Modelo de Política de Gestão de Provedor de Serviços

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0

Brasília, abril de 2024

MODELO DE POLÍTICA DE GESTÃO DE PROVEDORES DE SERVIÇOS

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

Julierme Rodrigues da Silva

Coordenador-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

Francisco Magno Felix Nobre

Ivaldo Jeferson de Santana Castro

Rogério Vinícius Matos Rocha

Equipe Revisora

Adriano de Andrade Moura

Rodrigo Duran Lima

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
22/04/2024	1.0	Modelo de Política de Gestão de Provedores de Serviços	Equipe Técnica de Elaboração

Sumário

Aviso Preliminar e Agradecimentos

O presente Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de uma Política de Gestão de Provedor de Serviços, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Gestão de Provedor de Serviços visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos - MGI e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO) e do *National Institute of Standards and Technology* (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação (DPSI) da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, à ABNT, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Gestão de Provedor de Serviços no âmbito institucional.

O Controle 15 do Guia do Framework de Privacidade e Segurança da Informação (p. 53) estabelece que:

Controle 15: Gestão de Provedor de Serviços *– Para garantir a proteção das informações, sistemas e processos críticos da organização, deve-se estabelecer um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.*

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 15 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 15 que estão contempladas por este modelo são 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 e 15.7.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão, apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). É importante destacar também que as informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

A Política de Gestão de Provedor de Serviços (PGPS) é um documento essencial que estabelece os princípios, diretrizes e procedimentos para garantir a segurança cibernética e a resiliência operacional da organização ao contratar e gerenciar provedores de serviços externos. Este Modelo de Política foi desenvolvido para orientar a organização na implementação de práticas eficazes de gestão de provedores de serviços, alinhadas com os padrões reconhecidos e melhores práticas do setor, no qual responsáveis pela segurança cibernética, gestão de riscos e demais partes interessadas e envolvidas na contratação e supervisão de provedores de serviços devem adaptá-lo às necessidades específicas e ao ambiente operacional da organização, garantindo a aplicação eficaz dos princípios e procedimentos delineados neste documento.

[1] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf - Acesso em 26/03/2024.

A gestão de provedores é o processo de contratação, identificação, rastreamento, manutenção de contratos e encerramento de contratos com provedores de serviço de uma organização. A PGPS fornece diretrizes para o estabelecimento de processos e procedimentos para governar o ciclo de vida da gestão de provedores de serviço enquanto uma instituição estiver utilizando de serviços providos por terceiros.

Política de Gestão de Provedor de Serviços

IMPORTANTE: Este modelo deve ser utilizado exclusivamente como referência, devendo o [órgão/empresa/fundação] considerar as particularidades técnicas especificas do seu ambiente, bem como observar a boa aderência aos processos internos a fim de construir uma política que seja adequada a sua realidade.

Este modelo tem por foco prover diretrizes para a elaboração da Política de Gestão de Provedor de Serviços (PGPS).

Para usar este modelo, basta substituir o texto em cinza por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplo e converta todo o texto restante em preto antes do processo de aprovação.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.
Políticas Relacionadas	Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Política de Gestão de Riscos \ Política de Proteção de Dados Pessoais \ POSIN
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.
Versão	Indique a versão atual desta política

Propósito [Objetivo da Política] conforme IN01 GSI/PR art.11

Levando em consideração a natureza e a finalidade do órgão ou entidade, descreva os fatores ou circunstâncias que determinam a existência da PGPS. Além disso, demonstre os objetivos básicos da Política e o que ela pretende alcançar.

Exemplo:

O principal objetivo da Política de Gestão de Provedor de Serviços (PGPS) é fornecer diretrizes que auxiliem ao órgão a avaliar, selecionar, monitorar e revisar os provedores de serviços contratados pelo órgão com o objetivo de mitigar os riscos associados à terceirização de serviços e proteger os ativos e informações críticas do [órgão/empresa/fundação] contra ameaças cibernéticas.

Ao adotar a PGPS, o [órgão/empresa/fundação] demonstra seu compromisso com a governança de serviços, além de estabelecer controles que minimizam riscos, fortalecendo a segurança cibernética e a proteção de seus ativos contra ameaças em constante evolução. A implementação eficaz desta Política fortalecerá a postura de segurança do [órgão/empresa/fundação] e contribuirá para sua resiliência operacional em um cenário digital cada vez mais complexo e desafiador.

