Guia Complementar de Segurança da Informação para Computação em Nuvem

Programa de Privacidade e Segurança da Informação
PPSI 2.0

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Versão 1.1
Brasília, novembro de 2025

GUIA COMPLEMENTAR DE SEGURANÇA DA INFORMAÇÃO PARA COMPUTAÇÃO EM NUVEM

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Marta Juvina de Medeiros

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Adriano de Andrade Moura

Anderson Souza de Araújo

Leonard Keyzo Yamaoka Batista

Raphael César Estevão

Rejane Monique Brelaz Castro

Ricardo Borges Almeida

Rogério Vinícius Matos Rocha

Thainan Cardoso Rezende

Histórico de versões

Data	Versão	Descrição	Autor
31/10/2025	1.0	1ª versão do Guia Complementar de Segurança da Informação para Computação em Nuvem	Equipe Técnica de Elaboração
13/11/2025	1.1	Complementação da introdução. Exclusão da seção Considerações Gerais. Ajustes de formatação.	Equipe Técnica de Elaboração

Sumário

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

1 Termos e definições

Os termos e definições a seguir foram traduzidos a partir do CIS *Controls Guide* v8.1 e adaptados ao contexto da Administração Pública federal, sendo adotados neste guia objetivando alinhamento entre os escopos de aplicação das medidas de segurança da informação [1]. Demais termos utilizados neste guia e respectivo *framework* podem ser encontrados na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 ou no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) aprovado pela Portaria nº 93, de 26 de setembro de 2019.

- **Ativos institucionais**: ativos com potencial de tratar dados, incluindo dispositivos de usuário final, dispositivos de rede, dispositivos da Internet das Coisas (*Internet of Things*, IoT) e não computacionais e servidores em ambientes virtuais, baseados em nuvem e físicos.
  - **Dispositivos de rede**: dispositivos eletrônicos essenciais para comunicação e interação entre dispositivos em uma rede de computadores. Incluem pontos de acesso sem fio, *firewalls*, *gateways*, roteadores e *switches*. Podem ser *hardware* físico, dispositivos virtuais ou baseados em nuvem.
  - **Dispositivos de usuário final**: ativos institucionais utilizados por agentes públicos de uma organização. Incluem *desktops*, estações de trabalho, assim como dispositivos portáteis e móveis, como *notebooks*, *smartphones* e *tablets*.
  - **Internet das Coisas (IoT) e dispositivos não computacionais**: dispositivos com sensores, *software* e outras tecnologias que podem conectar, armazenar e trocar dados com outros dispositivos e sistemas. A conexão com a internet pode ser intermitente, inexistente ou persistente. Exemplos incluem *smartwatches* e outros dispositivos vestíveis, impressoras, telas inteligentes, dispositivos para casa inteligente, alto-falantes, sistemas de controle industrial e sensores de segurança física.
  - **Servidores**: dispositivo ou sistema que fornece recursos, dados, serviços ou programas a outros dispositivos em uma rede local (*Local Area Network*, LAN) ou rede ampla (*Wide Area Network*, WAN). Servidores podem fornecer recursos e usá-los simultaneamente de outro sistema. Podem existir em *datacenters*, nuvens públicas, privadas ou híbridas, incluindo *containers* temporários ou *workloads serverless*. Exemplos incluem servidores *web*, servidores de aplicação, servidores de *e-mail* e servidores de arquivos.
- **Mídias removíveis**: qualquer tipo de dispositivo de armazenamento que pode ser removido de um computador enquanto o sistema está funcionando e permite movimentação de dados entre sistemas. Exemplos incluem CDs, DVDs, discos *blu-ray*, discos rígidos externos, cartões SD, *backups* em fita, disquetes e *drives* USB.
- **Soluções de *software***: conjuntos de dados e instruções usadas para direcionar um computador a realizar tarefas específicas. Soluções de *software* incluem sistemas operacionais e aplicações, ambos podendo incluir serviços, bibliotecas ou interfaces de programação de aplicações (APIs).

- **Aplicações**: programas ou grupos de programas que rodam sobre um sistema operacional hospedado em ativos institucionais. Exemplos: aplicação *web*, banco de dados, baseada em nuvem e móvel.
- **Sistemas operacionais**: soluções de *software* que executam em ativos institucionais para gerenciar *hardware* e recursos de *software*, fornecendo serviços comuns para programas. Exemplos: Windows, Ubuntu, MacOS, Android, z/OS.
  - **Serviços**: programas especializados que executam tarefas críticas definidas para o sistema operacional, frequentemente iniciados com o sistema, atuando em segundo plano e podendo ser iniciados e parados por usuários. Exemplos: gerenciamento de comunicações de rede, usuários, permissões de arquivos, segurança do sistema e interação com dispositivos.
  - **Biblioteca**: base de código pré-compilada e compartilhável que inclui classes, procedimentos, *scripts*, dados de configuração, usada para desenvolver programas e aplicações. Projetada para ajudar programadores e compiladores a construir e executar software eficientemente.
  - **Interface de Programação de Aplicação (*Application Programming Interface*, API)**: conjunto de regras e interfaces que permitem a interação padronizada entre componentes de *software*, facilitando o acesso e comunicação com recursos internos e externos.
- ***Firmware***: soluções *de software* armazenadas na memória não volátil do dispositivo, como ROM ou memória *flash*, que permitem comunicação entre diferentes tipos de *hardware* e sistema operacional. Geralmente atualizadas fora do processo de atualização do sistema operacional e aplicações da organização.

- **Dados:** conjunto de fatos que podem ser examinados, considerados e usados para tomada de decisão. Embora os dados possam ser físicos, o CIS *Controls* foca principalmente na proteção dos dados digitais armazenados, transferidos e processados por ativos institucionais.
  - **Dados críticos**: dados físicos ou digitais armazenados, processados ou geridos pela organização que devem ser mantidos privados, precisos, confiáveis e disponíveis. Caso publicizados, acessados por pessoas sem autorização ou destruídos indevidamente, podem causar danos à organização, seja por violação ou desrespeito a políticas, contratos ou regulamentos.
  - ***Log***: um *log* de eventos, ou simplesmente *log*, é uma coleção ordenada de registros de eventos. Termos como "*log* de dados", "*log* de atividades" e "arquivo de *log*" são frequentemente usados para se referir a "*log*". Os *logs* podem ser persistentes, como um arquivo armazenado em disco, ou podem ser transitórios, como um fluxo de registros de eventos fornecido a um signatário por meio de uma rede. Exemplos: *logs* de sistema operacional, detecção de *antimalware*, base de dados, aplicação, rede, *firewall*, servidor *web* ou controle de acesso. Existem dois tipos de *logs* que geralmente são tratados e

frequentemente configurados de forma independente: *logs* de sistema e *logs* de auditoria.

- ***Logs* de sistema**: normalmente fornecem eventos em nível de sistema que mostram, por exemplo, horários de início e fim de diversos processos do sistema, falhas, entre outros. Esses *logs* são nativos dos sistemas e exigem menos configuração para serem ativados.
- ***Logs* de auditoria**: frequentemente incluem eventos em nível de usuário – como quando um usuário fez *login* ou acessou um arquivo – e requerem mais planejamento e esforço para serem configurados. Estes *logs* geralmente contêm registros de eventos relevantes para a segurança.

- **Dados físicos**: dados armazenados em documentos físicos (ex: papel) ou mídias removíveis físicas (ex: *drives* USB, *backups* em fita).

- **Usuários:** agentes públicos, fornecedores terceirizados, contratados, prestadores de serviços, consultores ou qualquer pessoa autorizada a acessar ativos institucionais, incluindo contas de usuários, administradores e serviços.
  - **Prestadores de serviço**: entidades que oferecem plataformas, soluções de *software* e serviços a outras organizações. Exemplos: consultores de TI, provedores de serviço gerenciado (*Managed Service Provider*, MSP), plataformas de soluções de *software* como serviço e provedores de serviços em nuvem. Incluem prestadores terceirizados e fornecedores, pagos ou gratuitos.
  - **Contas de usuário**: identidade composta por credenciais (ex: nome de usuário, senha) que define um usuário em um sistema. Controla arquivos, pastas e recursos acessíveis e tarefas permitidas. Para este documento, refere-se a contas padrão com privilégios limitados para atividades gerais.
  - **Contas de administrador**: contas para usuários com privilégios elevados, usadas para gerenciar *aspectos* do computador, domínio ou infraestrutura de TI. Cada conta deve ser vinculada a um usuário único. Exemplos: contas *root*, administrador local, administrador de domínio, contas administrativas de rede ou dispositivos de segurança.
  - **Contas de serviço**: criadas especificamente para executar aplicações, serviços e tarefas automatizadas no sistema operacional. Podem existir somente para possuir dados e arquivos de configuração. Cada conta tem um dono responsável. Não devem ser usadas para computação geral.
- **Rede:** conjunto de dispositivos interconectados que troca dados. Rede é um conjunto mais amplo que infraestrutura e arquitetura de rede.
  - **Infraestrutura de rede**: conjunto de recursos que fornecem conectividade, gestão, operações de negócio e comunicação. Inclui *hardware*, soluções de *software*, sistemas e dispositivos físicos, virtuais e em nuvem, permitindo comunicação entre usuários, serviços, aplicações e processos.

- **Arquitetura de rede**: desenho físico e lógico de uma rede, definindo organização, conexões entre dispositivos e soluções de *software*, e os dados transmitidos. Deve incluir diagramas da arquitetura de rede e de segurança.

- **Documentação:** políticas, normas, procedimentos, processos, planos, diagramas e outros materiais escritos, físicos ou digitais. Exemplos: métodos de governança, processos adotados pelos usuários ou diagramas da arquitetura de rede.
  - **Plano**: documento que implementa políticas e pode incluir grupos de políticas, normas, procedimentos e processos.
  - **Política**: declaração oficial de governança que define objetivos específicos de um programa.
  - **Processo**: conjunto de tarefas e atividades gerais para alcançar objetivos relacionados à segurança.
  - **Procedimento**: conjunto ordenado de etapas que deve ser seguido para cumprir uma tarefa específica, definindo a forma aprovada de agir em ambiente tecnológico e organizacional.

