace). O segundo é calcular a **disponibilidade composta**: componentes de que o serviço depende em série multiplicam as disponibilidades, e o conjunto fica abaixo do pior deles. O terceiro é conhecer o **raio de impacto**: a falha de um serviço compartilhado derruba todos os que dependem dele. O mapeamento de dependências foi objeto de recomendação da própria CGU, a que a Secretaria de Governo Digital respondeu com um relatório técnico:

CITAÇÃO LITERAL

"Recomendação da Controladoria Geral da União (CGU): Disponibilizar template de documento ou ferramenta (ex.: planilha contendo esqueleto de itens ou colunas a serem consideradas) para apoiar os órgãos contratantes no mapeamento de dependências dos serviços hospedados em nuvem, de componentes nativos do provedor e mapeamento de softwares de terceiros utilizados a partir do marketplace do provedor."

SGD, Relatório técnico, Recursos de nuvem: boas práticas para minimizar o aprisionamento (lock-in) em nuvem (2024), p. 1 · abrir a fonte

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

EXEMPLO COMENTADO · O MAPA DE DEPENDÊNCIAS E A DISPONIBILIDADE COMPOSTA

```
from graphlib import TopologicalSorter

# Sistema fictício de gestão de auditorias e as dependências de cada componente
dep = {'portal web':        ('API de auditorias', 'identidade (SSO)'),
       'API de auditorias': ('banco gerenciado', 'fila de eventos',
                             'cofre de chaves', 'identidade (SSO)'),
       'fila de eventos':   ('cofre de chaves',),
       'banco gerenciado':  ('cofre de chaves',),
       'identidade (SSO)':  (), 'cofre de chaves': ()}
print('ordem para subir ou recuperar:')
for i, c in enumerate(TopologicalSorter(dep).static_order(), 1):
    print(f'  {i}. {c}')

sla = {'portal web': 0.9995, 'API de auditorias': 0.9995,
       'banco gerenciado': 0.9995, 'fila de eventos': 0.999,
       'cofre de chaves': 0.9999, 'identidade (SSO)': 0.999}
MES = 30 * 24 * 60
serie = 1.0
for a in sla.values():
    serie *= a                  # basta um falhar para o portal parar
print(f'disponibilidade composta: {serie:.3%}, '
      f'ou {(1 - serie) * MES:.0f} min fora do ar por mês')
frageis = [c for c in sla if sla[c] == min(sla.values())]
print('componentes mais frágeis:', ', '.join(frageis))
# duas cópias independentes de cada um, em zonas diferentes
for c in frageis:
    serie = serie / sla[c] * (1 - (1 - sla[c]) ** 2)
print(f'com os dois em duas zonas: {serie:.3%}, '
      f'ou {(1 - serie) * MES:.0f} min por mês')
```

SAÍDA DA EXECUÇÃO

```
ordem para subir ou recuperar:
  1. identidade (SSO)
  2. cofre de chaves
  3. fila de eventos
  4. banco gerenciado
  5. API de auditorias
  6. portal web
disponibilidade composta: 99.641%, ou 155 min fora do ar por mês
componentes mais frágeis: fila de eventos, identidade (SSO)
com os dois em duas zonas: 99.840%, ou 69 min por mês
```

A ordenação topológica dá a sequência de subida e de recuperação: identidade e cofre de chaves primeiro, porque todos dependem deles, e o portal por último. Seis componentes com 99,9% a 99,99% cada resultam em 99,641% para o portal, cerca de 155 minutos fora do ar por mês, bem abaixo do melhor componente. Duplicar em duas zonas os dois mais frágeis (fila e identidade) eleva o conjunto a 99,840%, cerca de 69 minutos por mês: a redundância rende mais onde o componente é mais frágil. A conta supõe falhas independentes; uma falha de região derruba as duas zonas ao mesmo tempo.