[Acrescente aqui os objetivos para a PGPS que julgar necessário.]

Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I

Defina a quem e a quais sistemas esta Política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique

quaisquer exclusões ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Exemplo:

Esta Política se aplica a todos os departamentos que contratam, supervisionam ou interagem com provedores de serviços externos. Isso inclui, mas não se limita a:

- Tecnologia da Informação (TI): Responsáveis pela contratação e supervisão de provedores de serviços de infraestrutura de TI, hospedagem na nuvem, suporte técnico, entre outros.
- Segurança Cibernética: Encarregados de avaliar os riscos de segurança associados à terceirização de serviços e de implementar controles para mitigar esses riscos.
- Departamentos Jurídicos e de Compliance: Responsáveis por revisar e avaliar contratos com provedores de serviços para garantir conformidade com regulamentações relevantes e requisitos legais.
- Compras e Aquisições: Encarregados do processo de licitações e contratação de provedores de serviços, em conformidade com as políticas e procedimentos estabelecidos.
- Todas as partes interessadas que interagem com os serviços fornecidos pelos provedores externos, incluindo funcionários, clientes e parceiros comerciais.

É fundamental que todas as áreas do [órgão/empresa/fundação] que tenham envolvimento direto ou indireto com provedores de serviços externos sigam as diretrizes estabelecidas nesta Política. Isso garante uma abordagem consistente e coordenada para mitigar os riscos associados à terceirização de serviços e proteger os interesses e ativos do [órgão/empresa/fundação].

[*Acrescente aqui mais definições sobre o escopo da PGPS que julgue necessárias.*]

Termos e Definições [Glossário] conforme IN01 GSI/PR art.12 item II

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Recomenda-se utilizar como referência as definições apresentadas na PORTARIA GSI/PRNº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA, além do Art. 2º da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 e do Art. 5º da LGPD].

Exemplo:

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Área de TIC: unidade setorial, seccional ou correlata do SISP, responsável por gerir a Tecnologia da Informação e Comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC do órgão ou entidade;

Gestor do Contrato: servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

Fiscal Técnico do Contrato: servidor representante da Área de TIC, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos;

Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

Fiscal Setorial do Contrato: servidor representante de setores distintos ou em unidades desconcentradas de um órgão ou uma entidade, indicado pela autoridade competente dessa área para o acompanhamento da execução do contrato nos aspectos técnicos ou administrativos;

Preposto: representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

Solução de TIC: conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC;

Requisitos da contratação de TIC: conjunto de características e especificações necessárias para definir a solução de TIC a ser contratada;

Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação dos impactos e de suas probabilidades;

Análise de riscos: processo de compreensão da natureza do risco e determinação do nível de risco. Fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos;

Avaliação de riscos: processo de comparar os resultados da análise de riscos para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis. A avaliação de riscos auxilia na decisão sobre o tratamento de riscos;

[*Acrescente os termos-chave, siglas ou conceitos que podem ser utilizados na Política.*]

Referência legal e de boas práticas [Documentos norteadores]

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a Política ou com as quais ela deve estar em conformidade ou ser cumprida. Confirme com a respectiva consultoria jurídica do órgão ou da entidade se a lista é completa e precisa.

Orientação	Seção
Lei nº 13.709, de 14 de agosto de 2018	Em sua íntegra
Lei nº 14.133, de abril de 2021. Lei de Licitações e Contratos Administrativos	Em sua íntegra
Instrução Normativa SGD/ME nº 94 de 23 de dezembro de 2022	Em sua íntegra
Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado	Em sua íntegra
Guia do Framework de Privacidade e Segurança da Informação	Controle 15
Portaria nº 93, de 26 de setembro de 2019	Em sua íntegra
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art. 11 e 12, itens I e II
Decreto Nº 9.637, de 26 de dezembro de 2018	Art. 17, inciso IX
Instrução Normativa Nº 5, de 30 de agosto de 2021	Art. 19
Center for Internet Security - CIS	*Critical Security Control 15: Service Provider Management*
International Organization for Standardization – ISO 27001:2022	Item 9.1
International Organization for Standardization – ISO 27002:2022	Itens 5.19, 5.20, 5.21, 5.22, 5.23 e 6.6
International Organization for Standardization – ISO 20000:2022	Item 9.1

Declarações da Política [Regras aplicáveis ao caso específico]

Descreva as regras que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas. A subdivisão desta seção em subseções pode ser necessária dependendo da complexidade da política.