2 Introdução

A computação em nuvem representa um modelo inovador de prestação de serviços de Tecnologia da Informação (TI), que possibilita o acesso sob demanda a recursos tecnológicos, sejam eles compartilhados ou dedicados, incluindo servidores, armazenamento, bancos de dados, redes, *softwares* e plataformas. No âmbito da Administração Pública Federal, a adoção da computação em nuvem tem se revelado fundamental para a modernização dos serviços públicos, a otimização dos recursos, bem como para conferir maior agilidade e flexibilidade à gestão da TI.

Desde 2018, o Governo Federal vem promovendo iniciativas que facilitam a contratação conjunta e o uso compartilhado de serviços de computação em nuvem entre órgãos públicos, incentivando a obtenção de ganhos de escala, o compartilhamento de conhecimento e a disseminação de boas práticas [1].

Apesar dos benefícios proporcionados, a adoção da computação em nuvem apresenta diversos desafios, tais como aspectos regulatórios, conformidade legal, governança, interoperabilidade, gestão de contratos e níveis de serviço, além dos riscos relacionados à segurança da informação, que exigem atenção especial [2]. Para mitigar os riscos relacionados à segurança da informação, a Administração Pública Federal observa normativos específicos, notadamente a **Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021**, e a **Instrução Normativa GSI/PR nº 8, de 15 de maio de 2025**, ambas emitidas pelo Gabinete de Segurança Institucional da Presidência da República, além da **Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023**. Complementarmente, a conformidade com a **Lei nº 13.709, de 14 de agosto de 2018** – Lei Geral de Proteção de Dados Pessoais (LGPD) reforça a necessidade de medidas técnicas e administrativas aptas a proteger os dados pessoais independentemente do ambiente computacional.

Nesse contexto, o presente Guia, elaborado para os órgãos da Administração Pública Federal direta, autárquica e fundacional integrantes do SISP, constitui instrumento essencial para a criação de um ambiente seguro e transparente, garantindo a proteção de dados pessoais e o cumprimento rigoroso das normas vigentes, além de fortalecer a confiança pública por meio da consolidação de políticas eficazes de segurança da informação. Sua concepção baseou-se nas demandas específicas desse contexto institucional, alinhando práticas internacionais consolidadas às exigências legais brasileiras, bem como fundamentando-se em pesquisa especializada, análise normativa e consulta a especialistas.

O objetivo é apresentar orientações para garantir a segurança da informação na adoção da computação em nuvem. Este Guia foi construindo de forma complementar ao **Guia do *Framework* de Privacidade e Segurança da Informação do PPSI 2.0**, apresentando uma extensão da aplicabilidade dos controles de segurança da informação voltada para soluções de computação em nuvem.

Para atingir o objetivo acima, primeiramente é apresentada uma contextualização sobre computação em nuvem, incluindo especialmente a descrição dos diferentes modelos de implantação e de serviços da computação em nuvem. Na sequência, são apresentados os controles de segurança da informação oriundos do ***framework* do PPSI 2.0** com a respectiva aplicabilidade de medidas de acordo com o modelo de computação em nuvem e orientações relevantes para apoiar a sua interpretação e implementação. Cada controle é detalhado com uma visão geral, a aplicabilidade na nuvem, a lista de medidas e suas associações com os modelos de serviço na nuvem, as considerações sobre serviços e modelos de implantação em nuvem e as considerações adicionais sobre nuvem. Essa sistematização viabiliza o mapeamento, a implementação e o aperfeiçoamento contínuo das ações institucionais, promovendo conformidade regulatória, maturidade operacional e resiliência organizacional.

3 Conceitos de computação em nuvem

A seção foi inspirada no documento do ***National Institute of Standards and Technology (NIST)*** [3] e tem por objetivo oferecer orientação básica sobre os conceitos relacionados a computação em nuvem, os quais são fundamentais para compreensão da seção seguinte que trata sobre os controles e respectivas medidas de segurança da informação aplicados no contexto da computação em nuvem.

Esta seção está organizada para proporcionar uma compreensão estruturada sobre a computação em nuvem, abordando inicialmente uma definição clara e contextualizada do conceito. Em seguida, exploram-se as características principais que conferem eficiência e flexibilidade à nuvem. Por fim, são apresentados os modelos de implantação e os modelos de serviços em nuvem.

3.1 Definição de computação em nuvem

Segundo Mell e Grance (2011, p. 1), a computação em nuvem é um modelo que permite acesso onipresente, conveniente e sob demanda a um conjunto de recursos computacionais configuráveis - por exemplo, redes, servidores, armazenamento, aplicativos e serviços - que podem ser provisionados e liberados rapidamente com esforço mínimo de gerenciamento ou interação com o provedor de serviços [3].

Essa abordagem viabiliza o uso de serviços flexíveis, escaláveis e eficientes, capazes de ajustar sua capacidade conforme as necessidades, sem comprometer o desempenho. Para a Administração Pública Federal, a computação em nuvem representa uma estratégia fundamental para redução de investimentos em infraestrutura física, otimização de custos operacionais e promoção da inovação em processos administrativos.

De acordo com o *NIST*, a computação em nuvem é composta por cinco características essenciais, quatro modelos de implantação e três modelos de serviço.

3.2 Características da computação em nuvem

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 [3]. Esses aspectos possibilitam alocação dinâmica de recursos conforme a demanda, autonomia dos gestores para provisionamento rápido, acesso remoto facilitado a partir de diversos dispositivos, ambiente tecnológico compartilhado de forma segura e transparência no uso dos recursos para controle e auditoria. Tais características contribuem para maior eficiência operacional, redução de custos, maior agilidade e inovação na prestação de serviços públicos.

3.3 Modelos de implantação

Os modelos de implantação de computação em nuvem definem como os recursos são estruturados e disponibilizados, influenciando diretamente o controle, a segurança e a gestão dos serviços. Conforme Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) aprovado pela Portaria nº 93, de 26 de setembro de 2019, os principais modelos são:

- **Nuvem privada:** Infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários. A sua propriedade, gerenciamento e operação podem ser da própria organização, de terceiros ou de ambos e pode existir dentro ou fora das suas instalações.

- **Nuvem comunitária:** Esse modelo é uma 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. Ela pode ser de propriedade, gerenciada e operada por organizações da comunidade, por terceiros ou ambos, bem como pode existir interna ou externamente às suas instalações.

- **Nuvem pública:** Infraestrutura de nuvem dedicada para uso aberto ao público em geral. A propriedade, o gerenciamento e a operação podem ser de organizações públicas, privadas ou de ambas. O ambiente computacional existe nas instalações do provedor de nuvem.

- **Nuvem híbrida:** Trata-se de uma 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.

3.4 Modelos de serviços

Os modelos de serviços em computação em nuvem são formas de entrega de recursos e soluções tecnológicas que definem o nível de abstração e responsabilidade entre o provedor de nuvem e o cliente. Eles indicam o que exatamente está sendo oferecido como serviço e até onde vai o gerenciamento do cliente. O ***Center for Internet Security* (*CIS*)** apresenta os seguintes modelos no documento [4]:

- **Infraestrutura como Serviço (*IaaS*):** O *IaaS* disponibiliza recursos computacionais, como servidores virtuais, armazenamento, redes e outras infraestruturas essenciais sob demanda. O órgão ou entidade pública utiliza seu próprio software, como sistemas operacionais, *middleware* e aplicativos. A infraestrutura de nuvem subjacente é gerenciada pelo provedor de serviço em nuvem.

- **Plataforma como Serviço (*PaaS*):** O *PaaS* oferece um ambiente completo para desenvolvimento, teste e implantação de aplicações, liberando os desenvolvedores das

preocupações com gerenciamento da infraestrutura subjacente, como servidores, armazenamento e redes.

- ***Software* como Serviço (*SaaS*):** *SaaS* é uma solução de software de computação em nuvem que fornece ao consumidor acesso a um produto de software completo. A solução de software reside em um ambiente de nuvem e é acessada pelo consumidor pela *web* ou por uma interface de programação de aplicativo (*API*). O cliente pode utilizar a solução de *software* para armazenar e analisar dados sem precisar se preocupar com o gerenciamento da infraestrutura, do serviço ou do *software*, pois essa responsabilidade é do provedor.

- **Função como Serviço (*FaaS*):** O *FaaS* permite que funções específicas sejam executadas na nuvem em resposta a eventos, sem que o cliente precise se preocupar com a gestão da infraestrutura.

4 Controles de segurança da informação para computação em nuvem

Esta seção foi concebida como uma extensão dos controles de segurança da informação definidos no ***Framework* de Privacidade e Segurança da Informação do PPSI 2.0**, o qual possui como base o ***CIS Controls*® v8.1**, formalmente conhecido como *CIS Critical Security Controls*® [5]. Dessa forma, a seção mantém a coerência conceitual com o ***framework* do PPSI 2.**0, ao mesmo tempo em que integra as melhores práticas de segurança recomendadas pelo *CIS*.

Considerando a crescente adoção de serviços em nuvem e as particularidades desse modelo de provisão tecnológica, esta seção tem por objetivo adaptar os controles do PPSI 2.0 ao contexto da computação em nuvem, oferecendo orientações sobre como interpretar e aplicar cada controle sob a perspectiva do órgão ou entidade pública cliente desses serviços.

O desenvolvimento desta abordagem tomou como principal referência o ***CIS Cloud Companion Guide*** [4], documento que fornece diretrizes práticas para a aplicação dos ***CIS Controls* v8.1** em diferentes tipos de ambientes de computação em nuvem. Esse guia apresenta a interpretação de cada controle à luz das responsabilidades do cliente, destacando diferenças em relação aos ambientes tradicionais de TI e incorporando considerações específicas para o contexto de nuvem.

A seguir, serão apresentados os controles de segurança da informação, incluindo a visão geral, descrição sobre a aplicabilidade na nuvem do controle, a lista de medidas relacionadas junto ao seu Grupo de Implementação (*GI*) e respectiva aplicabilidade na computação em nuvem e considerações sobre serviços e modelos de implantação em nuvem.

4.1 CONTROLE 1: Inventário de ativos institucionais

Visão geral

Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/Internet das Coisas (*IoT*); e servidores) conectados à infraestrutura física, virtual e remotamente, além daqueles em ambientes de nuvem, para conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos na organização. Isso também ajudará a identificar ativos não autorizados e não gerenciados objetivando remoção ou remediação.