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Os **requisitos de segurança** para o uso de nuvem pelos órgãos federais estão na IN GSI/PR 5/2021 e se dividem entre o órgão e o provedor:

Tema	O que a norma exige	Onde
Antes de migrar	Gestão de riscos precedida de relatório de impacto à proteção de dados, definição do modelo de serviço e de implantação, avaliação da informação a hospedar e planejamento dos custos de entrada e de saída	Art. 11
Identidade e registros	Identidade federada com autenticação única (SSO), sem acesso do provedor ao ambiente de autenticação do órgão; MFA conforme a criticidade; registros guardados pelo provedor por um ano e pelo órgão por cinco	Art. 13
Criptografia	Analisar a necessidade de cifrar conforme riscos e criticidade; chaves em hardware sempre que possível	Art. 14
Segregação	Isolamento lógico entre clientes e entre aplicações, sistemas operacionais, armazenamento e rede	Art. 15
Gerenciamento	Equipe capacitada, matriz de responsabilidades e processo de incidentes com o provedor	Art. 16
Localização	Dados no Brasil, com regras para cópias no exterior	Art. 18
Contrato	Confidencialidade, exclusividade de direitos sobre os dados, proibição de uso secundário (inclusive para treinar IA), devolução integral e eliminação ao fim do contrato	Art. 19
Provedor	Gestão de riscos, fortalecimento da virtualização, TLS, cifra com chaves geradas pelo órgão, plano de recuperação de desastres, auditoria SOC 2 tipos I e II por auditor independente	Arts. 20 e 25

CITAÇÃO LITERAL

"Art. 18. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições: I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro; II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;"

IN GSI/PR 5/2021, art. 18, I e II · abrir a fonte

A informação com restrição de acesso prevista em lei e suas cópias não podem ser tratadas fora do Brasil (art. 18, III), e a Portaria 5.950/2023 exige que cada provedor tenha ao menos dois data centers no território nacional (Anexo I, item 10.2, alínea b). Os controles detalhados (zero trust, firewall de aplicação, proteção contra negação de serviço) são da matéria Cibersegurança, Privacidade e Continuidade de Serviços.

SÓ NESTE MATERIAL

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

A dependência entre serviços de nuvem (mapeamento, disponibilidade composta, raio de impacto) e o conjunto dos requisitos da IN GSI/PR 5/2021 não estão nos capítulos já liberados do Estratégia. Para esses pontos, este material é a fonte de estudo.

PONTOS IMPORTANTES

- Componentes em série multiplicam as disponibilidades; o serviço fica abaixo do componente mais frágil, e a redundância deve atacar os mais frágeis.
- O mapeamento de dependências inclui os serviços nativos do provedor e os softwares de terceiros do marketplace.
- Os dados ficam no Brasil, com ao menos uma cópia atualizada no país; a informação com restrição legal não sai do território.
- O provedor comprova a conformidade com auditoria SOC 2, tipos I e II, por auditor independente.

COMO O CEBRASPE PODE COBRAR

- Afirmar que a disponibilidade de um serviço que depende de vários componentes é igual à do componente mais confiável.
- Dizer que a IN GSI/PR 5/2021 permite ao provedor acessar diretamente o ambiente de autenticação do órgão para viabilizar o login único.
- Afirmar que informação sem restrição de acesso não pode ter cópia de segurança fora do Brasil.
- Dizer que a responsabilidade pelos registros de acesso é só do provedor, que os guarda por cinco anos.

PARA IR ALÉM · CURSOS DA EVG E DA ENAP (OPCIONAL)

- Administração de Serviços na Nuvem de Governo (EVG): administração de serviços em nuvem de governo, com as normas do GSI
- O papel do DevOps na Transformação Digital dos Serviços Públicos (Enap): infraestrutura em nuvem e escalabilidade (módulo 3)

? Questões abertas de fixação

Responda sem consultar. As respostas estão na página seguinte.

1. Quais são as cinco características essenciais da computação em nuvem segundo o NIST?

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

2. O que o cliente controla na IaaS e no PaaS, segundo a Portaria SGD/MGI 5.950/2023?

3. Diferencie nuvem privada, comunitária, pública e híbrida.

4. Onde podem ficar, pela Portaria 5.950/2023 e pela IN GSI/PR 5/2021, as cargas com informação sem restrição, com sigilo legal e classificada, e os sistemas estruturantes?