A Política de Gestão de Provedores de Serviços - PGPS deve adotar uma abordagem abrangente no estabelecimento de diretrizes para auxiliar na avaliação, seleção, monitoramento e revisão contínua dos provedores de serviços contratados pela organização. Este modelo de política está alinhado com o Controle 15 do Guia de Framework de Privacidade e Segurança da Informação, que destaca a importância de estabelecer controles para proteger as informações e os sistemas do [órgão/empresa/fundação] devido ao acesso concedido a provedores de serviços.

Algumas das diretrizes a seguir podem ampliar os requisitos e práticas recomendadas para garantir a privacidade e segurança da informação ao gerenciar provedores de serviços, abrangendo áreas como seleção, contratação, monitoramento, gerenciamento de incidentes, treinamento e conscientização.

Esta Política também deve adotar uma abordagem proativa para mitigar os riscos associados à terceirização de serviços e garantir a segurança cibernética e operacional do [órgão/empresa/fundação]. Ao seguir esses princípios gerais, o [órgão/empresa/fundação] irá fortalecer sua postura de segurança e proteger seus ativos críticos contra ameaças cibernéticas.

Das Diretrizes Gerais

1. A organização estabelecerá a PGPS, que deve estar de acordo com as diretrizes estipuladas na Política de Segurança da Informação e na Política de Proteção de Dados Pessoais do órgão.
2. A PGPS demonstrará aspectos micros e macros de privacidade, proteção de dados e segurança da informação na relação do [órgão/empresa/fundação] com seus provedores de serviços de tecnologia da informação. Os relacionamentos com provedores de serviços e produtos também devem seguir as diretrizes da PGPS.
3. O [Comitê Gestor de Tecnologia da Informação] deverá estipular os prazos que os departamentos e provedores de serviço se adequem as diretrizes da PGPS.
4. A PGPS e suas atualizações deverão ser aprovadas pelo [Comitê Gestor de Tecnologia da Informação] do órgão.
5. A PGPS deve ser devidamente divulgada e estará disponível para todos os colaboradores do [órgão/empresa/fundação].
6. Os compromissos de melhoria contínua dos provedores de serviço devem estar expostos na PGPS.
7. A PGPS deverá ser revisada e atualizada de forma periódica, ou quando houver necessidade por motivos que o [órgão/empresa/fundação] julgar relevantes (como por exemplo, adequação a novas leis, boas práticas, incidentes de segurança).
8. A organização deverá seguir as orientações da Instrução Normativa SGD/ME nº 94 para a gestão e governança de contratos de prestação de serviços.
9. A avalição de provedores de serviço deverá ser realizada levando em consideração, mas não se limitando, as diretrizes da Instrução Normativa SGD/ME nº 94.
10. A organização deverá estabelecer nos requisitos de contratação de provedores de serviços os aspectos mínimos e relevantes de proteção de dados e segurança da informação.
11. Os acordos e contratos entre o [órgão/empresa/fundação] e os provedores devem ser estabelecidos e documentados para que haja um entendimento claro entre as partes sobre as obrigações de cumprimento os requisitos mínimos e relevantes de proteção de dados e segurança da informação.
12. Os acordos e contratos podem conter os seguintes termos de segurança da informação e proteção de dados:
    a. Descrição das informações a serem fornecidas ou acessadas e os métodos e meios de fornecimento ou acesso as estas informações aos provedores;
    b. Classificação das informações de acordo com o esquema de classificação das informações do [órgão/empresa/fundação];
    c. Mapeamento e análise de convergência entre o método de classificação de informações do [órgão/empresa/fundação] e do provedor de serviços.
    d. Requisitos mínimos de segurança da informação em relação a infraestrutura de TI do provedor;
    e. Requisitos e procedimentos para a gestão de incidentes de segurança da informação e violação de proteção de dados e privacidade.

f. Contatos relevantes de ambas as partes, para possível tratamento de incidentes.

13. A organização deve definir um plano de ação para mitigar não conformidades de um provedor quando forem identificadas por meio de monitoramento.

14. A organização deve definir em seus contratos com provedores de serviços as obrigações de cada parte contratual de implementar um conjunto de controles acordados, incluindo controle de acesso, análise crítica de desempenho, monitoramento, relatos e auditorias, e as obrigações do provedor de serviços de estar em conformidade com os requisitos de proteção de dados e segurança da informação do [órgão/empresa/fundação].