Aplicabilidade na nuvem

O primeiro Controle *CIS* é considerado o mais importante porque é necessário primeiro identificar os sistemas e dispositivos que precisam ser protegidos. O Controle *CIS* 1 trata de fazer um inventário e controle de ativos institucionais. Compreender e resolver o problema do

inventário de ativos institucionais e da visibilidade dos dispositivos é fundamental para gerenciar um programa de segurança organizacional. Isso se torna desafiador em ambientes de nuvem devido à responsabilidade compartilhada da segurança e ao modelo de serviço em nuvem utilizado.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
1.1	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	GI1	IaaS	PaaS	SaaS	FaaS
1.2	O órgão trata ativos institucionais não autorizados?	GI1	IaaS	PaaS	N/A	N/A
1.3	O órgão usa ferramenta de descoberta ativa para identificação de ativos institucionais?	GI2	IaaS	PaaS	N/A	N/A
1.4	O órgão usa o protocolo de configuração dinâmica de host (*Dynamic Host Configuration Protocol*, DHCP) para atualizar o inventário de ativos institucionais?	GI2	N/A	N/A	N/A	N/A
1.5	O órgão usa ferramenta de descoberta passiva para identificação de ativos institucionais?	GI3	N/A	N/A	N/A	N/A

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle CIS e suas medidas são aplicáveis ao modelo Privado (local / on-premises). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação utilizados pela organização.

- **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).
- ***PaaS*** - A organização gerencia o desenvolvimento, os testes e a implantação de suas aplicações. Ele tem controle total sobre os aplicativos e, em alguns casos, sobre as configurações do ambiente de hospedagem e os sistemas operacionais. O *CSP* é responsável pelos servidores físicos, rede física, armazenamento, hipervisor e sistemas operacionais. O registro *DHCP* e o controle de acesso em nível de porta podem não ser aplicáveis.

- ***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.
- ***FaaS*** - Não se aplica à organização, pois *SaaS* e *FaaS* estão categorizados como soluções de software. O *CSP* é responsável por tudo, exceto pelos dados.

Considerações adicionais sobre nuvem

- Em um ambiente de nuvem, os ativos institucionais nos modelos de serviço Privado, *IaaS* ou *PaaS* são virtuais e podem estar na forma de máquinas virtuais, redes virtuais, *switches* virtuais, etc., com exceções limitadas, como modelos dedicados de segurança de *hardware* (*HSMs*).
- Devido à natureza dos sistemas virtuais e à facilidade de colocar online um novo ativo virtual, é imprescindível manter uma lista abrangente de todos os ativos institucionais de *hardware* em nuvem gerenciados pelo órgão ou entidade.
- Sempre cabe à organização solicitar documentação que descreva como o *CSP* está protegendo a infraestrutura e a tecnologia que estão sob sua responsabilidade.
- Ao coletar o inventário de ativos institucionais, deve-se considerar a criticidade deste ativo, o sistema operacional e versão, quando o ativo institucional foi descoberto e a etiqueta deste ativo, se aplicável.

4.2 CONTROLE 2: Inventário de soluções de *software*

Visão geral

Gerenciar ativamente (inventariar, rastrear e corrigir) todas as soluções de *software* na rede para que somente as autorizadas sejam instaladas e possam ser executadas, e que as não autorizadas ou não gerenciadas sejam encontradas e impedidas de serem instaladas ou executadas.

Aplicabilidade na nuvem

O segundo Controle *CIS* oferece as orientações necessárias para identificar, rastrear e registrar todas as soluções de *softwares* utilizados em um ambiente. Isso representa um desafio em ambientes de nuvem, devido à responsabilidade de segurança compartilhada e ao modelo de serviço em nuvem utilizado.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
2.1	O órgão estabelece e mantém um inventário de soluções de software?	GI1	IaaS	PaaS	SaaS	FaaS

2.2	O órgão mantém em seu ambiente computacional apenas soluções de software suportadas pelos seus fornecedores?	GI1	IaaS	PaaS	SaaS	N/A
2.3	O órgão trata o uso de soluções de software não autorizadas?	GI1	IaaS	PaaS	SaaS	FaaS
2.4	O órgão utiliza ferramentas automatizadas de inventário de soluções de software?	GI2	IaaS	PaaS	SaaS	N/A
2.5	O órgão possui uma lista de soluções de software autorizadas?	GI2	IaaS	PaaS	N/A	N/A
2.6	O órgão possui uma lista de bibliotecas de software autorizadas?	GI2	IaaS	PaaS	N/A	N/A
2.7	O órgão possui uma lista de scripts autorizados?	GI3	IaaS	PaaS	N/A	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle CIS e suas medidas são aplicáveis ao modelo Privado (local / on-premises). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratados pela organização.

- **Privado (on-premises) -** A organização é responsável por manter o inventário de todo o *software* utilizado, independentemente do modelo de serviço.
- ***IaaS* -** A organização implanta, opera e mantém o *software* utilizado dentro desse modelo de serviço, mas não gerencia o *software* subjacente da nuvem, como o hipervisor, os sistemas operacionais ou os aplicativos que fornecem serviços específicos, pois essa é uma responsabilidade do CSP.
- ***PaaS* -** A organização gerencia o desenvolvimento, os testes e a implantação de seu *software* e aplicações. Ela possui controle total sobre os aplicativos e, em alguns casos, sobre os sistemas operacionais, sendo, portanto, responsável por todo o *software* em execução nesse nível. O *CSP* é responsável pelo hipervisor, pelos sistemas operacionais e por outros aplicativos que fornecem o serviço. Práticas como lista de permissões (*whitelisting*) de aplicativos, bibliotecas, *scripts* e segregação de aplicativos de alto risco podem não ser aplicáveis a todos os modelos de serviço *PaaS*.
- ***SaaS* -** A organização é responsável por registrar o *software* na lista de inventário como aprovado. Também é sua responsabilidade verificar se o fornecedor ainda oferece suporte e atualizações para o *software* e manter esse registro no inventário de *software*. O rastreamento do inventário de *software* pode ser feito manualmente.
- ***FaaS* -** A organização é responsável por manter um inventário do software autorizado. O rastreamento do inventário de software pode ser feito manualmente.

Considerações adicionais sobre nuvem

- Em um ambiente de nuvem, seja Privado, *IaaS*, *PaaS*, *SaaS* ou *FaaS*, o *software* utilizado e mantido deve ser inventariado, atualizado com *patches* e monitorado quando aplicável.
- É imprescindível manter uma lista abrangente dessas soluções de *software* em nuvem para identificar e mitigar quaisquer vulnerabilidades e proteger os dados associados ao *software* que a organização gerencia.
- Sempre cabe à organização solicitar documentação ao *CSP* detalhando suas responsabilidades e como o *CSP* está protegendo a infraestrutura e tecnologia.
- Além disso, como parte do inventário de *software*, a organização deve incluir os pontos finais de *API* (*API endpoints*).
- Para *PaaS* com serviços gerenciados de *Kubernetes*, a organização é responsável pelas atualizações/*patches* nos Nós de Trabalho (*Worker Nodes*).
- Capacidades de descoberta e inventário devem se estender ao *software* que roda dentro de *containers* (no caso de *Containers-as-a-Service* - *CaaS*). *CaaS* é considerado um subconjunto de *IaaS* e fica entre *IaaS* e *PaaS*.
- Se os *containers* forem considerados como *FaaS*, então o *CSP* frequentemente não é responsável pela segurança destes *containers* ou dos microsserviços que rodam dentro deles.

4.3 CONTROLE 3: Proteção de dados

Visão geral

Aplicar processos e controles técnicos para identificar, categorizar, utilizar, reter e descartar dados com segurança, garantindo a proteção dos dados ao longo de todo o seu ciclo de vida.

Aplicabilidade na nuvem

O foco deste Controle *CIS* é a proteção dos dados críticos à organização, por meio da confidencialidade, integridade e disponibilidade, além da garantia da privacidade. O ambiente de nuvem não é uma exceção quando se trata de dados privados. Se há algo que as organizações perceberam ao migrar seus dados para a nuvem, é que protegê-los pode ser bem mais complicado do que se pode imaginar. Essa é uma preocupação crescente tanto para os *CSPs* quanto para as organizações, pois vazamentos de dados podem permanecer sem detecção por longos períodos.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
3.1	O órgão estabelece e mantém um processo de gestão de dados?	GI1	IaaS	PaaS	SaaS	FaaS

3.2	O órgão estabelece e mantém um inventário de dados?	GI1	IaaS	PaaS	SaaS	FaaS
3.3	O órgão configura listas de controle de acesso a dados?	GI1	IaaS	PaaS	SaaS	FaaS
3.4	O órgão aplica retenção de dados?	GI1	IaaS	PaaS	SaaS	FaaS
3.5	O órgão descarta dados com segurança?	GI1	IaaS	PaaS	SaaS	FaaS
3.6	O órgão criptografa dados críticos em dispositivos de usuário final?	GI1	IaaS	PaaS	N/A	N/A
3.7	O órgão estabelece e mantém um esquema de classificação de dados?	GI2	IaaS	PaaS	SaaS	FaaS
3.8	O órgão documenta os fluxos de dados?	GI2	IaaS	PaaS	SaaS	FaaS
3.9	O órgão criptografa dados críticos em mídia removível?	GI2	N/A	N/A	N/A	N/A
3.10	O órgão criptografa os dados críticos que estão em trânsito?	GI2	IaaS	PaaS	SaaS	FaaS
3.11	O órgão criptografa os dados críticos que estão em repouso?	GI2	IaaS	PaaS	N/A	N/A
3.12	O órgão segmenta o processamento e o armazenamento de dados com base na criticidade?	GI2	IaaS	N/A	N/A	N/A
3.13	O órgão implanta uma solução de prevenção contra perda de dados?	GI3	IaaS	N/A	N/A	N/A
3.14	O órgão registra o acesso aos dados críticos?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle CIS e suas medidas são aplicáveis ao modelo Privado (local / on-premises). Para os modelos Privado (hospedado por terceiros), Público e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável por todos os dados, independentemente do modelo de serviço utilizado.
- ***IaaS*** - A organização é responsável pela proteção dos dados, mas essa responsabilidade se limita às redes virtuais e máquinas virtuais dentro desse modelo de serviço. O *CSP* não é responsável por qualquer perda de dados decorrente da falta de ação ou de medidas de segurança definidas para a organização.