5. O que é a responsabilidade compartilhada e o que fica sempre com o cliente?

6. O que a IN GSI/PR 5/2021 exige do órgão sobre a divisão de responsabilidades?

7. Diferencie sub-rede pública e sub-rede privada numa rede virtual.

8. Compare a VPN site a site e o enlace dedicado na integração com o ambiente local.

9. Diferencie escalabilidade vertical, escalabilidade horizontal e elasticidade.

10. Cite ações da Portaria 5.950/2023 para mitigar o aprisionamento ao provedor.

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

11. Como se calcula a disponibilidade de um serviço que depende de vários componentes em série, e o que a redundância muda?

12. Que regras de localização de dados a IN GSI/PR 5/2021 estabelece?

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

✓ Respostas das questões abertas

1.

Quais são as cinco características essenciais da computação em nuvem segundo o NIST?

Autoatendimento sob demanda, amplo acesso pela rede, agrupamento de recursos, elasticidade rápida e serviço medido.

2.

O que o cliente controla na IaaS e no PaaS, segundo a Portaria SGD/MGI 5.950/2023?

Na IaaS, o cliente controla os sistemas operacionais, o armazenamento e os aplicativos instalados, e talvez alguns componentes de rede; no PaaS, só as aplicações instaladas e, possivelmente, as configurações do ambiente de hospedagem. Em nenhum dos dois controla a infraestrutura subjacente.

3.

Diferencie nuvem privada, comunitária, pública e híbrida.

A privada é de uso exclusivo de um órgão e pode ser operada por ele ou por terceiros; a comunitária é de uso exclusivo de um grupo de órgãos com a mesma natureza de trabalho; a pública é aberta a qualquer organização; a híbrida combina duas ou mais dessas infraestruturas, que continuam distintas e se ligam por tecnologia padrão que permite a portabilidade.

4.

Onde podem ficar, pela Portaria 5.950/2023 e pela IN GSI/PR 5/2021, as cargas com informação sem restrição, com sigilo legal e classificada, e os sistemas estruturantes?

Sem restrição, em qualquer modelo; com sigilo legal, na nuvem de governo, salvo decisão do comitê de governança digital; classificada, nunca em nuvem pública; sistemas estruturantes, só em nuvem privada ou comunitária restrita a infraestruturas de órgãos.

5.

O que é a responsabilidade compartilhada e o que fica sempre com o cliente?

É a divisão das responsabilidades de operação e de segurança entre provedor e cliente, camada por camada, conforme o modelo de serviço. O provedor responde pelo físico e pelo hipervisor; o cliente sempre responde pelos dados, pelas identidades e pelas permissões.

6.

O que a IN GSI/PR 5/2021 exige do órgão sobre a divisão de responsabilidades?

Que exija do provedor a documentação dos seus papéis e responsabilidades de segurança e que elabore a própria matriz de responsabilidades, com as suas obrigações.

7.

Diferencie sub-rede pública e sub-rede privada numa rede virtual.

A pública tem rota para o gateway de internet e recebe o que precisa ser acessado de fora, como o balanceador; a privada não recebe conexões da internet, abriga aplicações e bancos e sai para a internet, quando precisa, por um gateway de NAT.

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

8.

Compare a VPN site a site e o enlace dedicado na integração com o ambiente local.

A VPN cria um túnel IPsec cifrado sobre a internet, rápido e barato, com banda e latência variáveis; o enlace dedicado é um circuito privado, que não passa pela internet, com banda contratada e latência estável, e não é cifrado por padrão.

9.

Diferencie escalabilidade vertical, escalabilidade horizontal e elasticidade.

A vertical aumenta os recursos de uma máquina e tem teto; a horizontal acrescenta instâncias e exige aplicação sem estado local; a elasticidade é o ajuste automático nos dois sentidos, acompanhando a demanda.

10.

Cite ações da Portaria 5.950/2023 para mitigar o aprisionamento ao provedor.

Padrões interoperáveis, contêineres, evitar ferramentas e bancos proprietários do provedor, mais de um provedor como contingência, a infraestrutura própria como contingência e cláusula de portabilidade de dados e aplicativos sem custo adicional.

11.

Como se calcula a disponibilidade de um serviço que depende de vários componentes em série, e o que a redundância muda?