15. A organização deverá implementar um processo de monitoramento com métodos estabelecidos para a validação de serviços e produtos em conformidade com os requisitos de proteção de dados e segurança da informação pré-estabelecidos.

[Acrescentar as diretrizes para a gestão de provedores de serviços].

Da Avaliação de Riscos

16. A avaliação de riscos poderá ocorrer antes e durante o contrato com um provedor de serviços.

17. A organização deve conduzir uma avaliação detalhada dos riscos associados à terceirização de serviços. Isso inclui, mas não se limita, a uma análise de vulnerabilidades potenciais, conformidade regulatória e impacto nas operações do [órgão/empresa/fundação].

18. Estabelecer processos e procedimentos para gerenciar a proteção de dados e a segurança da informação e os riscos que podem ser associados com o uso de serviços e produtos de provedores.

19. A organização deve estipular os responsáveis pela avaliação.

20. A organização deve definir quando os resultados da avaliação serão analisados e por quem.

21. Analisar os relatórios elaborados após as avaliações e auditorias de seus provedores de serviço.

22. Avaliar e gerenciar riscos à proteção de dados e à segurança da informação associados a:

    a. Uso das informações internas por provedores e seus associados.
    b. Vulnerabilidades e mal funcionamento de produtos ou serviços operados e criados pelos provedores e seus associados. (por exemplo, software, API, componentes de hardware e utilizados para a manutenção ativa dos produtos e serviços).

23. Implementar ferramentas de análise de risco contínuo para identificar e mitigar proativamente novas ameaças à segurança de dados apresentadas pelos provedores de serviços.

24. A organização deverá realizar a gestão de risco adequada em cada fornecedor e seus respectivos serviços.

25. A avaliação pode ser realizada após a ocorrência de um incidente de segurança.

[Acrescentar as diretrizes para a avaliação de provedores de serviços].

Dos Contratos e Acordos

Os acordos e contratos entre a organização e os provedores de serviço devem ser estabelecidos e documentados para que haja um entendimento claro entre a organização e o provedor de serviços sobre as obrigações de cumprimento dos requisitos mínimos e relevantes de proteção de dados e segurança da informação.

É recomendável que os contratos dos provedores de serviços incluam requisitos de segurança, tais como: requisitos mínimos do programa de segurança, notificação e resposta a incidentes de segurança e/ou violação de dados, criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gerenciamento do provedor de serviços.

A segurança deve ser implementada nas fases iniciais do desenvolvimento da PGPS. A segurança é importante desde o início porque pode se tornar cara a longo prazo se for negligenciada. Certifique-se de que os provedores de serviços considerados incorporam padrões de segurança do setor, como a ISO 27001.

Recomenda-se revisar contratos dos provedores de serviços anualmente para garantir que os contratos não faltem aos requisitos de segurança.

26. Todos os contratos com provedores de serviços devem incluir cláusulas específicas relacionadas à privacidade, proteção de dados, segurança da informação, responsabilidades, conformidade regulatória e requisitos de relatórios.
27. Quando necessário, o [órgão/empresa/fundação] deverá estabelecer procedimentos para a continuação da prestação de serviço em caso alteração do provedor, seja por conclusão do contrato ou por incapacidade do provedor original.
28. A organização deve solicitar a assinatura de termos de confidencialidade por parte dos funcionários e colaboradores dos provedores de serviço, sendo esta, uma condição a ser cumprida antes dos associados do provedor de serviço iniciarem a operação de serviços e produtos.
29. Os contratos devem ser revisados por profissionais jurídicos e de segurança cibernética para garantir que as obrigações sejam claramente definidas e aplicáveis.
30. Incluir cláusulas contratuais que estabeleçam o direito do [órgão/empresa/fundação] de auditar as práticas de proteção de dados e segurança da informação do provedor de serviços.
31. Estabelecer um mecanismo para revisar e atualizar periodicamente os requisitos de privacidade, proteção de dados e segurança da informação do contrato à medida que novas ameaças e regulamentações surjam.
32. Definir os recursos de TI e informações que os provedores de serviços podem acessar, usar, monitorar ou controlar.
33. Definir e fazer cumprir os prazos de confidencialidade das informações, produtos e serviços do [órgão/empresa/fundação].
34. Definir o nível de segurança física e lógica esperado dos provedores e associados e suas instalações.
35. Definir os requisitos de segurança da informação que irá utilizar para adquirir produtos ou serviços de TI;