- ***PaaS -*** A organização gerencia os dados e o acesso para as aplicações e, em alguns casos, para as configurações do ambiente de hospedagem e os sistemas operacionais.
- ***SaaS*** - A organização é responsável pelos dados. O *CSP* é responsável apenas por garantir que os dados estejam *online* e que o acesso não seja concedido fora da aplicação controlada pela organização.
- ***FaaS*** - A organização é responsável pelo código e por quaisquer dados. O *CSP* é responsável apenas por garantir que os dados estejam *online* e que o acesso não seja concedido fora das funções chamadas e controladas pela organização.

Considerações adicionais sobre nuvem

- Certifique-se de que os dados não estejam acessíveis ao público. Utilize criptografia ou tokenização para proteger dados críticos à organização. A criptografia tem várias limitações em soluções SaaS e não permite que os dados sejam pesquisados; no entanto, a tokenização resolve essa preocupação e limitação.
- Controle os sistemas e usuários que têm acesso à plataforma de nuvem e aos dados que possam estar expostos. Ao hospedar qualquer dado na nuvem, considere as possíveis implicações legais com base na classificação dos dados. Na maioria das vezes, a proteção, redundância e backup dos dados são responsabilidades da organização e não do CSP.

4.4 CONTROLE 4: Configuração segura de ativos institucionais e soluções de *software*

Visão geral

Estabelecer e manter a configuração segura de dispositivos de usuário final, incluindo portáteis e móveis, dispositivos de rede, dispositivos não computacionais/*IoT* e servidores, além de soluções de *software*.

Aplicabilidade na nuvem

Este Controle *CIS* fornece orientações para a proteção de *hardware* e *software*. Quando fornecidos pelo *CSP*, as configurações padrão de sistemas operacionais e aplicações geralmente são voltadas para a facilidade de implantação e uso, e não para a segurança. Controles básicos, serviços e portas abertas, contas ou senhas padrão, protocolos antigos (vulneráveis), *softwares* pré-instalados desnecessários — todos podem ser explorados em seu estado padrão. Mesmo que uma configuração inicial robusta seja desenvolvida e implantada na nuvem, ela deve ser gerenciada continuamente para evitar desvios de configuração à medida que o *software* é atualizado ou recebe *patches*, novas vulnerabilidades de segurança são reportadas, ou configurações são ajustadas para permitir a instalação de novos *softwares* ou atender a novos requisitos operacionais. Caso contrário, os atacantes encontrarão oportunidades para explorar tanto os serviços acessíveis pela rede quanto os *softwares* cliente.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
4.1	O órgão estabelece e mantém um processo de configuração segura?	GI1	IaaS	PaaS	SaaS	FaaS
4.2	O órgão estabelece e mantém um processo de configuração segura para a infraestrutura de rede?	GI1	IaaS	PaaS	N/A	N/A
4.3	O órgão configura o bloqueio automático de sessão nos ativos institucionais?	GI1	IaaS	PaaS	N/A	N/A
4.4	O órgão implementa e gerencia um *firewall* nos servidores?	GI1	IaaS	PaaS	N/A	N/A
4.5	O órgão implementa e gerencia um *firewall* em dispositivos do usuário final?	GI1	IaaS	PaaS	N/A	N/A
4.6	O órgão gerencia com segurança os ativos institucionais e soluções de software?	GI1	IaaS	PaaS	SaaS	FaaS
4.7	O órgão gerencia contas padrão?	GI1	IaaS	PaaS	SaaS	FaaS
4.8	O órgão desinstala ou desativa serviços desnecessários?	GI2	IaaS	PaaS	N/A	N/A
4.9	O órgão configura servidores Sistema de Nomes de Domínio (*Domain Name System*, DNS) confiáveis?	GI2	IaaS	PaaS	N/A	N/A
4.10	O órgão aplica o recurso de bloqueio automático nos dispositivos portáteis de usuário final?	GI2	IaaS	PaaS	N/A	N/A
4.11	O órgão aplica o recurso de limpeza remota nos dispositivos portáteis de usuário final?	GI2	IaaS	PaaS	N/A	N/A
4.12	O órgão separa os espaços de trabalho nos dispositivos móveis?	GI3	IaaS	PaaS	N/A	N/A

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável por aplicar uma linha de base de segurança para todos os sistemas físicos e virtuais, *softwares* e aplicações.
- ***IaaS*** - A organização é responsável por aplicar uma linha de base de segurança para o *software*, servidores virtuais, rede virtual, *middleware* e aplicações no ambiente de nuvem.
- ***PaaS*** - A organização é responsável por aplicar uma linha de base de segurança para as aplicações e ferramentas de desenvolvimento utilizadas.
- ***SaaS*** - A organização é responsável por aplicar uma linha de base de segurança dentro do *software* e dos dados que estão sendo utilizados.
- ***FaaS*** - A organização é responsável por aplicar uma linha de base de segurança dentro do código e dos dados que estão sendo utilizados.

Considerações adicionais sobre nuvem

- Quando ferramentas de gerenciamento de configuração são usadas, devem ser configuradas para modo de alerta apenas, sem reimplantação automática de configuração, a menos que seja seguro fazê-lo.
- O *CSP* hospeda o armazenamento típico de imagens em ambientes de nuvem para *PaaS*, *SaaS* e *FaaS*; portanto, a configuração segura dos servidores subjacentes é responsabilidade do *CSP*.
- Como parte das configurações seguras estabelecidas, *SaaS* e *FaaS* devem sempre se comunicar via *TLS* e validar o certificado do *endpoint TLS* da *API*.
- Considere também serviços de *broker* de segurança de acesso à nuvem (*CASB*) que podem fornecer controles granulares para monitorar sessões de aplicativos dos usuários e bloquear ações.

4.5 CONTROLE 5: Gestão de contas

Visão geral

Aplicar processos e ferramentas para atribuir e gerenciar autorização para credenciais de contas de usuário e contas de serviços.

Aplicabilidade na nuvem

Este Controle *CIS* tem como foco o gerenciamento do ciclo de vida de contas de sistemas, aplicações e usuários. Como parte desse gerenciamento, devem ser estabelecidas regras e processos para a criação, uso, inatividade e exclusão de todas as contas em nuvem, a fim de minimizar as oportunidades de exploração por atacantes. Quando um colaborador deixa a organização ou muda de função, podem surgir vulnerabilidades se as contas desse colaborador não forem encerradas ou modificadas. Se os privilégios de administrador forem distribuídos de forma ampla ou sem controle, ou se senhas idênticas forem utilizadas em sistemas menos críticos, o atacante terá mais facilidade para obter controle total dos sistemas,

pois haverá muito mais contas disponíveis que podem servir como caminhos para a elevação de privilégios administrativos.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
5.1	O órgão estabelece e mantém um inventário de contas?	GI1	IaaS	PaaS	SaaS	FaaS
5.2	O órgão promove ações para evitar a reutilização de senhas?	GI1	IaaS	PaaS	SaaS	FaaS
5.3	O órgão desabilita ou exclui contas inativas?	GI1	IaaS	PaaS	SaaS	FaaS
5.4	O órgão limita os privilégios de administrador às contas de administrador dedicadas?	GI1	IaaS	PaaS	SaaS	FaaS
5.5	O órgão estabelece e mantém um inventário de contas de serviço?	GI2	IaaS	PaaS	SaaS	FaaS
5.6	O órgão centraliza a gestão de contas?	GI2	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável por todas as contas, independentemente do modelo de serviço utilizado.
- ***IaaS*** - A organização é responsável por todas as contas utilizadas nas redes virtuais, máquinas virtuais, aplicações etc. O *CSP* não é responsável por esse acesso no nível das contas da organização.
- ***PaaS*** - A organização gerencia as contas das aplicações e, em alguns casos, também as contas dos sistemas operacionais hospedeiros.
- ***SaaS*** - A organização é responsável pelas contas de aplicação.
- ***FaaS*** - A organização é responsável pelas contas que têm a capacidade de criar e executar código com base nas funções em nuvem.

Considerações adicionais sobre nuvem

- Para as organizações que operam na nuvem, é ainda mais importante compreender e manter o gerenciamento de contas. A organização é responsável por todas as contas.
- Deve-se seguir o princípio do menor privilégio no gerenciamento de contas, garantindo que cada conta tenha apenas o nível mínimo de acesso necessário para executar suas funções.

4.6 CONTROLE 6: Gestão de acesso

Visão geral

Aplicar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos institucionais.

Aplicabilidade na nuvem

Este Controle *CIS* trata da necessidade de limitar e gerenciar o acesso. O uso indevido de privilégios administrativos é um dos principais métodos para que atacantes se movimentem lateralmente dentro de uma organização-alvo. Uma das duas formas principais para os atacantes se espalharem dentro de um sistema é enganando um usuário com credenciais elevadas para abrir um anexo de *e-mail*, baixar e executar um arquivo infectado, ou visitar um site malicioso a partir de um ativo conectado ao ambiente de nuvem. A segunda técnica comum usada por atacantes é a elevação de privilégios ao adivinhar ou quebrar a senha de um usuário administrador para obter acesso a uma máquina-alvo.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
6.1	O órgão estabelece um processo de concessão de acesso?	GI1	IaaS	PaaS	SaaS	FaaS
6.2	O órgão estabelece um processo de revogação de acesso?	GI1	IaaS	PaaS	SaaS	FaaS
6.3	O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para soluções de software expostas externamente?	GI1	IaaS	PaaS	SaaS	FaaS
6.4	O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para acesso remoto à rede?	GI1	IaaS	N/A	N/A	N/A
6.5	O órgão exige autenticação multifator (*Multi-Factor Authentication*, MFA) para acesso administrativo?	GI1	IaaS	PaaS	SaaS	FaaS

6.6	**O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?**	**GI2**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
6.7	**O órgão centraliza o controle de acesso?**	**GI2**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
6.8	**O órgão define e mantém o controle de acesso baseado em funções?**	**GI3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável por todas as contas, independentemente do modelo de serviço utilizado.
- ***IaaS*** - A organização é responsável por todas as contas utilizadas nas redes virtuais, máquinas virtuais, aplicativos etc. O *CSP* não é responsável por esse acesso no nível das contas da organização.
- ***PaaS*** - A organização gerencia as contas dos aplicativos e, em alguns casos, também as configurações do sistema operacional do *host*.
- ***SaaS*** - A organização é responsável pelas contas dentro do aplicativo.
- ***FaaS*** - A organização é responsável pelas contas que possuem permissão para criar e executar código com base nas funções em nuvem.