Multiplicam-se as disponibilidades dos componentes, e o resultado fica abaixo do pior deles. Com duas cópias independentes de um componente, a indisponibilidade dele passa a ser o produto das indisponibilidades das cópias.

12.

Que regras de localização de dados a IN GSI/PR 5/2021 estabelece?

Os dados devem ficar em território brasileiro, com ao menos uma cópia atualizada no país; a informação sem restrição de acesso pode ter cópias no exterior; a informação com restrição legal e suas cópias não podem ser tratadas fora do Brasil.

§ Questões de certo ou errado

Cada item cobra um ponto do tópico, do jeito que o Cebraspe cobra. Marque C ou E. O gabarito comentado está na página seguinte.

1. No autoatendimento sob demanda, característica essencial da computação em nuvem, o consumidor provisiona recursos sem precisar de interação humana com o provedor. ( )

2. A virtualização é uma das cinco características essenciais da computação em nuvem definidas pelo NIST. ( )

3. No modelo PaaS, o cliente controla o sistema operacional e o armazenamento da plataforma em que suas aplicações são executadas. ( )

4. No modelo IaaS, o cliente tem controle sobre os sistemas operacionais e os aplicativos instalados, mas não sobre a infraestrutura física subjacente. ( )

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

5. A nuvem privada, por definição, deve estar instalada nas dependências físicas do órgão que a utiliza. ( )

6. Na nuvem híbrida, as infraestruturas que a compõem permanecem distintas, mas são agrupadas por tecnologia padrão que permite a portabilidade de dados e aplicações. ( )

7. Segundo a IN GSI/PR 5/2021, os sistemas estruturantes podem ser hospedados em nuvem pública, desde que mantida cópia de segurança no Brasil. ( )

8. No modelo SaaS, a responsabilidade pelos dados armazenados e pela gestão dos acessos dos usuários passa integralmente ao provedor. ( )

9. O emparelhamento (peering) entre redes virtuais é transitivo: se a rede A está emparelhada com B e B com C, A alcança C por meio de B. ( )

10. A conexão por enlace dedicado entre o data center do órgão e o provedor de nuvem não trafega pela internet pública. ( )

11. A escalabilidade vertical consiste em acrescentar novas instâncias da aplicação, de modo a distribuir a carga entre elas. ( )

12. A elasticidade permite que os recursos sejam reduzidos automaticamente quando a demanda diminui. ( )

13. A Portaria SGD/MGI 5.950/2023 recomenda considerar o uso de contêineres como forma de mitigar o aprisionamento tecnológico. ( )

14. A disponibilidade de um serviço que depende, em série, de cinco componentes com 99,9% de disponibilidade cada é de 99,9%. ( )

15. Pela IN GSI/PR 5/2021, o órgão deve adotar identidade federada para autenticação única no provedor, negando a este o acesso direto ao seu ambiente de autenticação. ( )

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

✓ Gabarito comentado

1 C

No autoatendimento sob demanda, característica essencial da computação em nuvem, o consumidor provisiona recursos sem precisar de interação humana com o provedor.

É a primeira das cinco características do NIST.

2 E

A virtualização é uma das cinco características essenciais da computação em nuvem definidas pelo NIST.

A virtualização viabiliza o agrupamento de recursos, mas as características são autoatendimento, acesso pela rede, agrupamento, elasticidade e serviço medido.

3 E

No modelo PaaS, o cliente controla o sistema operacional e o armazenamento da plataforma em que suas aplicações são executadas.

No PaaS, o cliente controla as aplicações e, possivelmente, configurações do ambiente; sistema operacional e armazenamento ficam com o provedor.

> **Portaria SGD/MGI 5.950/2023, Anexo I, item 2.1, alínea y**
> "O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, **sistema operacional ou armazenamento**, mas tem controle sobre as aplicações instaladas [...]"

4 C

No modelo IaaS, o cliente tem controle sobre os sistemas operacionais e os aplicativos instalados, mas não sobre a infraestrutura física subjacente.

É a definição da Portaria 5.950/2023, alínea x.

> **Portaria SGD/MGI 5.950/2023, Anexo I, item 2.1, alínea x**
> "O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, mas **tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados** [...]"