36. Exigir que seus provedores propaguem e façam cumprir os requisitos de proteção de dados e segurança da informação do [órgão/empresa/fundação] em toda a cadeia de fornecimento;
37. Solicitar que os provedores de produtos e serviços de TI forneçam informações descrevendo os controles de proteção de dados e segurança da informação implementados em seus produtos e serviços e as configurações necessárias para a sua operação segura;
38. Obter garantia de que os produtos e serviços de TI entregues estejam funcionando como o esperado;
39. Especificar as responsabilidades do provedor de serviços em relação à exclusão segura de dados ao final do contrato ou quando não forem mais necessários.
40. Incluir disposições contratuais que garantam a conformidade do provedor de serviços com as diretrizes de segurança de dados disposto na Seção II (Da responsabilidade) da Lei Geral de Proteção de Dados - LGPD.
41. Estabelecer protocolos para revisão e aprovação de quaisquer subcontratados ou provedores de serviços adicionais que o provedor de serviços possa envolver.
42. Definir procedimentos para resolver divergências relacionadas à proteção de dados e à segurança da informação entre o [órgão/empresa/fundação] e o provedor de serviços.
    [Acrescentar as diretrizes para o contrato com provedores de serviços].

Dos Provedores de Serviço

Após a identificação e documentação dos potenciais provedores de serviços que atendam à política estabelecida, procede-se à classificação. Por exemplo: Tipos de fornecedores (por exemplo, infraestrutura de TI, fábrica de software e aplicativos, serviços de nuvem, suporte aos usuários internos, canais de atendimento a usuários externos). Isso dará uma representação mais granular dos provedores de serviços.

Inventário

43. A organização deve criar e manter um inventário de provedores de serviço e seus ativos associados, incluindo o número do contrato, tipo de serviço contratado, quantidade de operadores, e habilidades dos operadores.
44. A organização deverá realizar a atualização do inventário a cada [período] e quando ocorrerem novas contratações, alterações e encerramento de contratos.
45. O inventário é um ativo de informação como um catálogo de serviços, e devem ser aplicados controles de privacidade, proteção de dados e segurança da informação para evitar acessos indevidos, adulterações de conteúdo e vazamento de informações.
46. O inventário deve conter informações sobre os ativos de informação necessários a serem utilizados pelos provedores para a entrega e operação de serviços.

Classificação

47. A classificação dos provedores de serviço deve ser realizada a cada [período].

48. Estabelecer como classificar os provedores de serviço de acordo com a sensibilidade das informações, produtos e serviços utilizados pelos provedores.
49. Definir os tipos de componentes de serviços de infraestrutura de TI e nuvem fornecidos pelos fornecedores que podem degradar a proteção de dados e segurança da informação.
50. Os provedores de serviço devem ser classificados de acordo com a criticidade do serviço prestado para o [órgão/empresa/fundação]. Os responsáveis pela gestão do contrato devem auxiliar o processo de classificação dos provedores de serviço.
51. Incluir uma ou mais características, como sensibilidade dos dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis, risco inerente e risco mitigado.
52. A classificação deverá ser atualizada a cada [período] ou quando ocorrerem mudanças significativas nas execuções dos contratos que possam impactar esta salvaguarda.
53. A organização deverá avaliar se é interessante criar grupos de provedores de acordo com suas classificações, para que assim, sejam aplicadas medidas de privacidade, proteção de dados e segurança da informação específicas para cada grupo.

[Acrescentar as diretrizes para a inventário e classificação de provedores de serviços].

Da Avaliação e do Monitoramento Contínuo

O provedor de serviços deve permitir que a organização monitore e avalie a adesão e cumprimento aos requisitos contratuais por parte do provedor, principalmente de proteção de dados e segurança da informação.