Considerações adicionais sobre nuvem

- Para as organizações que operam na nuvem, é ainda mais importante compreender e manter o controle das contas. consumidora organização é responsável por todas as contas e pelos níveis de acesso que essas contas possuem ao seu ambiente em nuvem.
- Sempre que possível, deve-se exigir autenticação multifator (*MFA*). Por padrão, o *PaaS* não permite acesso direto à rede virtual; nesse caso, o *MFA* é limitado ao acesso aos aplicativos, conforme descrito na medida 6.3.
- O uso de contas de serviço compartilhadas deve ser restrito ao mínimo necessário.
- As permissões devem ser concedidas por meio de pertencimento a grupos, pois isso facilita o gerenciamento.
- O controle de acesso baseado em função (*RBAC – Role-Based Access Control*) tornou-se a metodologia principal e é uma capacidade essencial para gerenciar o acesso a recursos baseados em nuvem.

4.7 CONTROLE 7: Gestão contínua de vulnerabilidades

Visão geral

Desenvolver um plano para avaliar e monitorar continuamente vulnerabilidades em todos os ativos institucionais e soluções de software, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar fontes públicas e privadas em busca de novas informações sobre ameaças e vulnerabilidades.

Aplicabilidade na nuvem

O Controle *CIS* aborda a necessidade de gerenciamento contínuo de vulnerabilidades, o que pode ser uma tarefa significativa na maioria das organizações. Compreender e gerenciar vulnerabilidades em um ambiente de nuvem pode ser mais desafiador do que em sistemas tradicionais de TI. Um ambiente em nuvem é dinâmico, permitindo que a infraestrutura organizacional seja dimensionada em um ritmo constantemente variável. Com o uso crescente de *DevSecOps*, o cenário tecnológico interno está sempre mudando. À medida que as organizações migram para a nuvem, eles se encontram em uma posição difícil devido aos riscos e vulnerabilidades associados ao seu uso. Transferir o controle de alguns ativos para um terceiro, dependendo do modelo de implantação utilizado, e verificar o status de segurança e vulnerabilidade desses ativos nem sempre é responsabilidade direta das organizações que utilizam esse serviço. Ambientes em nuvem também hospedam vulnerabilidades específicas desse tipo de tecnologia, que precisam ser continuamente monitoradas e gerenciadas.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
7.1	O órgão estabelece e mantém um processo de gestão de vulnerabilidade?	GI1	IaaS	PaaS	SaaS	FaaS
7.2	O órgão estabelece e mantém um processo de remediação?	GI1	IaaS	PaaS	SaaS	FaaS
7.3	O órgão executa a gestão automatizada de atualizações do sistema operacional?	GI1	IaaS	PaaS	N/A	N/A
7.4	O órgão executa a gestão automatizada de atualizações de aplicações?	GI1	IaaS	PaaS	N/A	FaaS
7.5	O órgão realiza varreduras automatizadas de vulnerabilidades internas?	GI2	IaaS	PaaS	N/A	N/A
7.6	O órgão realiza varreduras automatizadas de vulnerabilidades expostas externamente?	GI2	IaaS	PaaS	N/A	N/A
7.7	O órgão corrige vulnerabilidades detectadas?	GI2	IaaS	PaaS	N/A	N/A

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pelo gerenciamento contínuo de vulnerabilidades do *hardware* e *software*, tanto dos servidores físicos quanto virtuais, rede, *middleware* e aplicações utilizadas.
- ***IaaS* -** A organização é responsável pelo gerenciamento contínuo de vulnerabilidades do *software*, servidores virtuais, rede virtual, *middleware* e aplicações utilizadas. O CSP é responsável pelo gerenciamento contínuo de vulnerabilidades da infraestrutura e da tecnologia que fornece.
- ***PaaS*** - A organização é responsável pelo gerenciamento contínuo de vulnerabilidades das aplicações e ferramentas de desenvolvimento utilizadas. O *CSP* é responsável pelo gerenciamento contínuo de vulnerabilidades da infraestrutura de *hardware* e das tecnologias de *software* que fornece.
- ***SaaS*** - A organização é responsável pelo processo de gerenciamento de vulnerabilidades e pelo processo de remediação. O *CSP* é responsável pela gestão automatizada de *patches* e pelas varreduras de vulnerabilidades.
- ***FaaS*** - A organização é responsável pelo processo de gerenciamento de vulnerabilidades e pelo processo de remediação. O *CSP* é responsável pela gestão automatizada de *patches* e pelas varreduras de vulnerabilidades.

Considerações adicionais sobre nuvem

- É sempre responsabilidade da organização solicitar documentação ao *CSP* detalhando como o este está protegendo a infraestrutura e a tecnologia pelas quais é responsável.
- A organização deve continuamente adquirir, avaliar e agir sobre novas informações a fim de identificar vulnerabilidades, remediar e minimizar a janela de oportunidade para atacantes.
- Ao considerar ambientes *PaaS*, alguns terão imagens ou modelos que, por padrão, não permitem usuários interativos, como contas de *scanner*. O órgão deve considerar uma solução que identifique vulnerabilidades sem introduzir novos riscos e que não exija uma conta de *scanner* dedicada.
- Alguns agentes possuem dependências de *download* que podem exigir a abertura de *proxies* ou *firewalls*, o que pode introduzir outros elementos de risco que o órgão público usuário de serviços de nuvem precisa estar ciente.

4.8 CONTROLE 8: Gestão de registros de auditoria

Visão geral

Coletar, alertar, analisar e reter registros de auditoria de eventos que possam ajudar a detectar, compreender ou se recuperar de um ataque.

Aplicabilidade na nuvem

Este Controle *CIS* fornece orientações para a manutenção e o monitoramento de *logs* de auditoria. Sem registros protegidos e completos, incidentes de segurança podem permanecer indefinidamente sem detecção e o dano pode ser irreversível, comprometendo a continuidade do serviço e a integridade das informações. O CSP auxilia a organização no atendimento a este Controle, fornecendo mecanismos para geração e monitoramento de *logs* de auditoria.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
8.1	O órgão estabelece e mantém um processo de gestão de *logs* de auditoria?	GI1	IaaS	PaaS	SaaS	FaaS
8.2	O órgão coleta *logs* de auditoria?	GI1	IaaS	PaaS	SaaS	FaaS
8.3	O órgão armazena adequadamente os *logs* de auditoria?	GI1	IaaS	PaaS	SaaS	N/A
8.4	O órgão padroniza a sincronização de tempo?	GI1	IaaS	N/A	N/A	N/A
8.5	O órgão coleta *logs* de auditoria detalhados?	GI2	IaaS	PaaS	SaaS	FaaS
8.6	O órgão coleta *logs* de auditoria de consulta do Sistema de Nomes de Domínio (*Domain Name System*, DNS)?	GI2	IaaS	PaaS	N/A	N/A
8.7	O órgão coleta *logs* de auditoria de requisição de *Uniform Resource Locator* (URL)?	GI2	IaaS	PaaS	N/A	N/A
8.8	O órgão coleta *logs* de auditoria de linha de comando?	GI2	IaaS	PaaS	N/A	N/A
8.9	O órgão centraliza os *logs* de auditoria?	GI2	IaaS	PaaS	SaaS	FaaS
8.10	O órgão retém os *logs* de auditoria?	GI2	IaaS	PaaS	SaaS	FaaS
8.11	O órgão conduz revisões de *logs* de auditoria?	GI2	IaaS	PaaS	SaaS	FaaS
8.12	O órgão coleta *logs* de provedores de serviços?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pela configuração, manutenção, monitoramento e processamento de *logs* de auditoria de todos os sistemas sob sua gestão direta.
- ***IaaS*** - A organização é responsável pela configuração, manutenção, monitoramento e análise dos *logs* de auditoria referentes a *software*, servidores virtuais, redes virtuais, *middleware* e aplicações utilizadas, quando aplicável no ambiente em nuvem.
- ***PaaS*** - A organização é responsável pela configuração, manutenção, monitoramento e análise dos *logs* de auditoria relacionados às aplicações, sistemas operacionais e ferramentas de desenvolvimento.
- ***SaaS*** - A organização é responsável pela configuração, manutenção, monitoramento e análise dos *logs* de auditoria a partir de sua disponibilização pelo *CSP*. Fontes de tempo e habilitação de *logs* dependem do provedor.
- ***FaaS*** - A organização é responsável pela configuração, manutenção, monitoramento e análise dos *logs* de auditoria a partir de sua disponibilização pelo *CSP*, respeitando as limitações de habilitação e sincronização de registros fornecidas pelo provedor.

Considerações adicionais sobre nuvem

- Para soluções *SaaS* e *FaaS*, normalmente é exigido que o *CSP* disponibilize os *logs* necessários para a organização poder acessá-los, analisá-los e mantê-los conforme normativos e controles internos.
- Alguns serviços podem não oferecer o nível de auditoria recomendado por este Controle e suas medidas, devendo tal limitação ser documentada e considerada em contratos e análises de risco.
- É responsabilidade da organização solicitar *logs* ao *CSP* quando estes não forem entregues automaticamente, garantindo canal seguro e rastreável para transferência das informações.
- O gerenciamento adequado da capacidade de armazenamento de *logs* é essencial em modelos *IaaS*, devendo a organização planejar espaço que contemple requisitos legais e operacionais.
- Manter *logs* de auditoria dos ativos tecnológicos por no mínimo 90 dias ou conforme legislação específica, regulamentações e políticas internas aplicáveis à organização.