5 E

A nuvem privada, por definição, deve estar instalada nas dependências físicas do órgão que a utiliza.

A propriedade e o gerenciamento podem ser de terceiros; o que a define é o uso exclusivo.

> **IN GSI/PR 5/2021, art. 3º, I**
> "nuvem privada (ou interna) - infraestrutura de nuvem dedicada para uso exclusivo do órgão [...] e sua propriedade e seu gerenciamento podem ser da própria organização, **de terceiros ou de ambos**;"

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

6 C

Na nuvem híbrida, as infraestruturas que a compõem permanecem distintas, mas são agrupadas por tecnologia padrão que permite a portabilidade de dados e aplicações.

É a definição do art. 3º, IV, da IN GSI/PR 5/2021.

> **IN GSI/PR 5/2021, art. 3º, IV**
> "nuvem híbrida - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas [...], que **permanecem com suas próprias características**, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações."

7 E

Segundo a IN GSI/PR 5/2021, os sistemas estruturantes podem ser hospedados em nuvem pública, desde que mantida cópia de segurança no Brasil.

Só nuvem privada ou comunitária restrita às infraestruturas de órgãos ou entidades (art. 11, IV).

> **IN GSI/PR 5/2021, art. 11, IV**
> "utilizar, para os sistemas estruturantes, **somente os modelos de implementação de nuvem privada ou de nuvem comunitária**, desde que restritas às infraestruturas de órgãos ou de entidades;"

8 E

No modelo SaaS, a responsabilidade pelos dados armazenados e pela gestão dos acessos dos usuários passa integralmente ao provedor.

Os dados, as identidades e as permissões continuam com o cliente em qualquer modelo.

> **SGD, Guia Complementar de Segurança da Informação para Computação em Nuvem, controle 1**
> "SaaS - Não se aplica à organização, pois SaaS e FaaS estão categorizados como soluções de software. O CSP é responsável por tudo, **exceto pelos dados**."

9 E

O emparelhamento (peering) entre redes virtuais é transitivo: se a rede A está emparelhada com B e B com C, A alcança C por meio de B.

O emparelhamento não é transitivo; para isso se usa um centro de trânsito (hub).

10 C

A conexão por enlace dedicado entre o data center do órgão e o provedor de nuvem não trafega pela internet pública.

É um circuito privado; a VPN site a site é que usa a internet, com túnel cifrado.

11 E

A escalabilidade vertical consiste em acrescentar novas instâncias da aplicação, de modo a distribuir a carga entre elas.

Isso é a escalabilidade horizontal; a vertical aumenta os recursos da mesma máquina.

12 C

A elasticidade permite que os recursos sejam reduzidos automaticamente quando a demanda diminui.

Elasticidade é o ajuste nos dois sentidos, acompanhando a demanda.

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

13 C

A Portaria SGD/MGI 5.950/2023 recomenda considerar o uso de contêineres como forma de mitigar o aprisionamento tecnológico.

Item 8.2, alínea b, do Anexo I.

> **Portaria SGD/MGI 5.950/2023, Anexo I, item 8.2, alínea b**
> "Como forma de mitigar os riscos de dependência tecnológica ou aprisionamento (lock-in) [...] b) **considerar o uso de tecnologia de contêineres**, de forma a facilitar a implantação padronizada de soluções;"

14 E

A disponibilidade de um serviço que depende, em série, de cinco componentes com 99,9% de disponibilidade cada é de 99,9%.

Em série, as disponibilidades se multiplicam: 0,999 elevado a 5 dá cerca de 99,5%.

15 C

Pela IN GSI/PR 5/2021, o órgão deve adotar identidade federada para autenticação única no provedor, negando a este o acesso direto ao seu ambiente de autenticação.

Art. 13, I e II.