54. Os provedores de serviços devem ser reavaliados de forma contínua.
55. Avaliar se os requisitos de proteção de dados e segurança da informação estão sendo cumpridos com cada provedor e contrato de forma individual.
56. Avaliar a qualidade e eficiência dos provedores de serviço de acordo com produtos e serviços entregues e em execução.
57. Realizar avaliações, utilizando-se ou não de terceiros independentes, para verificar a conformidade do provedor de serviços com as normas de proteção de dados e segurança da informação.
58. A organização deve implementar processos de monitoramento contínuo para avaliar o desempenho do provedor de serviços em relação aos padrões acordados de privacidade, proteção de dados, segurança da informação e conformidade regulatória.
59. O monitoramento pode envolver auditorias regulares, revisões de relatórios de segurança e testes de penetração.
60. A organização deve determinar o que deve ser monitorado e medido, incluindo processos, controles e requisitos de proteção de dados e segurança da informação.
61. Métodos para o monitoramento que consigam gerar resultados válidos e comparáveis devem ser definidos pela organização.
62. A organização deve definir o período para a realizar o monitoramento do provedor de serviços e suas soluções de TI.

63. Definir quando os resultados do monitoramento e de medições devem ser analisados.
64. Definir quem deve analisar e avaliar o resultado do monitoramento e da medição.
65. Definir quem é o responsável pelo monitoramento do provedor de serviços.
66. Toda a documentação do monitoramento deve ser retida como evidência dos resultados.
67. O monitoramento de conformidade do provedor de serviços pode ser implementado de maneira automatizada por meio de soluções de gerenciamento de riscos e conformidade.
68. Os registros detalhados de todas as interações com o provedor de serviços, incluindo comunicações, incidentes de segurança e auditorias deve ser mantido por [período].
69. Implementar um sistema de alerta precoce para notificar o [órgão/empresa/fundação] sobre quaisquer anomalias ou comportamentos suspeitos por parte do provedor de serviços.
70. Um inventário organizado dos provedores de serviços deve ser mantido atualizado de forma a permitir identificar um ponto de contato com cada prestador de serviços.
71. Os provedores de serviços devem ser listados, classificados e designados em contato formal para cada provedor de serviços.
72. A revisão e atualização do inventário de provedores de serviços deve ser feita a cada [período] ou quando ocorrerem mudanças significativas que possam impactar esta salvaguarda.
73. Desenvolver painéis de controle personalizados para visualizar métricas de privacidade, proteção de dados e segurança da informação em tempo real relacionadas aos provedores de serviços.
74. Realizar processo abrangente de diligência (*due diligence*) para avaliar a credibilidade, reputação e práticas de segurança cibernética do provedor de serviços. Isso envolve revisar suas políticas de segurança, histórico de incidentes de segurança e certificações relevantes.
75. A organização poderá utilizar a avaliação dos serviços e produtos prestados pelos provedores de serviço para verificar se estes atingiram os níveis de proteção de dados e segurança da informação necessários.

[Acrescentar as diretrizes para o monitoramento de provedores de serviços].

Da Gestão de Incidentes

76. Definir os requisitos mínimos de notificação de incidentes de segurança de dados pelo provedor de serviços, incluindo prazos e formato da comunicação.
77. Procedimentos claros e responsabilidades devem ser estabelecidos para lidar com incidentes de segurança cibernética relacionados aos serviços fornecidos pelo provedor.
78. Dentre os procedimentos pode-se incluir a comunicação eficaz, investigação de incidentes e ações corretivas para mitigar danos e evitar recorrências.
79. Tratar incidentes de segurança da informação e violações a proteção de dados e privacidade que por algum motivo estejam correlacionados a algum provedor de serviços.
80. Fazer uso de medidas de recuperação, contingência e resiliência cibernética para garantir a disponibilidade do tratamento de dados e informações dos provedores e do [órgão/empresa/fundação].

81. Mitigar qualquer ação do provedor de serviços que venha causar dano o [órgão/empresa/fundação], independente da maneira que o [órgão/empresa/fundação] tomou conhecimento da ação.
82. Integrar planos de resposta a incidentes comuns com o provedor de serviços para facilitar a coordenação e colaboração durante incidentes de segurança de dados.
83. Designar pontos de contato dedicados entre o [órgão/empresa/fundação] e o provedor de serviços para facilitar a comunicação e a troca de informações durante incidentes de segurança.
84. Implementar simulações regulares de incidentes de segurança com o provedor de serviços para garantir uma resposta coordenada e eficaz.
85. Documentar todas as interações e atividades relacionadas à resposta a incidentes com o provedor de serviços para fins de revisão e análise pós-incidente.
86. Estabelecer um protocolo claro para a condução de investigações conjuntas com o provedor de serviços para identificar a causa raiz de incidentes de segurança.
87. Realizar revisões pós-incidente em colaboração com o provedor de serviços para identificar áreas de melhoria nos processos de resposta a incidentes.
88. Fornecer treinamento regular aos colaboradores sobre os procedimentos de notificação de incidentes e como interagir com o provedor de serviços durante um incidente de segurança.