4.9 CONTROLE 9: Proteção de *e-mail* e navegador *web*

Visão geral

Aprimorar as proteções e detecções de ameaças provenientes de *e-mails* e da *web*, pois essas são oportunidades para invasores manipularem o comportamento humano por meio de diferentes técnicas.

Aplicabilidade na nuvem

Este Controle *CIS* se concentra na segurança de navegadores *web* e clientes de *e-mail*, que representam vetores de ataque comuns, podendo resultar em exposição de informações sigilosas, interrupção de serviços essenciais ou violação de dados pessoais. Ambientes em nuvem organizacionais geralmente exigem acesso à internet via navegador. O uso de clientes de *e-mail* pode ser limitado, sendo comum sua utilização apenas para envio de alertas e relatórios automáticos gerados por sistemas organizacionais. Esses *e-mails* normalmente são acessados por ativos institucionais conectados a redes internas da organização. Atualmente, grande parte das aplicações organizacionais opera em plataformas *web* hospedadas em nuvem.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
9.1	O órgão permite o uso apenas de navegadores e clientes de e-mail totalmente suportados por seus fornecedores?	GI1	IaaS	PaaS	SaaS	FaaS
9.2	O órgão usa serviços de filtragem de Sistema de Nomes de Domínio (*Domain Name System*, DNS?	GI1	IaaS	PaaS	N/A	N/A
9.3	O órgão mantém e aplica filtros de *Uniform Resource Locator* (URL) baseados em rede?	GI2	IaaS	PaaS	N/A	N/A
9.4	O órgão restringe extensões desnecessárias ou não autorizadas de navegadores e clientes de e-mail?	GI2	IaaS	PaaS	SaaS	FaaS
9.5	O órgão implementa o *Domain-based Message Authentication, Reporting, and Conformance* (DMARC)?	GI2	IaaS	PaaS	SaaS	N/A
9.6	O órgão bloqueia tipos de arquivo desnecessários?	GI2	IaaS	PaaS	SaaS	N/A
9.7	O órgão implementa e mantém proteções *antimalware* nos servidores de e-mail?	GI3	IaaS	PaaS	SaaS	N/A

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pela configuração, manutenção, monitoramento e análise da segurança de *e-mail* e de navegadores *web* em todos os ativos sob sua gestão direta.
- ***IaaS*** - A organização é responsável pela configuração, manutenção, monitoramento e análise dos mecanismos de segurança de *e-mail* e navegação no *software*, servidores virtuais, redes virtuais, *middleware* e aplicações, quando aplicável.
- ***PaaS*** - A organização é responsável pela segurança relacionada ao uso de *e-mail* e navegadores *web* em aplicações, sistemas operacionais e ferramentas de desenvolvimento que utiliza sobre a plataforma do provedor.
- ***SaaS*** - A organização mantém responsabilidade sobre a configuração e uso seguro de *e-mail* e navegadores *web* por seus usuários, seguindo políticas de segurança vigentes.
- ***FaaS*** - A organização permanece responsável pela segurança no uso de *e-mail* e navegadores *web*, respeitando as capacidades disponibilizadas pelo *CSP*.

Considerações adicionais sobre nuvem

- Medidas relacionadas a navegadores autorizados, filtros de execução de *scripts* e registros de auditoria são aplicáveis sempre que houver acesso a aplicações remotas via navegador.
- Em serviços *SaaS* e possivelmente *FaaS*, navegadores *web* deve estar atualizados e configurados conforme políticas e normas internas de segurança do órgão, incluindo controle rígido de *plugins* e extensões.
- Garantir que nenhum cliente de *e-mail* seja instalado em quaisquer servidores da organização. Quando sistemas organizacionais necessitarem enviar alertas ou relatórios por *e-mail*, a comunicação deve ser somente de saída (*outbound only*), evitando superfícies de ataque desnecessárias.

4.10 CONTROLE 10: Defesa contra *malware*

Visão geral

Prevenir a instalação, disseminação e execução de aplicativos, códigos ou *scripts* maliciosos em ativos institucionais.

Aplicabilidade na nuvem

Este Controle *CIS* trata das medidas necessárias para garantir proteção contra *malware* em ambientes organizacionais. A introdução de código malicioso pode comprometer dados sigilosos da organização, impactar serviços essenciais e gerar danos que podem ser irreversíveis. Mesmo com segmentação de rede e defesa em profundidade, as organizações devem contar com ferramentas e processos específicos para prevenir, detectar, responder e reportar incidentes de *malware* em conformidade com as políticas de segurança da organização.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
10.1	O órgão instala e mantém um software *antimalware*?	GI1	IaaS	PaaS	N/A	N/A
10.2	O órgão configura atualizações automáticas de assinatura *antimalware*?	GI1	IaaS	PaaS	N/A	N/A
10.3	O órgão desabilita a execução e reprodução automática para mídias removíveis?	GI1	IaaS	N/A	N/A	N/A
10.4	O órgão configura a varredura *antimalware* automática de mídias removíveis?	GI2	IaaS	N/A	N/A	N/A
10.5	O órgão habilita funções antiexploração (*anti-exploit*)?	GI2	IaaS	PaaS	N/A	N/A
10.6	O órgão gerencia o software *antimalware* de forma centralizada?	GI2	IaaS	PaaS	N/A	N/A
10.7	O órgão utiliza software *antimalware* baseado em comportamento?	GI2	IaaS	PaaS	N/A	N/A

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pela configuração, manutenção, monitoramento e análise de soluções *antimalware* e demais controles de segurança aplicados a todos os ativos físicos e virtuais sob sua gestão, com vistas à prevenção de intrusões e ataques.

- ***IaaS*** - A organização é responsável pelas ferramentas e configurações de defesa contra *malware* aplicadas ao *software*, servidores virtuais, redes virtuais, *middleware* e aplicações que gere no ambiente em nuvem.
- ***PaaS*** - A organização é responsável por soluções e mecanismos *antimalware* relativos às aplicações, sistemas operacionais e ferramentas de desenvolvimento sob sua administração na plataforma do provedor.
- ***SaaS*** - Este Controle e suas medidas não se aplicam diretamente à organização, pois a responsabilidade de defesa contra *malware* é do provedor. A organização deve, entretanto, exigir e validar garantias contratuais de segurança.
- ***FaaS*** - Este Controle e suas medidas não se aplicam diretamente à organização, ficando a responsabilidade sob o *CSP*, com verificação contratual pela organização.

Considerações adicionais sobre nuvem

- Em alguns provedores de nuvem, há dispositivos virtuais que não suportam soluções *antimalware* tradicionais, exigindo o uso de abordagens alternativas (varredura em infraestrutura, segurança na *pipeline* de *CI/CD*, monitoramento comportamental, entre outros).
- Quando a responsabilidade de defesa contra *malware* não é atribuída ao órgão público (ex.: *SaaS* e *FaaS*), esta passa inteiramente ao *CSP*, devendo ser formalizada em legislação específica.

4.11 CONTROLE 11: Recuperação de dados

Visão geral

Estabelecer e manter práticas de realização de cópias de segurança e recuperação de dados suficientes para restaurar os ativos institucionais para um estado confiável e pré-incidente.

Aplicabilidade na nuvem

Este Controle *CIS* estabelece os requisitos para garantir que as organizações mantenham capacidade de recuperação de dados em caso de incidentes, falhas ou ataques cibernéticos. A perda de dados organizacionais pode resultar na interrupção de serviços essenciais e descumprimento de obrigações legais, incluindo leis de proteção de dados pessoais, acarretando assim em prejuízos diversos. Embora os provedores de nuvem assegurem a disponibilidade da infraestrutura, a integridade e a proteção dos dados continuam sendo responsabilidade da organização, incluindo *backups* regulares, testes de recuperação e mecanismos de redundância.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
11.1	O órgão estabelece e mantém um processo de realização de cópias de segurança (*backup*)?	GI1	IaaS	PaaS	N/A	N/A
11.2	O órgão executa *backups* automatizados?	GI1	IaaS	PaaS	SaaS	FaaS
11.3	O órgão protege os dados de recuperação?	GI1	IaaS	PaaS	SaaS	FaaS
11.4	O órgão estabelece e mantém uma instância isolada de dados de recuperação?	GI1	IaaS	PaaS	SaaS	FaaS
11.5	O órgão testa a recuperação dos dados?	GI2	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*) -** A organização é totalmente responsável pela implementação e gestão das capacidades de *backup* e recuperação de dados em toda a infraestrutura sob sua gerência.
- ***IaaS* -** A organização é responsável pela estratégia de *backup* e recuperação de dados de servidores virtuais, aplicações, redes virtuais, *middleware* e demais recursos geridos no provedor.
- ***PaaS* -** A organização é responsável por *backups* associados às aplicações, configurações de sistemas operacionais e ferramentas de desenvolvimento que administra dentro da plataforma.
- ***SaaS* -** A organização deve garantir mecanismo de *backup* complementar para os dados utilizados pela aplicação, ainda que executada como serviço. Deve exigir contratualmente garantias de retenção, recuperação e exportação dos dados junto ao *CSP*.
- ***FaaS* -** A organização é responsável pelos *backups* e recuperação do código e das funções desenvolvidas, assegurando que possam ser restaurados quando necessário.

Considerações adicionais sobre nuvem

- Dados organizacionais podem ser afetados em qualquer modelo de serviço, o que reforça a necessidade de gestão eficaz de cópias de segurança.
- Sempre incluir dados pessoais no escopo de *backup* de sistemas, preservando a continuidade do atendimento e o cumprimento da LGPD.

- Quando o *CSP* for responsável por parte da recuperação, isso deve estar formalizado em contrato, com *SLAs* claros e planos de contingência revisados regularmente.