> **IN GSI/PR 5/2021, art. 13, I e II**
> "I - adotar um padrão de **identidade federada** para permitir o uso de tecnologia single sign-on [...]; II - **negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação** do órgão ou da entidade;"

≡ Documentação oficial, normas e fontes

Documentação oficial e normas

- NIST, SP 800-145, The NIST Definition of Cloud Computing (características, modelos de serviço e de implantação), SP 500-292, Cloud Computing Reference Architecture (atores, inclusive o cloud broker) e SP 800-146, Cloud Computing Synopsis and Recommendations.
- Portaria SGD/MGI 5.950/2023, modelo de contratação de software e de serviços de computação em nuvem: art. 4º; Anexo I, itens 2.1 (definições), 5.4 (direcionadores por sigilo da informação), 8 (continuidade e aprisionamento), 10.2 (segurança) e 25 (governança com integrador e matriz de responsabilidades).
- IN GSI/PR 5/2021, requisitos mínimos de segurança para o uso de nuvem: arts. 3º (modelos de implantação), 11 (antes de migrar), 13 a 19 (identidade, criptografia, segregação, gerenciamento, tratamento e localização da informação, cláusulas) e 20 a 25 (provedor e integrador).
- Portaria Normativa SE-CGU 223/2025, provisionamento de nuvem pública na CGU: art. 2º (definições) e art. 3º (princípios, inclusive multinuvem). IN SGD/ME 94/2022, Anexo I, item 4 (nuvem como regra para nova infraestrutura de centro de dados).
- SGD, Guia Complementar de Segurança da Informação para Computação em Nuvem, PPSI 2.0 (2025): conceitos (p. 12 a 14) e responsabilidade do órgão em cada controle e modelo de serviço. SGD, relatório técnico Boas práticas para minimizar o aprisionamento (lock-in) em nuvem (2024).

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

- MGI, Estratégia de Uso de Software e de Serviços de Computação em Nuvem (Resolução CGDSI/MGI 13/2025): art. 7º (preferência pela nuvem híbrida sem maturidade suficiente) e art. 12 (cloud first, lift and shift como último recurso, integrador multinuvem).
- Documentação dos provedores sobre redes virtuais e responsabilidade compartilhada, em português: AWS, modelo de responsabilidade compartilhada; Microsoft, responsabilidade compartilhada na nuvem; AWS, blocos CIDR de sub-redes (os cinco endereços reservados).

Jurisprudência e entendimentos

- TCU, Acórdão 157/2024-Plenário: acompanhamento da contratação conjunta de serviços de nuvem por TCU, CGU e CNJ (riscos de gestão e fiscalização, catálogo aberto de serviços de terceiros e falta de memória de cálculo; a CGU revisou o orçamento de R$ 164 milhões para R$ 84 milhões).
- TCU, Acórdão 292/2025-Plenário: contratação centralizada de nuvem pelo MGI via integrador multinuvem (riscos de níveis de serviço, fiscalização do integrador e indefinição da responsabilidade compartilhada entre provedor e integrador).

Atividades sugeridas do curso e do TEC neste tópico

Curso e aula	Páginas	Foco
Redes de Computadores e Segurança da Informação para CGU (TI, Infraestrutura de TI) · Capítulo 10 (Computação em nuvem: modelos e arquitetura de nuvem)	previsto para 01/11/2026	Modelos de serviço e de implantação, arquitetura de nuvem
Sistemas Operacionais para CGU (TI, Infraestrutura de TI) · Capítulo 5 (Armazenamento)	p. 5 a 8	Data center próprio e nuvem, escalabilidade vertical e horizontal

Links do Estratégia: o LDI (Livro Digital Interativo) de cada curso, no objetivo da área. As páginas são as do PDF do capítulo baixado no botão Baixar curso do LDI, versão Completo.

Cadernos do TEC

Caderno	Assuntos cobrados (questões do Cebraspe em cada um)
Caderno do tópico, 302 questões tecconcursos.com.br/s/Q4pFIh	Cloud Computing (Computação em Nuvem) (302).

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Quem escreveu isso

Meu nome é Pietro Viecili. Auditor Federal de Finanças e Controle. aprovado em 2º lugar na CGU. Sou pai de 4 crianças e não abro mão da convivência com elas.

Em 1º de abril de 2022 eu recebi o salário às 10h da manhã. Às 15h44 eu tinha pouco mais de 1 real na conta. A luz estava atrasada há dois meses. a água no gato. a internet já cortada. Eu tinha ganhado uma passagem para fazer a prova da CGE-MS e não tinha dinheiro para chegar no aeroporto. Já era pai. e tinha acabado de fazer a prova da CGU sem saber o resultado.