[Acrescentar as diretrizes para a gestão de incidentes].

Da Revisão e Melhoria Contínua

89. A PGPS dever ser revisada a cada [período] para garantir sua eficácia contínua e alinhamento com as melhores práticas de privacidade, proteção de dados e segurança da informação.
90. Manter-se atualizado sobre a legislação e melhores práticas de mercado em relação a gestão de provedores de serviço e adaptar as políticas conforme necessário para manter a relevância e eficácia.
91. Estabeleça canais de comunicação para receber feedback contínuo dos usuários internos e externos sobre a qualidade dos serviços dos provedores, utilizando essas informações para ajudar a melhorar a PGPS.
92. Lições aprendidas com incidentes passados e mudanças no ambiente operacional devem ser incorporadas para aprimorar os processos e controles.
93. Estabelecer um processo formal para revisão e validação dos relatórios de conformidade fornecidos pelo provedor de serviços.

[Acrescentar as diretrizes para a melhoria contínua].

Treinamento e Conscientização

94. Desenvolver materiais de treinamento personalizados para colaboradores de diferentes níveis e funções na organização sobre a gestão de provedores de serviços.
95. Realizar sessões de treinamento interativo e workshops para simular cenários práticos envolvendo provedores de serviços e práticas recomendadas de segurança.

96. Estabelecer um programa de recompensas e reconhecimento para funcionários que demonstrarem um bom entendimento e adesão às políticas de gestão de provedores de serviços.
97. Fornecer recursos online acessíveis, como vídeos, guias e FAQs, para facilitar o aprendizado contínuo sobre segurança de dados e gestão de provedores de serviços.
98. Incorporar o treinamento sobre gestão de provedores de serviços e segurança de dados em programas de integração de novos funcionários e treinamentos regulares de reciclagem.
99. Realizar avaliações periódicas de conhecimento e conscientização entre os funcionários para medir a eficácia do treinamento sobre gestão de provedores de serviços.
100. Incentivar a participação em eventos e conferências do setor relacionados a proteção de dados e segurança da informação para promover a educação contínua e a conscientização.

[Acrescentar as diretrizes para treinamentos e conscientização].

Encerramento de Contrato

101. O provedor de serviço deverá realizar atividades para o descarte seguro de dados e informações nos ativos de informação que estão sob sua responsabilidade ou foram utilizados para a prestação de serviço.
102. Contratos que utilizem a locação de ativos computacionais devem estabelecer o estado de preservação quando o ativo for devolvido.
103. Definir requisitos para garantir o término seguro de relacionamentos com os provedores e associados, incluindo, mas não se limitando a:
    a. Tratamento de informações;
    b. Desprovisionamento de direitos de acessos;
    c. Determinação da propriedade intelectual dos artefatos desenvolvidos durante o contrato;
    d. Possível portabilidade e repasse de informações em caso de alteração de provedor ou internalização de serviços;
    e. Atualização do inventário de provedores;
    f. Gerenciamento de registros;
    g. Devolução de ativos de informação;
    h. Descarte e eliminação segura de informações e ativos de informação utilizados pelos provedores e seus associados.
104. O prestador de serviço deverá realizar a limpeza segura dos ativos de informação utilizados no contrato.

[Acrescentar as diretrizes para encerramento de contrato].

Não conformidade

Descrever claramente as consequências (legais e/ou disciplinares) para o não cumprimento da PGPS. Pode ser pertinente descrever o processo de escalonamento para repetida não conformidade.

Ex.: Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

Exemplo:

a) Processo Administrativo Disciplinar de acordo com a legislação aplicável;
b) Exoneração;
c) Ação judicial de acordo com as leis aplicáveis e acordos contratuais;
d) Rescisão contratual ao bem do serviço público.

Concordância

Inclua uma seção que confirme o entendimento e o acordo para cumprir a política. Assinaturas e datas são necessárias. Uma declaração de amostra é fornecida abaixo.

Eu li e entendi a Política de Gestão de Provedores de Serviços do [órgão/empresa/fundação]. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do [órgão/empresa/fundação].

[Acrescentar mais informações sobre a concordância].

Nome do Servidor/Empregado

Assinatura do funcionário e data