4.12 CONTROLE 12: Gestão de infraestrutura de rede

Visão geral

Estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) os ativos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Aplicabilidade na nuvem

Este Controle *CIS* aborda a necessidade de gerenciar a configuração da rede utilizando diagramas de arquitetura juntamente com autenticação, autorização e auditoria. A infraestrutura de rede de um ambiente em nuvem deve exigir o mesmo rigor em gestão de configuração e processo de controle de mudanças que um ambiente físico. Os vetores de ataque, embora virtuais, continuam os mesmos: serviços inseguros, configurações inadequadas de *firewalls* e rede, e credenciais padrão ou legadas.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
12.1	O órgão mantém atualizada a infraestrutura de rede?	GI1	IaaS	N/A	N/A	N/A
12.2	O órgão estabelece e mantém uma arquitetura de rede segura?	GI2	IaaS	PaaS	SaaS	FaaS
12.3	O órgão gerencia a infraestrutura de rede com segurança?	GI2	IaaS	PaaS	SaaS	FaaS
12.4	O órgão elabora e mantém diagramas de arquitetura?	GI2	IaaS	PaaS	SaaS	FaaS
12.5	O órgão centraliza a autenticação, a autorização e a auditoria (*Authentication, Authorization, and Accounting*, AAA) de rede?	GI2	IaaS	N/A	N/A	N/A
12.6	O órgão utiliza protocolos seguros de comunicação e gerenciamento de rede?	GI2	IaaS	N/A	N/A	N/A
12.7	O órgão assegura que os dispositivos remotos utilizem uma Rede Privada Virtual (*Virtual Private Network*, VPN) e se conectam em uma infraestrutura de autenticação,	GI2	IaaS	N/A	N/A	N/A

	autorização e auditoria (*Authentication, Authorization, and Accounting*, AAA)?					
12.8	**O órgão utiliza e mantém recursos computacionais dedicados para todas as atividades administrativas de TI?**	**GI3**	**IaaS**	**N/A**	**N/A**	**N/A**

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pela configuração segura de todos os dispositivos de rede.
- ***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*.
- ***PaaS*** - A organização gerencia a aplicação e, por vezes, algumas configurações de rede do ambiente de hospedagem e das ferramentas de desenvolvimento. O *CSP* é responsável pelos servidores físicos, rede física, armazenamento, hipervisor e sistemas operacionais.
- ***SaaS*** - Este Controle não é aplicável à organização. O *CSP* é responsável pela configuração de todos os dispositivos de rede físicos e virtuais.
- ***FaaS*** - Este Controle não é aplicável à organização. O *CSP* é responsável pela configuração de todos os dispositivos de rede físicos e virtuais.

Considerações adicionais sobre nuvem

- Garantir que todos os *firewalls* virtuais estejam configurados com política de negação por padrão (*deny by default*).
- Aplicar autenticação multifator (*MFA*) para manter responsabilização e controle eficiente da configuração.
- Em alguns casos, soluções *SaaS* ou *FaaS* podem permitir controle de certos aspectos de rede, seja interna ou externamente. Geralmente o controle ocorre em modelos *IaaS* ou *PaaS*, mas deve ser avaliado também quando utilizando outros modelos de serviço.

4.13 CONTROLE 13: Monitoramento e defesa de rede

Visão geral

Implementar processos e ferramentas para estabelecer e manter monitoramento abrangente de rede e defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuários da organização.

Aplicabilidade na nuvem

Este Controle *CIS* enfatiza a gestão do fluxo de informações entre redes de diferentes níveis de confiança. Para controlar o fluxo de tráfego e monitorar conteúdo em busca de ataques ou evidências de comprometimento, as defesas de borda devem ser multicamadas, contando com *firewalls*, *proxies*, *DMZs*, sistemas de prevenção e detecção de intrusão. No ambiente de nuvem, nem sempre é possível configurar múltiplas camadas como em ambientes físicos. Mesmo assim, é preciso estruturar uma defesa adequada, pois os limites mudam e a localização das defesas é diferente.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
13.1	O órgão centraliza alertas de eventos de segurança?	GI2	IaaS	PaaS	SaaS	FaaS
13.2	O órgão implanta soluções de detecção de intrusão baseada em *host*?	GI2	IaaS	N/A	N/A	N/A
13.3	O órgão implanta soluções de detecção de intrusão de rede?	GI2	IaaS	N/A	N/A	N/A
13.4	O órgão realiza filtragem de tráfego entre os segmentos de rede?	GI2	IaaS	N/A	N/A	N/A
13.5	O órgão realiza o gerenciamento de controle de acesso para ativos remotos?	GI2	IaaS	N/A	N/A	N/A
13.6	O órgão coleta *logs* de fluxo de tráfego de rede?	GI2	IaaS	N/A	N/A	N/A
13.7	O órgão implanta soluções para prevenção de intrusão baseada em *host*?	GI3	IaaS	N/A	N/A	N/A
13.8	O órgão implanta soluções para prevenção de intrusão de rede?	GI3	IaaS	N/A	N/A	N/A
13.9	O órgão implanta controle de acesso em nível de porta?	GI3	IaaS	N/A	N/A	N/A
13.10	O órgão realiza a filtragem da camada de aplicação?	GI3	IaaS	N/A	N/A	N/A

13.11	O órgão ajusta limites de alertas de eventos de segurança?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização é responsável pelo monitoramento e defesa da borda da rede.
- ***IaaS*** - A organização é responsável pela defesa da borda virtual; o *CSP* responde pela infraestrutura física.
- ***PaaS*** - A organização pode controlar portas de rede, configurações do *host* e ferramentas de desenvolvimento para bloquear comunicações.
- ***SaaS*** - A organização é responsável pelo acesso à aplicação; o *CSP* garante a segurança da aplicação e fornece acesso para varredura de vulnerabilidades.
- ***FaaS*** - A maioria das medidas deste controle de segurança não se aplica à organização, ficando sob a responsabilidade do *CSP*.

Considerações adicionais sobre nuvem

- Manter e impor padrão mínimo de segurança para dispositivos acessando remotamente a nuvem em ambientes locais e *IaaS*.
- Registrar todas as atividades e tráfego no ambiente de nuvem (especialmente para *IaaS*).
- Nem todo tráfego vai necessariamente passar por um único dispositivo virtual.

4.14 CONTROLE 14: Conscientização e treinamento de competências

Visão geral

Estabelecer e manter ações de treinamento e um programa de conscientização em segurança da informação contínuo para influenciar o comportamento dos agentes públicos, tornando-os qualificados e conscientes para reduzir os riscos de segurança da informação para a organização.

Aplicabilidade na nuvem

Este Controle *CIS* foca na educação e treinamento do time organizacional, abordando desde práticas básicas até habilidades avançadas para reforçar a segurança. Erros humanos e negligência são causas comuns de vulnerabilidades, podendo causar danos significativos em ambientes de nuvem. A responsabilidade pelo treinamento é sempre da organização, independente do modelo de serviço ou implantação.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
14.1	O órgão implementa um programa de conscientização em segurança da informação?	GI1	IaaS	PaaS	SaaS	FaaS
14.2	O órgão conscientiza os agentes públicos para reconhecer ataques de engenharia social?	GI1	IaaS	PaaS	SaaS	FaaS
14.3	O órgão conscientiza os agentes públicos nas melhores práticas de autenticação?	GI1	IaaS	PaaS	SaaS	FaaS
14.4	O órgão conscientiza os agentes públicos nas melhores práticas de tratamento de dados?	GI1	IaaS	PaaS	SaaS	FaaS
14.5	O órgão conscientiza os agentes públicos sobre as causas ocorrências não intencionais que podem expor dados?	GI1	IaaS	PaaS	SaaS	FaaS
14.6	O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?	GI1	IaaS	PaaS	SaaS	FaaS
14.7	O órgão conscientiza os agentes públicos sobre como identificar e comunicar se os ativos institucionais estão sem atualizações de segurança?	GI1	IaaS	PaaS	SaaS	FaaS
14.8	O órgão conscientiza os agentes públicos sobre os perigos de se conectar e transmitir dados organizacionais em redes inseguras?	GI1	IaaS	PaaS	SaaS	FaaS
14.9	O órgão implementa ações para capacitação sobre segurança da informação?	GI2	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - Responsabilidade total da organização por treinamentos.
- ***IaaS*, *PaaS*, *SaaS*, *FaaS*** - O programa de conscientização e treinamento é sempre demanda da organização, mesmo que o *CSP* possua seu próprio programa.

Considerações adicionais sobre nuvem

- Não há considerações adicionais específicas além da responsabilização total da organização pela capacitação dos usuários.

4.15 CONTROLE 15: Gestão de provedor de serviço

Visão geral

Desenvolver um processo para avaliar provedores de serviços que detêm dados críticos para a organização ou são responsáveis por plataformas ou processos críticos de TI do órgão, a fim de garantir que esses provedores estejam protegendo essas plataformas e dados adequadamente.

Aplicabilidade na nuvem

Este Controle *CIS* trata da avaliação de provedores de serviço que armazenam dados críticos ou gerenciam plataformas críticas para a organização. Provedores podem ser internos, externos ou compartilhados, e incluem aplicações, serviços de nuvem, internet, entre outros. Em ambientes de nuvem, a armazenagem e transferência de dados críticos, e a responsabilidade compartilhada, tornam crucial o rastreamento dessas informações.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
15.1	O órgão estabelece e mantém o inventário de provedores de serviços?	GI1	IaaS	PaaS	SaaS	FaaS
15.2	O órgão estabelece e mantém uma política de gestão de provedores de serviços?	GI2	IaaS	PaaS	SaaS	FaaS
15.3	O órgão categoriza provedores de serviços?	GI2	IaaS	PaaS	SaaS	FaaS
15.4	O órgão descreve os requisitos mínimos de segurança da informação nos contratos dos provedores de serviços?	GI2	IaaS	PaaS	SaaS	FaaS
15.5	O órgão avalia provedores de serviços?	GI3	IaaS	PaaS	SaaS	FaaS
15.6	O órgão monitora provedores de serviço?	GI3	IaaS	PaaS	SaaS	FaaS
15.7	O órgão encerra de forma segura o contrato com o provedor de serviços?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A organização mantém todas as informações sobre provedores. Geralmente isso engloba aplicação, rede, internet, armazenamento, telecomunicações etc.
- ***IaaS, PaaS, SaaS, FaaS*** - A organização sempre é responsável por reunir informações dos provedores, recebendo dados do *CSP* quando solicitado.

Considerações adicionais sobre nuvem

- É fundamental identificar que o *CSP* se enquadra em todos os modelos de serviço.
- Outros provedores podem ser categorizados conforme os serviços utilizados, demandando coleta adicional de informações para além do *CSP*.