Antes daquele dia eu estudei numa tábua de passar roupa. porque não tinha mesa. e dormia num colchonete no chão. Estudava de madrugada. no Natal. com bebê no colo. Foram 7 reprovações. Uma por 0.05 ponto. Outra porque eu troquei a folha de resposta da discursiva.

A virada não foi esforço. Eu já estava no limite. Foi parar de tratar concurso como prova de resistência e começar a estudar como atleta: estratégia. análise. planejamento e periodização. Veio o 2º lugar na CGU. o 1º no TJ-RO e na DPE-RO. a PF e a FAB. São 7 aprovações em 14 concursos. e hoje mais de 150 mentorados acompanhados com esse método.



Escrevi estes 143 resumos com o edital aberto item por item e as fontes oficiais do lado: o Manual de Orientações Técnicas. as instruções normativas da Secretaria Federal de Controle. a Lei 14.133. a Lei de Acesso à Informação. as normas de integridade pública e privada. os materiais da Escola Virtual de Governo e. nos resumos de TI. a documentação oficial das tecnologias cobradas. São 2.113 citações literais. cada uma conferida no texto oficial e com o artigo ou a página de onde saiu, porque é dali que o Cebraspe tira a frase e troca uma palavra.

Em 121 dos 143 tópicos existe pelo menos uma seção que você não vai achar em aula nenhuma. Essas eu precisei escrever do zero.

Você não nasceu pra ser mais um.
Nasceu pra ser o ZeroUm.

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Você já tem o conteúdo certo

Os resumos te dão o recorte do edital e o conteúdo do jeito que a banca cobra. O que eles não decidem é a terça-feira. Quando o trabalho atropela a semana, quando o simulado volta com 54% e você não sabe qual das 13 disciplinas atacar primeiro, quando falta um mês e meio e você precisa escolher o que vai abandonar. Material nenhum decide isso por você, porque a decisão depende da sua rotina, do seu histórico de acerto e da sua data.

É isso que eu faço na Mentoria Pós-Edital CGU, com você, até 13 de dezembro:

- plano montado sobre este edital e sobre a sua rotina real, com meta diária de teoria, questão e revisão
- periodização até o pico na data da prova, do jeito que atleta treina para competição
- plantão de dúvidas e acesso direto a mim no WhatsApp
- módulo de discursiva, que vale metade da nota da prova
- Assinatura Premium do Estratégia Concursos inclusa

Dois meses, R$ 797 com a assinatura do Estratégia inclusa, ou R$ 627 sem ela.

O que você pagou por este material é abatido integralmente. Me chame no WhatsApp, confiro seu pedido e aplico o crédito.

Chamar o Pietro no WhatsApp

Silêncio e trabalho. VAMO.

AMOSTRA

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui

Esta foi uma amostra completa

Você acabou de ler um dos 143 resumos do Resumo Completo CGU, inteiro, do jeito que o aluno recebe: o recorte exato do edital, as citações literais conferidas na norma, os quadros do Cebraspe, as questões com gabarito e os cadernos do TEC.

O material completo cobre a P1 e a P2, iguais para todos, e as quatro P3: Auditoria, Ciência de Dados, Infraestrutura e Desenvolvimento. São mais de 2.100 citações literais e 3.053 questões com gabarito.

Só o Resumo Completo CGU

Os 143 resumos por R$ 197 à vista ou 12x de R$ 20,37.

Quero o Resumo Completo CGU

Missão CGU, com o Resumo incluso

Dois meses de mentoria individual até a prova, com plano de estudos, reuniões semanais, acesso a mim pelo WhatsApp, 3 simulados no formato Cebraspe e os 143 resumos inclusos. A partir de R$ 627 à vista.

Quero a Missão CGU

Ficou com dúvida? Me chame no WhatsApp.

Silêncio e trabalho. VAMO.

AMOSTRA

Resumo Completo CGU · Edição 2026

Mentoria ZeroUm

AMOSTRA · Resumo Completo CGU · material completo do tópico, sem cortes · garanta o seu aqui