4.16 CONTROLE 16: Segurança de aplicações

Visão geral

Gerenciar o ciclo de vida de segurança de todas as soluções de *software* desenvolvidas, hospedadas ou adquiridas internamente, com o objetivo de prevenir, detectar e corrigir vulnerabilidades de segurança antes que elas possam impactar a organização.

Aplicabilidade na nuvem

Este Controle *CIS* aborda o ciclo de vida de segurança para *softwares* desenvolvidos internamente, hospedados ou adquiridos. Qualquer programa organizacional deve incluir a nuvem em suas políticas e testes de vulnerabilidades, integrando gestão da cadeia de suprimentos de *software* e desenvolvimento seguro.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
16.1	O órgão estabelece e mantém um processo de desenvolvimento seguro de aplicações?	GI2	IaaS	PaaS	N/A	FaaS
16.2	O órgão estabelece e mantém um processo para aceitar e tratar vulnerabilidades de software?	GI2	IaaS	PaaS	N/A	FaaS
16.3	O órgão executa análise de causa raiz em vulnerabilidades de segurança?	GI2	IaaS	PaaS	N/A	FaaS

16.4	O órgão estabelece e gerencia um inventário de componentes de software de terceiros?	GI2	IaaS	PaaS	N/A	N/A
16.5	O órgão usa componentes de software de terceiros atualizados e confiáveis?	GI2	IaaS	PaaS	N/A	N/A
16.6	O órgão estabelece e mantém um sistema e processos para a classificação de severidade de vulnerabilidades de aplicações?	GI2	IaaS	PaaS	N/A	FaaS
16.7	O órgão usa modelos de configurações de proteção padrão para infraestrutura de aplicações?	GI2	IaaS	PaaS	N/A	N/A
16.8	O órgão separa sistemas de produção e não produção?	GI2	IaaS	PaaS	SaaS	FaaS
16.9	O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?	GI2	IaaS	PaaS	N/A	FaaS
16.10	O órgão aplica princípios de *design* seguro em arquiteturas de aplicações?	GI2	IaaS	PaaS	N/A	FaaS
16.11	O órgão reutiliza os módulos ou serviços validados quanto aos requisitos de segurança das aplicações?	GI2	IaaS	PaaS	N/A	N/A
16.12	O órgão implementa verificações de segurança em nível de código?	GI3	IaaS	PaaS	N/A	FaaS
16.13	O órgão realiza teste de intrusão de aplicação (*pentest*)?	GI3	IaaS	PaaS	SaaS	N/A
16.14	O órgão realiza a modelagem de ameaças?	GI3	IaaS	PaaS	N/A	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A responsabilidade completa é da organização pelo *software*.
- ***IaaS*, *PaaS*:** A organização responde pela segurança das aplicações, podendo precisar de permissão do *CSP* para varreduras.
- ***SaaS*** - A organização deve tratar vulnerabilidades, e o *CSP* deve fornecer relatórios sobre segurança do produto.
- ***FaaS*** - A responsabilidade é da organização pela segurança do código funcional.

Considerações adicionais sobre nuvem

- Para varreduras de vulnerabilidades em *SaaS*, geralmente é preciso requisitar acesso ao *CSP* com detalhes de *IPs*, períodos etc.
- O *CSP* pode fornecer relatórios de gestão de vulnerabilidades para serviços *SaaS*.

4.17 CONTROLE 17: Gestão de resposta a incidentes

Visão geral

Estabelecer um programa para desenvolver e manter um processo de gestão de incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.

Aplicabilidade na nuvem

Este Controle *CIS* trata do gerenciamento de incidentes na nuvem, exigindo monitoramento constante das atividades e uma clara definição, em contrato, das responsabilidades do *CSP* versus consumidor. As ações em resposta a incidentes devem englobar detecção, contenção, erradicação e recuperação.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
17.1	O órgão designou agente responsável, e respectivo substituo, para gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?	GI1	IaaS	PaaS	SaaS	FaaS
17.2	O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?	GI1	IaaS	PaaS	SaaS	FaaS
17.3	O órgão estabelece e mantém um processo institucional para notificar incidentes de segurança da informação?	GI1	IaaS	PaaS	SaaS	FaaS
17.4	O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?	GI2	IaaS	PaaS	SaaS	FaaS
17.5	O órgão atribui funções e responsabilidades para gestão de incidentes de segurança da informação?	GI2	IaaS	PaaS	SaaS	FaaS

17.6	O órgão define mecanismos de comunicação a ser realizado durante o tratamento de incidentes de segurança da informação?	GI2	IaaS	PaaS	SaaS	FaaS
17.7	O órgão conduz exercícios de tratamento de incidentes de segurança da informação regularmente?	GI2	IaaS	PaaS	SaaS	FaaS
17.8	O órgão realiza análises pós-incidente de segurança da informação?	GI2	IaaS	PaaS	SaaS	FaaS
17.9	O órgão estabelece a diferença entre evento e incidente de segurança da informação?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*)** - A responsabilidade pela resposta é integral da organização.
- ***IaaS*, *PaaS*, *SaaS*, *FaaS*** - consumidora organização é sempre responsável pelo plano de resposta; o *CSP* pode ter responsabilidades contratuais pela comunicação e mitigação, devendo ser claros os limites de atuação**.**

Considerações adicionais sobre nuvem

- Contratos e *SLAs* precisam prever tempos de resposta, notificações e detalhamento das obrigações do *CSP* em incidentes.
- Ferramentas e registros do *CSP* devem ser acessíveis ao consumidor para facilitar as investigações.

4.18 CONTROLE 18: Testes de intrusão

Visão geral

Testar a eficácia e a resiliência dos ativos institucionais e soluções de *software* identificando e explorando vulnerabilidades e simulando os objetivos e ações de um invasor.

Aplicabilidade na nuvem

Este Controle *CIS* trata dos testes de intrusão em nuvem, que exigem autorização formal do *CSP* para determinados tipos de varredura e ataques simulados. O teste deve respeitar as regras do *CSP* e os limites impostos pelo contrato, evitando riscos à disponibilidade dos serviços.

Lista de medidas

ID	Título da medida	GI	Aplicabilidade na computação em nuvem			
18.1	O órgão elabora e mantém um programa de teste de intrusão (*pentest*)?	GI2	IaaS	PaaS	SaaS	FaaS
18.2	O órgão realiza testes de intrusão externos periódicos (*pentest*)?	GI2	IaaS	PaaS	SaaS	FaaS
18.3	O órgão corrige os resultados dos testes de intrusão (*pentest*)?	GI2	IaaS	PaaS	SaaS	FaaS
18.4	O órgão valida as medidas de segurança?	GI3	IaaS	PaaS	SaaS	FaaS
18.5	O órgão realiza testes de intrusão internos periódicos (*pentest*)?	GI3	IaaS	PaaS	SaaS	FaaS

Considerações sobre serviços e modelos de implantação em nuvem

Ao considerar os modelos de implantação, é possível perceber que este Controle *CIS* e suas medidas são aplicáveis ao modelo Privado (local / *on-premises*). Para os modelos Privado (hospedado por terceiros), Público, Comunitário e Híbrido, será necessário seguir as especificações do(s) modelo(s) de serviço/implantação contratado(s) pela organização.

- **Privado (*on-premises*) -** A organização tem total liberdade para realizar testes.
- ***IaaS*, *PaaS*, *SaaS*, *FaaS* -** A organização deve solicitar permissão ao *CSP*, seguir *guidelines* específicas e informar datas, escopo e endereçamento *IP*.

Considerações adicionais sobre nuvem

- Alguns *CSPs* possuem portais específicos para submissão e acompanhamento de autorizações de *pentests*.
- Os testes devem ser agendados e realizados em consenso com o *CSP* para evitar impactos adversos.

5 Considerações finais

A adoção da computação em nuvem representa um avanço estratégico indispensável para a modernização e eficiência da Administração Pública federal, promovendo maior agilidade, flexibilidade e otimização de recursos. Este guia complementar busca oferecer um entendimento abrangente e prático das melhores práticas e controles de segurança da informação aplicáveis ao contexto da computação em nuvem, alinhando requisitos regulatórios brasileiros já estabelecidos no *framework* do PPSI 2.0 com referenciais internacionais consolidados.

A segurança na nuvem é complexa e exige a cooperação ativa entre os órgãos públicos e os provedores de serviços, considerando os modelos de implantação e os diferentes níveis de responsabilidade compartilhada. A implementação das medidas apresentadas serve para mitigar riscos e assegurar a conformidade regulatória.

Além disso, o aperfeiçoamento contínuo dos processos de governança, conscientização dos agentes públicos e a avaliação constante da eficiência desses controles e medidas são fundamentais para fortalecer a resiliência organizacional frente aos desafios e ameaças dinâmicas do ambiente digital. Assim, este guia se configura como um instrumento essencial para orientar e apoiar a transformação digital segura, promovendo a confiança pública e a sustentabilidade operacional dos serviços oferecidos.

6 Referências

[1] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Adoção de serviços de computação em nuvem no âmbito da Administração Pública federal**. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ambiente-tecnologico/nuvem. Acesso em: 23 out. 2025.

[2] CLOUD SECURITY ALLIANCE. **Top threats to cloud computing: Egregious eleven**. 2023. Disponível em: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive. Acesso em: 23 out. 2025.

[3] MELL, Peter; GRANCE, Timothy. **The NIST Definition of Cloud Computing**. Gaithersburg: National Institute of Standards and Technology, 2011. (NIST Special Publication 800-145).

[4] CENTER FOR INTERNET SECURITY (CIS). **CIS Controls v8.1 Cloud Companion Guide**. East Greenbush, NY, USA: Center for Internet Security, 2024. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-cloud-companion-guide. Acesso em: 23 out. 2025.

[5] CENTER FOR INTERNET SECURITY (CIS). **CIS Controls v8.1 Guide**. East Greenbush, NY, USA: Center for Internet Security, 2024. Disponível em: https://www.cisecurity.org/controls. Acesso em: 07 out. 2025.

gov.br

Dúvida?

Entre em contato conosco

Formulário:
https://forms.office.com/r/j8w0h9Mvi1

Email:
ppsi.sgd@gestao.gov.br

Telefone:
(61) 2020-2046

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO