Guia do Framework de Privacidade e Segurança da Informação

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.1.3

Brasília, março de 2024

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

Afrânio Henrique Teixeira Machado

Bruno Pierre Rodrigues de Sousa

Erion Dias Monteiro

Ivaldo Jeferson De Santana Castro

Francisco Magno Felix Nobre

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Marcus Paulo Barbosa Vasconcelos

Rafael da Silva Ribeiro

Raphael César Estevão

Rogério Vinícius Matos Rocha

Romário César de Almeida

Valdecy Oliveira de Araújo

William Oliveira Lima

Yuri Arcanjo De Carvalho

EQUIPE TÉCNICA DE REVISÃO

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Julierme Rodrigues da Silva

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
04/11/2022	1.0	Primeira versão do Guia do Framework de Privacidade e Segurança da Informação	Equipe Técnica de Elaboração
30/03/2023	1.1	Atualizações realizadas no Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo VI.	Equipe Técnica de Revisão
14/06/2023	1.1.1	Ajuste da medida 31.2 contemplada no Anexo V, conforme destacado no Anexo VI.	Equipe Técnica de Revisão
06/09/2023	1.1.2	Padronização do termo “Unidade de Controle Interno” e atualização da Figura 5.	Equipe Técnica de Revisão
21/03/2024	1.1.3	Ajuste da fórmula do iMC em alinhamento com a Ferramenta do Framework.	Equipe Técnica de Revisão

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

ABNT/NBR	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
APF	Administração Pública Federal
API	*Application Programming Interface* (Interface de Programação de Aplicação)
Audin	Auditoria Interna
CGU	Controladoria-Geral da União
CIS	*Center for Internet Security*
Ciset	Secretarias de Controle Interno
CSA	*Control Self-Assessment*
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
DSIC	Departamento de Segurança da Informação e Comunicações
Dump	Contém um registro da estrutura de tabela e ou dados de um banco de dados, e normalmente está na forma de uma lista de declarações SQL.
E-CIBER	Estratégia Nacional de Segurança Cibernética
ETIR	Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais
EUA	Estados Unidos da América
GCD	Governança no Compartilhamento de Dados
GI	Grupo de Implementação
GRC	Governança, Riscos e *Compliance*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IDP	Inventário de Dados Pessoais
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusão)
IN	Instrução Normativa
iMC	*Indicador de Maturidade por Controle*
IoT	*Internet of Things* (Internet das Coisas)
IP	*Internet Protocol*
iPriv	Indicador de Privacidade
IPS	*Intrusion Prevention System* (Sistema de Prevenção de Intrusão)
iSeg	Indicador de Segurança
ISO/IEC	*International Organization of Standardization/International Electrotechnical Commission*
ITAM	*IT Asset Management* (Gerenciamento de Ativos de TI)
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais

MCI	Marco Civil da Internet
NC	Normas Complementares
NIST	*National Institute of Standards and Technology*
NSC	Núcleo de Segurança e Credenciamento
PDCA	Método iterativo de gestão de quatro passos (*Plan, Do, Check e Act*), utilizado para o controle e melhoria contínua de processos e produtos.
PMC	Somatório das pontuações das medidas avaliadas no controle QMC
PNSI	Política Nacional de Segurança da Informação
PPSI	Programa de Privacidade e Segurança da Informação
QMC	Quantidade de Medidas do Controle
QMNAC	Quantidade de Medidas não Aplicáveis do Controle
RIPD	Relatório de Impacto de Proteção de Dados
SaaS	*Software as a Service* (Software como um Serviço)
SCI	Sistema de Controle Interno
SGD/MGI	Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos
SGIP	Sistema de Gerenciamento de Informações de Privacidade
SIEM	*Security Information and Event Management* (Gerenciamento e Correlação de Eventos de Segurança)
SLA	*Service Level Agreement* (Acordo de Nível de Serviço)
SQL injection	*Structured Query Language Injection*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal – APF, visa a difundir as melhores práticas em matéria de privacidade e segurança da informação, em atendimento à Política Nacional de Segurança da Informação (PNSI – Decreto nº 9.637, de 26 de dezembro de 2018), ao "CAPÍTULO VII – DA SEGURANÇA E DAS BOAS PRÁTICAS" da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018) e outros normativos vigentes sobre o tema de privacidade, proteção de dados pessoais e segurança da informação, o que não impede de ser aproveitado por outras instituições que busquem orientações sobre o tema.

Este documento é de autoria exclusiva da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, contendo referências a publicações e a outros documentos técnicos, com destaque para aqueles do *Center for Internet Security* (CIS)[1], do *National Institute of Standards and Technology* (NIST)[2], da *International Standardization Organization/Eletrotechnical Commission* (ISO/IEC)[3] e da Associação Brasileira de Normas Técnicas (ABNT NBR)[4]. Muitas das referências foram traduzidas de forma livre pelos técnicos da SGD com propósitos educativos e não comerciais a fim de difundir tais conhecimentos para as instituições públicas.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, do NIST, da ABNT NBR ou da ISO/IEC e vice-versa;

b) não se manifesta em nome do TCU, da CGU, do GSI e da ANPD;

c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente **Guia**;

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações do CIS, do NIST ou da ISO/IEC em suas versões originais, na língua inglesa, deverá consultar diretamente as fontes oficiais de informação ofertadas pelas referidas instituições.

Agradecimento especial ao CIS, ao NIST, à ABNT NBR e à ISO/IEC pelas valiosas

[1] Disponível em: https://www.cisecurity.org/
[2] Disponível em: https://www.nist.gov/
[3] Disponível em: https://www.iso.org/standards.html
[4] Disponível em: https://www.abntcatalogo.com.br/

contribuições para a comunidade de privacidade e segurança da informação.

Cumpre também reconhecer a fundamental parceria com o Governo do Reino Unido, no âmbito do Programa de Acesso Digital, que viabilizou o desenvolvimento de uma ferramenta para aplicação do framework proposto por esta publicação.

INTRODUÇÃO

O **Guia do Framework de Privacidade e Segurança da Informação** é uma adição à série de guias operacionais[5] elaborados pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos para fomentar a privacidade, a proteção de dados pessoais e a segurança da informação[6].

O objetivo deste **Guia** é propor às instituições públicas diretrizes no sentido de auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de privacidade e segurança da informação presentes na instituição com base nas obrigações da PNSI e LGPD, bem como, nos controles elaborados pelo (a) CIS, NIST, ISO/IEC e ABNT NBR.

O **Framework de Privacidade e Segurança da Informação** constante deste **Guia** está organizado nos seguintes capítulos e anexos:

- O Capítulo 1 destaca sua fundamentação e estruturação dos controles;
- O Capítulo 2 descreve o controle de estruturação básica de gestão em privacidade e segurança da informação;
- O Capítulo 3 descreve os controles de segurança cibernética adotados pelo framework;
- O Capítulo 4 descreve os controles de privacidade adotados pelo framework;
- O Capítulo 5 trata da implementação dos controles de privacidade e segurança cibernética;
- O Capítulo 6 contempla a forma de avaliação de maturidade da instituição;
- O Capítulo 7 menciona a utilização de uma ferramenta para acompanhamento da implementação deste **Framework**.
- O Capítulo 8 apresenta as considerações finais, ressaltando os benefícios esperados com a aplicação do framework pelas instituições;
- O Anexo I apresenta o modelo de avaliação de criticidade de sistemas;
- O Anexo II traz uma lista com os normativos do GSI/PR;
- O Anexo III apresenta o controle de estruturação básica em privacidade e segurança da informação;
- O Anexo IV lista em formato de questões as medidas dos controles CIS; e

[5] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd
[6] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

- O Anexo V elenca em formato de questões as medidas dos controles de privacidade.

Ressalta-se que a instituição é livre para adequar todas as proposições deste documento a sua realidade. A abordagem proposta oferece uma sugestão de uso dos controles e medidas de privacidade e segurança da informação, contudo, esse fato não exclui a necessidade de que a instituição compreenda sua própria postura de risco institucional. A intenção é ajudar a organização a concentrar seus esforços com base nos recursos disponíveis, integrando-os a qualquer processo de gestão de risco pré-existente.

Nesse sentido, reforça-se que a adoção do framework não equivale necessariamente ao cumprimento da legislação brasileira vigente sobre privacidade, proteção de dados pessoais e segurança da informação, em especial a PNSI e a Lei nº 13.709, de 14 de agosto de 2018 – LGPD. Contudo, o presente Guia seguramente poderá auxiliar a instituição adotante a atingir os objetivos previstos nas normas correlatas, ao permitir a visualização da maturidade de seus trabalhos de privacidade, de proteção de dados, e de segurança da informação de forma a ampliar a implementação das melhores práticas sobre o tema.

Este **Guia** será revisto e atualizado anualmente ou sempre que se fizer necessária a inclusão de ajustes para acompanhar o amadurecimento dos processos de privacidade e segurança da informação, bem como para alinhamento às novas determinações especificadas pela ANPD e GSI.

1. FUNDAMENTAÇÃO E ESTRUTURAÇÃO DOS CONTROLES

O **Framework de Privacidade e Segurança da Informação** é resultado de extensa pesquisa de abordagens e modelos para implementação de controles e medidas que visam a assegurar a privacidade, a proteção de dados pessoais e a segurança da informação.

Existe uma gama extraordinária de normas, frameworks e guias disponíveis atualmente no mercado sobre os temas de privacidade, proteção de dados pessoais e segurança da informação. Esses modelos e orientações variam desde os mais abrangentes, com controles e medidas aplicáveis em qualquer negócio, até os mais específicos, que consideram detalhes de normas vigentes em um país específico. Ambos os casos necessitam de uma adaptação para a realidade de quem os adota.

A estratégia utilizada para a construção do Framework deste **Guia** não consistiu em adotar uma única referência específica e sim na combinação de algumas das mais abrangentes. A combinação se justifica pela complementação, na medida do possível, dos *gaps* presentes em cada referência adotada de forma a atender a pluralidade de serviços e de tratamento de dados pessoais pelo Poder Público. A APF tem diversos órgãos, com políticas públicas próprias e atribuições institucionais específicas, isto é, o que se aplica a um órgão, pode não se aplicar a outro.

A fundamentação do **Framework** aborda normas legais de conformidade e é inspirada na: abordagem de controles e implementação do CIS (CIS, 2021), estrutura do núcleo do *Privacy Framework* (NIST, 2020) e normas ISO/IEC e ABNT NBR. Tal fundamentação é destacada pelas seções a seguir.

Importante ressaltar que este **Guia** não substitui a avaliação dos documentos originais que embasaram a estruturação deste **Framework**.

1.1 Normas Legais de Conformidade

A necessidade de elaboração e adoção de um Framework de Privacidade e Segurança da Informação vem ao encontro da exigência de conformidade com normas vigentes, tais como a Lei n° 13.709, de 14 de agosto de 2018 - LGPD, as publicações ANPD e as Instruções Normativas (INs) ou Normas Complementares (NCs) estabelecidas pelo GSI/PR que serão destacadas na sequência deste **Guia**.

Embora a LGPD, as publicações ANPD e os Normativos do GSI/PR demandem as principais ações de conformidade em privacidade, proteção de dados pessoais e segurança da informação, isto não isenta a alta administração e o gestor do negócio de

estarem cientes e em conformidade com outras normas relativas à segurança da informação, a proteção de dados e privacidade vigentes, dentre as quais pode-se destacar:

- Privacidade, com especial atenção à proteção de dados pessoais e dados pessoais sensíveis dos titulares:
    - Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI);
    - Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet (MCI);
    - Decreto nº 10.046, de 09 de outubro de 2019, Governança no Compartilhamento de Dados (GCD);
    - IN SGD/ME nº 117, de 19 de novembro de 2020[7];
    - IN SGD/ME nº 31, de 23 de março de 2021[8];
    - Documentos e Publicações da ANPD[9].
- Segurança da Informação, com especial atenção quanto à segurança cibernética:
    - Decreto nº 10.222, de 05 de fevereiro de 2020, Estratégia Nacional de Segurança Cibernética (E-CIBER);
    - Decreto nº 10.748, de 16 de julho de 2021, Rede Federal de Gestão de Incidentes Cibernéticos;
    - Portaria GSI/PR nº 93, de 18 de outubro de 2021, Glossário de Segurança da Informação.

1.1.1 *LGPD*

A LGPD dispõe sobre o tratamento de dados pessoais das pessoas naturais, dispostos em meio físico ou digital, definindo as hipóteses em que tais dados podem legitimamente ser utilizados por terceiros e estabelecendo mecanismos para proteger os titulares dos dados contra usos inadequados.

A lei é aplicável ao tratamento de dados realizado por pessoas naturais ou por pessoas jurídicas de direito público ou privado, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade

[7] Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596
[8] Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-31-de-23-de-marco-de-2021-310081084
[9] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

da pessoa natural.

Seu objetivo é proteger os direitos fundamentais relacionados à esfera informacional do titular de dados pessoais. Assim, a Lei introduziu uma série de novos direitos que asseguram maior transparência quanto ao tratamento dos dados e conferem protagonismo ao titular quanto ao seu uso.

Dentre as diversas ações a serem observadas na LGPD, destacam-se os direitos dos titulares de dados pessoais, previstos no Capítulo III, as hipóteses de tratamento previstas no Capítulo II, o tratamento de dados pessoais pelo Poder Público, previsto no Capítulo IV, as obrigações dos agentes de tratamento, previstas no Capítulo VI, a transferência internacional de dados pessoais, prevista no Capítulo V e a segurança de dados pessoais e as boas práticas a serem observadas no Capítulo VII.

1.1.2 *Publicações da ANPD*

A Autoridade Nacional de Proteção de Dados (ANPD) tem a missão precípua de zelar pela proteção de dados pessoais e por regulamentar e fiscalizar o cumprimento da LGPD no País, a fim de promover a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos. Suas principais competências estão listadas no artigo 55-j da LGPD. No cumprimento dessas competências, a ANPD tem realizado diversas publicações, e há perspectivas da publicação de enunciados, que servirão de substantiva orientação aos órgãos da Administração Pública Federal na conformidade à LGPD. As publicações da ANPD podem ser encontradas no sítio da Autoridade na internet em Publicações da ANPD[10].

1.1.3 *Normativos do GSI*

O GSI/PR planeja, coordena e supervisiona a atividade de segurança da informação no âmbito da APF. O GSI/PR, na condição de órgão governante superior, publica normativos (INs e NCs) de cumprimento obrigatório que norteiam as ações de segurança da informação na APF.

Diversos domínios relacionados à segurança da informação e cibernética já são contemplados por INs e NCs vigentes, dentre as quais podem-se destacar a IN GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da APF, a IN GSI/PR nº 5, de 31 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para

[10] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da APF e a NC nº 05/IN01/DSIC/GSIPR, e seu anexo que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da APF.

As demais INs e NCs do GSI, entre outras legislações, portarias e mais detalhes podem ser acessados em: Normativos GSI[11].

1.1.4 *PNSI*

Com o objetivo de estabelecer estrutura e modelo de governança para a integração e a coordenação nacional das atividades de segurança da informação, o GSI/PR coordenou uma série de ações voltadas para a elaboração da Política Nacional de Segurança da Informação (PNSI).

A PNSI tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. Essa política abrange: segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais.

Para mais detalhes, a Política Nacional de Segurança da Informação instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 pode ser acessada em: PNSI GSI/PR.

1.2 Estruturação básica de gestão em privacidade e segurança da informação

A estruturação básica de gestão em privacidade e segurança da informação tem bases na política de governança da APF direta, autárquica e fundacional estabelecida no Decreto nº 9.203, de 22 de novembro de 2017, que define governança pública como o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade, bem como apresenta o conceito de gestão de riscos como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

O Decreto ainda destaca como diretrizes da governança pública dois comandos relacionados ao contexto do presente documento: "direcionar ações para a busca de

[11] Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao

resultados para a sociedade, encontrando soluções tempestivas e inovadoras para lidar com a limitação de recursos e com as mudanças de prioridades, bem como implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores".

Tal norma fornece direcionadores para a alta administração das organizações da APF direta, autárquica e fundacional, que deverão estabelecer, manter, monitorar e aprimorar sistemas de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os princípios indicados no Decreto.

Dessa forma, a Estrutura Básica de Gestão em Privacidade e Segurança da Informação no âmbito dos órgãos e entidades da APF, direta e indireta, contempla os seguintes papéis fundamentais para condução e implementação deste **Framework**:

- o Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;
- o Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis;
- o Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;
- o Responsável pela Unidade de Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa

prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017;

- o Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;
- a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da APF, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do GSI/PR; e
- a Política de Segurança da Informação - POSIN, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

O responsável pela Unidade de Controle Interno integra a segunda linha de defesa nos termos da IN CGU nº 3, de 9 de junho de 2017. Os demais papéis que constituem a Estrutura Básica de Gestão em Privacidade e Segurança da Informação, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas, compõem a primeira linha de defesa, quando se tratar de controles de privacidade e segurança da informação, tendo o Encarregado o papel de apoiar com orientações nas questões que envolvam privacidade e proteção de dados pessoais nos termos do art. 41, da Lei 13.709/2018.

1.3 Abordagem de controles e implementação de cibersegurança

O CIS é uma organização sem fins lucrativos voltada para a comunidade, responsável pelo *CIS Critical Security Controls v8* e *CIS Controls v8 Privacy Companion Guide,* melhores práticas reconhecidas globalmente para proteger sistemas e dados de TI. Lidera uma comunidade global de profissionais de TI para evoluir continuamente esses padrões e fornecer produtos e serviços para proteger proativamente contra ameaças emergentes.

O Guia CIS v.8 adota as funções de Cibersegurança do Framework do NIST como complemento às medidas trazidas no documento. O NIST é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. Na área de segurança Cibernética ela tem como função identificar e desenvolver diretrizes de risco de segurança cibernética para uso voluntário de proprietários e operadores de infraestrutura crítica.

Os controles e medidas de cibersegurança deste **Guia** foram embasados no Guia

CIS Controls v8, o qual compartilha percepções sobre ataques e invasores, identifica as causas básicas e as traduz em classes de ação defensiva. Além disso, o CIS, por meio do seu Guia, mapeia seus controles com estruturas regulatórias e de *compliance*, a fim de garantir o alinhamento e trazer prioridade e foco para eles. Adicionalmente, o CIS identifica, em seu Guia, problemas e barreiras comuns (como avaliação inicial e roteiros de implementação), e os resolve como uma comunidade.

Os Controles CIS são desenvolvidos por uma comunidade de especialistas em TI que aplicam sua experiência em primeira mão como defensores cibernéticos para criar essas melhores práticas de segurança globalmente aceitas. Esses especialistas vêm de uma ampla gama de setores, incluindo varejo, manufatura, saúde, transporte, educação, governo, entre outros.

A aplicação dos controles do CIS consiste em um importante passo de um processo para orientar o programa de melhoria de segurança da instituição, sendo **importante destacar que o documento não se trata de "somente uma lista" de boas práticas que podem ajudar na segurança da instituição, e sim de um documento confiável com recomendações de segurança e suporte de uma comunidade de especialista para tornar os controles implementáveis, utilizáveis, escaláveis e alinhados com todos os requisitos de segurança da indústria ou do governo.**

Vale ressaltar que o TCU considera uma boa prática a implementação dos controles do CIS v8, visto que os utiliza no acompanhamento de controles críticos de segurança cibernética das organizações públicas federais. A implementação desses controles, inicialmente, foi aprovada por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de *backup/restore* dos órgãos e entidades da APF). Nesse sentido, o TCU mediante o Acórdão 1.768/2022-TCU-Plenário reforçou a adoção dos dezoito controles críticos da versão 8 do CIS a serem gradativamente verificados ao longo de sete ciclos de execução de auditorias nas instituições públicas. Mais detalhes podem ser encontrados em Auditoria de Cibersegurança do TCU.

1.3.1 *CIS Controls - Cibersegurança*

O documento *CIS Critical Security Controls v8*[12] é um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura de rede por meio de controles que aplicam as melhores práticas para mitigar os mais comuns tipos

[12] Disponível em: https://www.cisecurity.org/controls

de ataques cibernéticos.

O Guia *CIS Controls v8* é composto de 18 controles que abordam os diversos temas da cibersegurança, tais como: ativos, cópia segura, proteção de dados, contas e acesso, incidentes, vulnerabilidades, monitoramento e auditoria, entre outros.

A estrutura dos controles do CIS apresenta os seguintes elementos:

- Visão geral: Uma breve descrição da intenção do Controle e sua utilidade como ação defensiva;
- Por que este controle é crítico? Uma descrição da importância deste Controle no bloqueio, mitigação ou identificação de ataques, e uma explicação de como os invasores exploram ativamente a ausência deste Controle;
- Medidas de Segurança: uma tabela das ações específicas que as empresas devem realizar para implementar o Controle.

1.3.2 *CIS Guia Complementar de Privacidade*

Quanto à privacidade e proteção de dados pessoais, o CIS por meio do documento CIS *Controls Privacy Guide*[13], tem o objetivo de desenvolver as melhores práticas e orientações para a implementação dos *CIS Critical Security Controls* (*CIS Controls*), levando em consideração os impactos na privacidade e proteção de dados pessoais tratados pela instituição. O Guia apoia os objetivos dos Controles CIS, alinhando os princípios de privacidade e destacando possíveis preocupações referentes à proteção de dados pessoais que possam surgir ao utilizar os Controles CIS.

As orientações apresentadas no CIS *Controls Privacy Guide* contribuem para que a equipe de TI, jurídica ou outras com responsabilidades pela privacidade e proteção de dados pessoais na instituição possam identificar oportunidades e agregar suas considerações previamente na implementação dos controles de cibersegurança em seus sistemas informacionais, abordando a segurança dos dados pessoais por padrão desde a sua concepção. Portanto, recomenda-se a leitura do CIS *Controls Privacy Guide* durante a implementação dos controles e medidas de cibersegurança.

1.3.3 *Grupos de Implementação*

As medidas contidas nos controles do CIS auxiliam a mitigação das

[13] Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide

vulnerabilidades dos mais comuns aos mais avançados tipos de ataque. Dessa forma, existem medidas com mais complexidade em serem implementadas do que outras.

O CIS elaborou uma metodologia de implementação das medidas que auxiliam a mitigação das vulnerabilidades numa organização. Essa metodologia consiste em 3 Grupos de Implementação (GI). O primeiro GI representa uma instituição de pequeno a médio porte com limitação no corpo de profissionais em TI e na experiência em cibersegurança. O segundo GI representa uma instituição que emprega indivíduos responsáveis por gerenciar e proteger a infraestrutura de TI. Por fim, o terceiro GI emprega especialistas em segurança especializados nas diferentes facetas da segurança cibernética.

Reforça-se que os três GIs acima tentam criar uma identificação de perfil e ajudar a instituição no amadurecimento das linhas de defesa, de forma gradativa. Esse quadro não impede que medidas de segurança de perfil mais avançado sejam implementados na instituição.

Vale ressaltar que cada GI indica medidas de segurança cibernética que devem ser atendidas e são cumulativas a cada GI avançado.

1.3.4 *NIST Cybersecurity Framework*

O Framework de Cibersegurança do NIST[14] conceitua a Estrutura Básica de Segurança Cibernética. Trata-se de um conjunto de atividades de segurança cibernética que visam a produzir resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica.

A Estrutura Básica consiste em cinco funções simultâneas e contínuas — **Identificar, Proteger, Detectar, Responder** e **Recuperar**. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização.

- **Identificar** - Desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos.

As atividades na função **"Identificar"** são fundamentais para o uso eficiente do Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica[15]. Uma organização é capaz de focar e priorizar seus esforços de forma consistente com sua

[14] Disponível em: https://www.nist.gov/cyberframework/framework
[15] Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018pt.pdf

estratégia de gerenciamento de riscos e demandas empresariais, a partir da compreensão do contexto de seu nicho, dos recursos que suportam funções críticas e dos riscos de segurança cibernética envolvidos. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Ativos; Ambiente Empresarial; Governança; Avaliação de Risco; e Estratégia de Gerenciamento de Risco.

- **Proteger** - Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos.

A função **"Proteger"** fornece apoio à capacidade de limitar ou conter o impacto de uma possível ocorrência de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Identidade e Controle de Acesso; Conscientização e Treinamento; Segurança de Dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção.

- **Detectar** - Desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética.

A função **"Detectar"** permite a descoberta oportuna de ocorrências de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Anomalias e Ocorrências; Monitoramento Contínuo de Segurança; e Processos de Detecção.

- **Responder** - Desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado.

A função **"Responder"** suporta a capacidade de conter o impacto de um possível incidente de segurança cibernética. Exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Resposta; Notificações; Análise; Mitigação; e Aperfeiçoamentos.

- **Recuperar** - Desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

A função **"Recuperar"** oferece apoio ao restabelecimento pontual para as operações normais de modo a reduzir o impacto de determinado incidente de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Restabelecimento; Aperfeiçoamentos; e Notificações.

1.4 Abordagem de controles e implementação de privacidade

Os controles e medidas de privacidade foram baseados nas principais referências de privacidade disponibilizadas atualmente. Foram utilizadas como base as normas ISO/IEC relativas à privacidade e proteção de dados pessoais e como referência complementar o Framework de Privacidade do NIST publicado em 2020[16]. Todos os controles e medidas presentes nestas duas referências foram correlacionados com a LGPD, considerando também orientações dos Guias publicados pela ANPD.

A ISO/IEC é uma organização internacional não governamental independente, com membros de normalização de vários países. Ela reúne especialistas para compartilhar conhecimento e desenvolver normas internacionais voluntárias, baseadas em consenso e relevantes para o mercado mundial que apoiam a inovação e soluções para os desafios globais. Já a ABNT NBR é um conjunto de normas e diretrizes de caráter técnico que tem como função padronizar processos nacionais e internacionais para a elaboração de produtos e serviços no Brasil.

Dentre os diversos documentos publicados pela ISO/IEC e ABNT NBR este **Guia de Framework de Privacidade e Segurança da Informação** tem como base principal as seguintes publicações: ISO/IEC 29100:2011[17], ISO/IEC 29151:2017[18], ABNT NBR ISO/IEC 27701:2019[19], ISO/IEC 27018:2014[20], ISO/IEC 29134:2017[21] e a ABNT NBR ISO/IEC 29184:2021[22].

Além das publicações ISO/IEC e ABNT NBR mencionadas, o Framework de Privacidade do NIST teve uma contribuição bastante significativa na construção deste **Guia.** O NIST é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos que promove a inovação e a competitividade industrial nos EUA (Estados Unidos da América) por meio do avanço da ciência, dos padrões e da tecnologia de medição de forma a aumentar a segurança econômica e melhorar a qualidade de vida. Em relação à privacidade de dados, ela tem como função: o gerenciamento de risco de privacidade por meio da conexão entre a empresa e os responsáveis pela missão, funções e responsabilidades organizacionais,

[16] Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020pt.pdf
[17] Disponível em: https://www.iso.org/standard/45123.html
[18] Disponível em: https://www.iso.org/standard/62726.html
[19] Disponível em: https://www.abntcatalogo.com.br
[20] Disponível em: https://www.iso.org/standard/61498.html
[21] Disponível em: https://www.iso.org/standard/62289.html
[22] Disponível em: https://www.abntcatalogo.com.br

e atividades de proteção à privacidade.

1.4.1 *ISO/IEC 29100:2011*

Esta norma internacional fornece uma estrutura de alto nível para a proteção de dados pessoais em sistemas de TI e Tecnologia da Informação e comunicação (TIC). É de natureza geral e coloca os aspectos organizacionais, técnicos e processuais em uma estrutura geral de privacidade.

A estrutura de privacidade trazida por essa norma destina-se a ajudar as organizações a definir seus requisitos de proteção de privacidade relacionados a dados pessoais tratados em um ambiente de TIC:

- especificando uma terminologia de privacidade comum;
- definindo os atores e seus papéis no processamento de dados pessoais;
- descrevendo os requisitos de proteção da privacidade; e
- referenciando princípios de privacidade conhecidos.

A seção 5 dessa norma apresenta os princípios de privacidade organizados em uma estrutura derivada de princípios desenvolvidos por vários países e organizações internacionais. Esses princípios devem ser usados para orientar o projeto, desenvolvimento e implementação de políticas e controles de privacidade. Além disso, eles podem servir como uma linha base no monitoramento e medição de aspectos de desempenho, *benchmarking* e auditoria de programas de gerenciamento de privacidade em uma organização.

Os princípios mencionados acima foram analisados e utilizados na construção dos controles de privacidade deste **Guia**.

1.4.2 *ISO/IEC 29151:2017*

A ISO/IEC 29151:2017 estabelece controles e diretrizes para atender aos requisitos identificados por uma avaliação de risco e impacto relacionado à proteção de dados pessoais.

Em particular, essa norma traz diretrizes baseadas na ISO/IEC 27002:2013[23], levando em consideração os requisitos para o processamento de dados pessoais que podem ser aplicáveis no contexto do(s) ambiente(s) de risco de segurança da informação de uma organização.

[23] Disponível em: https://www.iso.org/standard/54533.html

A ISO/IEC 27002:2013 fornece diretrizes para as organizações sobre a segurança da informação e práticas de gerenciamento. Esta norma foi projetada para ser usada por organizações que pretendem:

- selecionar controles dentro do processo de implementação de um Sistema de Gestão de Segurança da Informação baseado na ISO/IEC 27001[24];
- implementar controles de segurança da informação comumente aceitos;
- desenvolver suas próprias diretrizes de gerenciamento de segurança da informação.

Já a ISO/IEC 27001:2013 apresenta os requisitos para sistemas de gestão da segurança da informação.

A ISO/IEC 29151:2017 apresenta ainda uma extensão de controles voltados especificamente para a proteção de dados pessoais, baseados na ISO/IEC 29100:2011 e é aplicável a todos os tipos e tamanhos de organizações que atuam como controladores de dados pessoais, incluindo instituições públicas e privadas, entidades governamentais e organizações sem fins lucrativos.

A construção deste **Framework** se baseou principalmente na análise do Anexo A da ISO/IEC 29151:2017 que discorre sobre a extensão dos controles voltados para a proteção de dados pessoais.

1.4.3 *ABNT NBR ISO/IEC 27701:2019*

A ABNT NBR ISO/IEC 27701:2019 especifica os requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade (SGIP) na forma de uma extensão da ABNT NBR ISO/IEC 27001:2013[25] e ABNT NBR ISO/IEC 27002:2013[26] para gerenciamento de privacidade no contexto da organização.

Esse padrão traz os requisitos relacionados ao SGIP e fornece orientações para que os controladores e operadores de dados pessoais possam aperfeiçoar o programa de governança sobre os dados pessoais sob suas responsabilidades. A ABNT NBR ISO/IEC 27701:2019 é aplicável a todos os tipos e tamanhos de organizações, incluindo instituições públicas e privadas, entidades governamentais e organizações sem fins lucrativos.

[24] Disponível em: https://www.iso.org/standard/54534.html
[25] Disponível em: https://www.abntcatalogo.com.br
[26] Disponível em: https://www.abntcatalogo.com.br

Especificamente, em seus capítulos 7 e 8, a norma ABNT NBR ISO/IEC 27701:2019 traz diretrizes adicionais para controladores e operadores de dados pessoais, abordando os seguintes temas: condições para o tratamento, direitos dos titulares de dados pessoais, *Privacy by Default* e *Privacy by Design e* compartilhamento, transferência e divulgação de dados pessoais. A construção deste **Guia** se baseou principalmente na análise desses capítulos.

1.4.4 *ISO/IEC 27018:2014*

A ISO/IEC 27018:2014 é uma norma internacional sobre privacidade em serviços de computação em nuvem promovido pela indústria. É considerada um adendo à ISO/IEC 27001:2013, o primeiro código de prática internacional para privacidade na nuvem. Ela ajuda os provedores de serviços em nuvem que processam dados pessoais na avaliação de riscos e na implementação de controles para a proteção desses dados.

A ISO/IEC 27018:2014 se apresenta na forma de uma extensão da ISO/IEC 27001:2013 e ISO/IEC 27002:2013 voltada para o contexto de processamento de dados pessoais em nuvem. Ela apresenta ainda uma extensão de controles voltados especificamente para a proteção de dados pessoais em nuvem, baseados na ISO/IEC 29100:2011.

O objetivo dessa norma, quando usada em conjunto com os objetivos e controles de segurança da informação na ISO/IEC 27002:2013, é criar um conjunto comum de categorias e controles de segurança que podem ser implementados por um provedor de serviços de computação em nuvem pública atuando como um operador de dados pessoais.

A construção do **Guia** se baseou principalmente na análise do Anexo A que aborda a extensão dos controles voltados para a proteção dos dados pessoais tratados em nuvem por operadores terceiros.

1.4.5 *ISO/IEC 29134:2017*

A ISO/IEC 29134:2017 é uma norma internacional que fornece diretrizes para um processo de Avaliação de Impacto à Privacidade, estrutura e conteúdo que vai compor o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Os dois instrumentos são aplicáveis a todos os tipos e tamanhos de organizações e normalmente são conduzidos por uma organização que leva sua responsabilidade a sério ao tratar dados pessoais.

A construção do **Guia** se baseou principalmente na análise de impacto de

privacidade e na confecção do RIPD tratada na norma ISO/IEC 29134:2017 para que as instituições possam atender aos requisitos legais necessários.

1.4.6 *ABNT NBR ISO/IEC 29184:2021*

A ABNT NBR ISO/IEC 29184:2021 apresenta diretrizes que formatam o conteúdo e a estrutura das políticas (avisos) de privacidade *on-line*, bem como o processo de solicitação de consentimento para coletar e tratar dados pessoais dos titulares.

A análise dessa norma auxiliou principalmente na construção de controles voltados para a abertura, transparência e notificação neste **Guia**.

1.4.7 *NIST Privacy Framework*

O NIST Privacy Framework é destinado a ajudar as organizações a identificar e gerenciar o risco de privacidade para criar produtos e serviços inovadores, protegendo a privacidade dos indivíduos. Esse Framework conceitua a Estrutura Básica de Privacidade e aborda um conjunto de funções de privacidade de dados pessoais, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica.

As funções organizam as atividades fundamentais de privacidade em mais alto nível. Elas ajudam uma organização a expressar a sua gestão do risco de privacidade, ao entender e gerenciar o tratamento de dados, possibilitando decisões concernentes à gestão de risco, e ao determinar como interagir com os indivíduos, além de estabelecer melhorias ao aprender com atividades anteriores.

As funções não foram criadas para serem aplicadas de forma sequencial. Ao contrário, as funções devem ser aplicadas simultânea e continuamente para formar ou aprimorar uma cultura operacional que trate da natureza dinâmica do risco de privacidade.

A Estrutura Básica consiste em cinco funções simultâneas e contínuas — **Identificar-P, Governar-P, Controlar-P, Comunicar-P, Proteger-P**. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de privacidade de uma organização.

- **Identificar-P** - Desenvolve o entendimento organizacional para gerenciar riscos de privacidade dos indivíduos decorrentes do processamento de dados.

As atividades na função **“Identificar-P”** são fundamentais para avaliar as

circunstâncias em que os dados são tratados, entendendo os interesses de privacidade dos indivíduos que são servidos ou afetados direta ou indiretamente por uma instituição, além de realizar avaliações de risco, permite que uma organização entenda o ambiente de negócios em que está funcionando, e identifique e priorize riscos de privacidade.

- **Governar-P** - Desenvolve e implementa a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gestão de riscos da organização que são transmitidas pelo risco de privacidade.

A função **"Governar-P"** é fundamental para atividades de nível organizacional, como estabelecer valores e políticas de privacidade, identificar requisitos legais/regulatórios e entender a tolerância ao risco organizacional que permite que uma instituição concentre e priorize esforços que sejam consistentes com a sua estratégia de gestão de riscos e necessidades de negócios.

- **Controlar-P** – Desenvolve e implementa atividades adequadas para permitir que organizações ou indivíduos gerenciem dados com detalhamento suficiente para gerenciar riscos de privacidade.

A função **"Controlar-P"** leva em consideração o gerenciamento do processamento de dados do ponto de vista da organização e do indivíduo.

- **Comunicar-P** – Desenvolve e implementa atividades adequadas para permitir que organizações e indivíduos tenham uma compreensão confiável e permaneçam engajados em um diálogo sobre como os dados são processados, além dos riscos de privacidade a eles associados.

A função **"Comunicar-P"** reconhece que, tanto as organizações quanto os indivíduos gostariam de saber como os dados são processados para gerenciar o risco de privacidade de forma eficaz.

- **Proteger-P** - Desenvolve e implementa medidas para o processamento de dados.

A função **"Proteger-P"** abrange a proteção de dados para evitar eventos de privacidade relacionados à cibersegurança e a sobreposição entre privacidade e gerenciamento de riscos de cibersegurança.

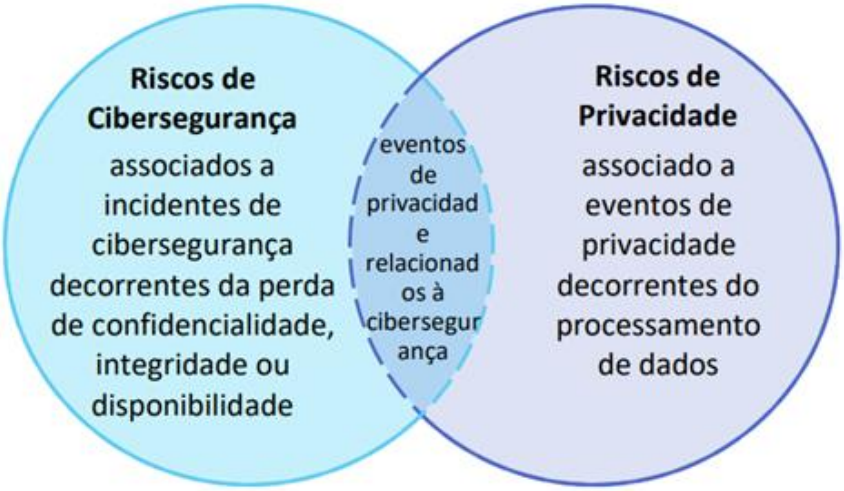
O núcleo do Framework de Privacidade do NIST é composto por Funções, Categorias e Subcategorias. Esses elementos do núcleo trabalham juntos.

As Categorias são as subdivisões de uma função em grupos de resultados de privacidade intimamente ligados às necessidades programáticas e atividades

específicas. Essas Categorias representam grupos de domínios específicos de privacidade e podem ser interpretadas como controles. Já as subcategorias dividem ainda mais uma categoria em resultados específicos de atividades técnicas e/ou de gestão que podem ser interpretadas em ações ou medidas de proteção de dados pessoais e privacidade. Elas fornecem um conjunto de resultados que, embora não sejam completos, ajudam a validar o efeito do que foi encontrado em cada categoria.

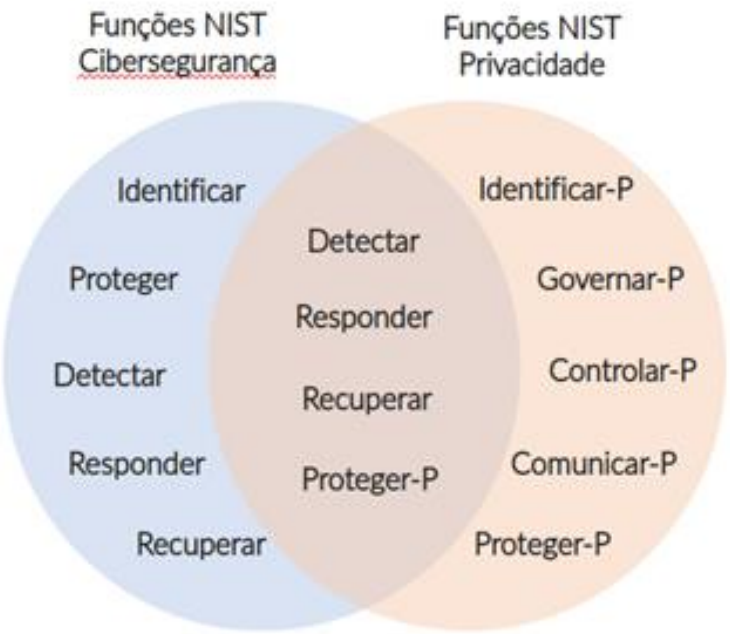
Embora o *Cybersecurity Framework* tenha sido criado para cobrir todos os tipos de incidentes de cibersegurança, ele pode ser usado para alavancar mais apoio à gestão de riscos dos eventos de privacidade, como pode ser visto na Figura 1 abaixo.

Figura 1: RELAÇÃO ENTRE OS RISCOS DE CIBERSEGURANÇA E PRIVACIDADE.



Portanto, existe uma relação entre a área de privacidade e cibersegurança. De acordo com o NIST, a privacidade e a cibersegurança compartilham funções para atender aos eventos de privacidade relacionados à cibersegurança, conforme Figura 2 a seguir.

Figura 2: RELAÇÃO ENTRE AS FUNÇÕES DE CIBERSEGURANÇA E PRIVACIDADE.



1.4.8 *Guias Orientativos da ANPD*

Considerando o papel fundamental da ANPD de orientação e normatização da proteção de dados pessoais, a Autoridade vem elaborando Guias Orientativos com o objetivo de delinear parâmetros que possam auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD. As orientações apresentadas no Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público[27] constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao Poder Público.

Para a construção deste Guia, foram utilizadas as seções “V. Compartilhamento de Dados Pessoais Pelo Poder Público” e “VI. Divulgação de Dados Pessoais”, do Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público da ANPD. É importante ressaltar que a inclusão destas seções não substitui a leitura desse e de outros Guias da ANPD.

1.5 Estruturação dos controles

Os controles que compõem este **Framework** estão organizados nas seguintes categorias:

[27] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf

- Estruturação básica de gestão em privacidade e segurança da informação:
  - Controle 0;
- Segurança cibernética:
  - Controles de 1 a 18;
- Privacidade:
  - Controles de 19 a 31.

2. CONTROLE DE ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

O controle de estruturação básica de gestão em privacidade e segurança da informação visa a atender às ações específicas de conformidade básica estabelecidas na IN SGD/ME nº 94, de 23 de dezembro de 2022, IN CGU nº 3, de 9 de junho de 2017, IN GSI/PR nº 1, de 27 de maio de 2020 e LGPD - Lei nº 13.709, de 14 de agosto de 2018.

A alta administração desempenha papel fundamental na estruturação proposta por este controle, especialmente, no que se refere a garantir que tal estruturação seja estabelecida no órgão ou entidade.

A lista das medidas deste controle consta do Anexo III. Tais medidas focam, em maior parte, nos papeis e estruturas fundamentais para a condução da implementação deste **Framework.**

No próximo capítulo serão abordados os controles de cibersegurança.

3. CONTROLES DE CIBERSEGURANÇA

Neste capítulo, serão apresentados os controles de cibersegurança fundamentados no CIS 8.

Cada seção subsequente apresenta um resumo do controle e o porquê implementá-lo, bem como a aplicabilidade e as implicações (consequências) da implementação do controle para a privacidade.

Mais detalhes sobre a aplicação dos controles de cibersegurança podem ser consultados no Guia *CIS Controls v8* e sobre aspectos de privacidade, especificamente no que se refere aos princípios de privacidade na implementação dos controles CIS, podem ser observados no Guia *CIS Controls Privacy Guide*.

As medidas, em formato de pergunta, a serem aplicadas para cada controle estão detalhadas no Anexo II deste **Guia**. As medidas foram organizadas de acordo com a sequência de funções do *NIST Cybersecurity Framework.* Além disso, foi realizado um mapeamento com os identificadores originais das medidas do *CIS Controls v8.*

3.1 Controle 1: Inventário e Controle de Ativos Institucionais

Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da empresa, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.

Por que implementar?

As instituições não podem defender aquilo que não está mapeado ou não se tem conhecimento de sua existência. Por esta razão, ter um inventário de ativos institucionais é essencial para que uma atitude de defesa possa acontecer. Neste intuito o Inventário e Controle de Ativos Institucionais desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As organizações devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos institucionais que mantêm ou gerenciam esses dados críticos, para que as medidas de segurança apropriadas possam ser aplicadas. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

Vale ressaltar que entram na lista de ativos:

- dispositivos de usuário final (computador institucional, dispositivos portáteis e móveis);
- dispositivos de rede;
- dispositivos não computacionais;
- dispositivos de *Internet of Things* (IoT);
- Servidores (conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem)

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 3 de 28 de maio de 2021, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR preveem ações a serem observadas e implementadas neste controle.

3.1.1 *Aplicabilidade e Implicações de Privacidade*

Princípios de privacidade devem ser incorporados ao processo de inventário de dispositivos, tanto do ponto de vista tecnológico quanto do processual.

O conhecimento sobre um dispositivo, onde está localizado, quem o está usando e como está usando pode fornecer informações pessoais. Muitas instituições utilizam o nome ou identificador de um indivíduo, que o vincula explicitamente ao dispositivo.

Assim, os inventários de ativos do órgão devem ser tratados com a possibilidade de conter dados pessoais. Em algum momento, é possível que o software de monitoramento e de rastreamento afete a privacidade dos funcionários e a segurança dos dados pessoais.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Ativos, com enfoque em prover diretrizes para gestão de ativos que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o gerenciamento de ativos da instituição.

Disponível em: Modelo de Política de Gestão de Ativos

3.2 Controle 2: Inventário e Controle de Ativos de Software

Gerenciar ativamente (inventariar, rastrear e corrigir) todo o software na rede para que apenas o software autorizado seja instalado e possa ser executado, e que todo o software não autorizado e não gerenciado seja encontrado e impedido de instalação ou

execução.

Por que implementar?

Um inventário de software completo é um recurso crítico para prevenir ataques. Os atacantes realizam varreduras na infraestrutura do órgão continuamente em busca de versões vulneráveis de software que possam ser exploradas. Contudo, sem um inventário completo dos ativos de software, um órgão não pode determinar se possui software vulnerável ou se há violações de licenciamento em potencial.

É fundamental inventariar, compreender, avaliar e gerenciar todos os softwares conectados à infraestrutura. Além de revisar seu inventário de software para identificar quaisquer ativos executando software que não sejam necessários para suas atividades.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020 e nº 3 de 28 de maio de 2021, preveem ações a serem observadas e implementadas neste controle.

3.2.1 *Aplicabilidade e Implicações de Privacidade*

Princípios de privacidade devem ser incorporados ao processo de inventário de software, tanto do ponto de vista tecnológico quanto processual.

Os inventários de software listam softwares autorizados instalados em dispositivos aprovados pela instituição. Esses ativos de software estão diretamente vinculados a indivíduos específicos podendo coletar e manipular seus dados pessoais.

Certos ativos de software podem conter informações sobre funcionários e em algum momento, é possível que o software de monitoramento e rastreamento afete negativamente a privacidade dos funcionários e a segurança dos dados pessoais.

Os tipos de dados comuns coletados para este controle incluem, entre outros, informações sobre o dispositivo, como modelo, proprietário, *Internet Protocol* (IP) e nome do dispositivo.

Essas informações podem ser armazenadas em uma planilha disponível para um administrador de sistema ou hospedadas em um banco de dados local armazenado na rede corporativa.

3.3 Controle 3: Proteção de Dados

Utilizar processos e ferramentas para identificar, classificar, manusear, reter e descartar dados.

Por que implementar?

No momento atual sabemos que os dados podem não estar apenas dentro da estrutura das instituições; podemos ter dados na nuvem, em dispositivos portáteis do usuário final, compartilhados com parceiros ou com serviços *on-line* em qualquer lugar do mundo.

As organizações possuem uma série de dados, que são importantes para o negócio, dentre eles os dados pessoais. O tratamento desses dados deve estar de acordo com as regulamentações de proteção de dados e privacidade pois a não conformidade pode afetar os direitos e garantias dos titulares de dados, além de acarretar prejuízos financeiros e reputacionais.

A proteção de dados está ganhando cada vez mais destaque no cenário global e as organizações estão aprendendo que o respeito ao uso e gestão apropriados de dados são fundamentais, não se restringindo apenas à criptografia. Os dados devem ser gerenciados de maneira adequada em todo o seu ciclo de vida.

A perda de controle da organização sobre os dados protegidos ou sensíveis é um sério e frequente impacto relatado no negócio. A adoção da criptografia dos dados, tanto em trânsito quanto em repouso, pode fornecer mitigação contra o comprometimento dos dados e, ainda mais importante, é um requisito regulatório para a maioria dos dados controlados.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 5 de fevereiro de 2013, nº 3 de 6 de março de 2013, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021, nº 6 de 23 de dezembro de 2021 e NCs nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B), nº 08 /IN01/DSIC/GSIPR, nº 09 /IN01/DSIC/GSIPR e nº 20 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.3.1 *Aplicabilidade e Implicações de Privacidade*

A implementação do controle de proteção de dados pode ajudar a proteger uma infinidade de informações em uma rede corporativa, incluindo Informações de

Identificação Pessoais. Sem as medidas listadas aqui, muitas das informações pessoais de clientes estariam em risco de exposição não autorizada.

Estabelecer e manter um Esquema de Classificação de Dados não precisa necessariamente ser realizado de forma automatizada por meio de software, mas os administradores de TI e os responsáveis pela privacidade devem ter um conhecimento geral dos tipos de dados coletados. Os funcionários de TI devem saber como identificar e relatar instâncias de dados pessoais recém-descobertos.

Quaisquer dados armazenados em sistemas em nuvem também devem ser protegidos, e os dados pessoais armazenados devem ser explicitamente entendidos e aprovados. O descarte de dados pessoais armazenados deve ser realizado de maneira segura em consulta com a equipe de segurança da informação da instituição ou com a política existente. Isso deve ser realizado para todos os papéis físicos, mídias digitais e plataformas de IoT e móveis.

3.4 Controle 4: Configuração Segura de Ativos Institucionais e Software

Estabelecer e manter a configuração segura de ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/*IoT*; e servidores) e software (sistemas operacionais e aplicações).

Por que implementar?

As configurações padrões para ativos e softwares são normalmente voltadas para a facilidade de implantação e uso, em vez da segurança. Controles básicos, serviços e portas abertas, contas ou senhas padrão e pré-instalação de software desnecessário podem ser explorados se deixados em seu estado padrão.

Referente às atualizações de configuração de segurança, elas precisam ser gerenciadas e mantidas ao longo do ciclo de vida dos ativos e software da instituição. Elas precisam ser rastreadas e aprovadas por meio de um processo de fluxo de trabalho de gestão de configuração para manter um registro que pode ser revisado para *compliance*, aproveitado para resposta a incidentes e para apoiar auditorias.

Além disso, as INs GSI/PR nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.4.1 *Aplicabilidade e Implicações de Privacidade*

As configurações seguras para ativos institucionais e software podem ajudar a viabilizar a privacidade dos funcionários, evitando violações de dados e invasões de contas. Algumas configurações podem ser vistas como vulnerabilidades absolutas, enquanto outras configurações podem enfraquecer um sistema ou software e torná-lo mais suscetível a um ataque bem-sucedido. Com isso, a maioria das medidas dentro deste controle pode ter um impacto na privacidade quando implementada em uma instituição.

Determinadas configurações de hardware e software podem afetar negativamente a privacidade dos funcionários. Portanto, é necessária uma revisão de privacidade nas definições de configuração para garantir que determinados produtos não armazenem ou transmitam, intencionalmente ou não, dados pessoais de funcionários.

A configuração de determinados ativos e softwares pode fazer com que dados, incluindo dados pessoais, sejam coletados, e estes podem conter informações confidenciais. Os administradores devem entender as configurações e habilitar funções para que essas informações não fiquem desprotegidas.

3.5 Controle 5: Gestão de Contas

Usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, contas de administrador, contas de serviço para ativos e softwares institucionais.

Por que implementar?

É mais fácil para um agente de ameaça (externo ou interno) obter acesso não autorizado a ativos ou dados da organização usando credenciais de usuário válidas do que “hackeando” o ambiente. Existem várias formas de obter acesso a contas de usuário; como por exemplo:

- senhas fracas;
- contas ainda válidas depois que um colaborador deixa de trabalhar na organização;
- contas de teste;
- contas compartilhadas;
- contas de serviço incorporadas em aplicações para scripts;

- um usuário com a mesma senha que ele usa para uma conta *on-line* que foi comprometida (em um *dump* de senha pública);
- engenharia social em um usuário para fornecer sua senha;
- malware para capturar senhas ou tokens na memória ou na rede.

Contas administrativas ou com privilégio alto são alvos preferenciais porque permitem que atacantes adicionem novas contas ou façam alterações em ativos que podem torná-los mais vulneráveis a ataques. As contas de serviço também são críticas, pois geralmente são compartilhadas entre as equipes, internas e externas à organização e as vezes desconhecidas, apenas para serem reveladas em auditorias de gestão de contas padrão.

Além disso, as INs GSI/PR nº 2 de 5 de fevereiro de 2013 e NCs nº 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B), preveem ações a serem observadas e implementadas neste controle.

3.5.1 *Aplicabilidade e Implicações de privacidade*

O gerenciamento de contas é aplicável a todos os aplicativos, dispositivos e serviços. Todos os usuários precisarão de uma conta para acessar aplicativos, dispositivos e provedores de serviços internos ou externos.

Em razão disso, medidas devem ser gerenciadas durante o controle de acesso para evitar que, dados pessoais possam vazar por meio da criação, uso e divulgação de credenciais. O armazenamento seguro de informações de contas e outros dados relativos à autenticação também devem ser verificados durante a gestão de contas. Os sistemas que armazenam informações de contas precisam permanecer atualizados em relação aos patches de segurança, garantindo a aplicação dos métodos seguros de armazenamento, de acordo com as práticas de segurança utilizadas para proteger as informações antes de usar qualquer serviço.

3.6 Controle 6: Gestão do Controle de Acesso

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

Por que implementar?

Deve ser assegurado que os usuários tenham acesso apenas aos dados ou ativos

institucionais apropriados para suas funções e garantir que haja autenticação forte para dados ou funções corporativas críticas ou sensíveis. As contas devem ter apenas a autorização mínima necessária para a função. O desenvolvimento de direitos de acesso consistentes para cada função e a atribuição de funções aos usuários é uma prática recomendada.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 5 de fevereiro de 2013, nº 5 de 31 de agosto de 2021 e NCs nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B) e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.6.1 *Aplicabilidade e Implicações de Privacidade*

O Controle de Gerenciamento de Acesso destina-se a gerenciar grande parte do processo de autenticação e autorização, desde como um usuário acessa um dispositivo até a revogação de credenciais e privilégios de acesso.

As informações de identificação pessoal são frequentemente armazenadas em sistemas de autenticação e autorização. Esses sistemas precisam ser configurados de maneira que preserve a privacidade. Geralmente, o gerenciamento de acesso automatizado é preferido, pois ajuda a evitar exposições acidentais de informações privadas e confidenciais por pessoas. A revogação de direitos deve ser preferencialmente realizada também de forma automatizada.

A falha em controlar o acesso, mesmo de administradores, pode ser um requisito de conformidade ou pode levar a acesso e divulgação não autorizados.

Registros (*Logs*) relativos à sistemas de autenticação e autorização em geral podem registrar ações privadas e consequentemente podem ser usados para comprometer a privacidade. Devido a esse e outros fatores, é uma prática recomendada auditar e verificar regularmente quem tem acesso aos dados de autenticação e autorização e manter esses dados apenas pelo tempo necessário.

Os sistemas de informação que ajudam os administradores a gerenciar direitos e privilégios dentro da organização podem coletar dados pessoais ao cadastrar usuários. Administradores e provedores de serviços terceirizados (operadores, conforme art. 5º, inciso VII da LGPD) geralmente terão acesso a esses dados. Isso também vale para os sistemas de autenticação usados para usuários remotos.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Controle de Acessos com enfoque em prover diretrizes para controle de acesso que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o gerenciamento dos acessos da instituição.

Disponível em: Modelo de Política de Controle de Acesso

3.7 Controle 7: Gestão Contínua de Vulnerabilidades

Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

Por que implementar?

Compreender e gerenciar vulnerabilidades em uma rede corporativa é uma atividade contínua, que requer tempo, foco e recursos. Por isso, os profissionais de segurança devem ter informações oportunas de ameaças disponíveis, tais como:

- Atualizações de software;
- Patches;
- Avisos de segurança;
- Boletins de ameaças.

Além de revisar regularmente seu ambiente para identificar essas vulnerabilidades antes que os atacantes o façam e as explorem para obter acesso ao ambiente.

Além disso, a IN GSI/PR nº 4, de 26 de março de 2020 prevê ações a serem observadas e implementadas neste controle.

3.7.1 *Aplicabilidade e Implicações de Privacidade*

Este controle é voltado ao monitoramento de possíveis vulnerabilidades em softwares ou hardwares usados pela instituição. Abrange processos para tomada de decisões com ações proativas e correções naquilo que possa comprometer a privacidade, incluindo ações defensivas.

A combinação do inventário de ativos com as ferramentas e o ecossistema de software usado para varredura de vulnerabilidades podem compartilhar dados pessoais com outras instituições.

Portanto a recomendação do uso de softwares de gerenciamento de vulnerabilidades deve ser usada de modo a coletar somente o necessário uma vez que essas ferramentas podem coletar informações pessoais sem o consentimento do titular.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Gerenciamento de Vulnerabilidades com enfoque no gerenciamento de vulnerabilidades que constitui uma referência importante para instituições e profissionais de segurança da informação, que desejam realizar a construção de processos para o gerenciamento das vulnerabilidades.

Disponível em: Guia de Gerenciamento de Vulnerabilidades

3.8 Controle 8: Gestão de Registros de Auditoria

Coletar, alertar, analisar e reter logs de eventos com o objetivo de ajudar a detectar, compreender ou se recuperar de um ataque.

Por que implementar?

A coleta e análise de log são procedimentos críticos para que uma organização possa detectar atividades maliciosas rapidamente. Em certas ocasiões, os registros de auditoria são a única evidência de um ataque bem-sucedido.

A gestão de registros de auditoria deve ser mantida em constante monitoramento e uso, porque os atacantes sabem que muitas organizações mantêm logs de auditoria para fins de conformidade, entretanto raramente os analisam. Baseado nesse conhecimento, eles conseguem ocultar sua localização, um software malicioso ou atividades nas máquinas das vítimas. Caso os processos de análise de log sejam

insatisfatórios ou inexistentes, os atacantes às vezes, podem controlar as máquinas das vítimas por meses ou anos sem que sejam percebidos pela organização-alvo.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 21 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Registros (Logs) de Auditoria com o objetivo de prover diretrizes para a gestão de registros de auditoria, uma referência importante para instituições e profissionais de segurança da informação, que desejam realizar a gestão dos registros (logs).

Disponível em: Modelo de Política de Gestão de Registros (Logs) de Auditoria

3.8.1 *Aplicabilidade e Implementações de Privacidade*

Os logs são muito úteis, tanto para desenvolvedores quanto para equipe de TI, na melhoria e na solução de problemas, porém podem armazenar informações pessoais, trazendo implicações para privacidade.

Eles podem conter todo tipo de informação pessoal (nomes, e-mails etc). Para evitar isso, deve ser definido um processo de gerenciamento de log de auditoria que leve em consideração a privacidade e, além disso, deve ser acordado previamente como estes logs serão tratados por terceiros (operadores, conforme art. 5º, inciso VII da LGPD).

Medidas de segurança devem ser aplicadas como por exemplo criptografia e controle de acesso a fim de evitar violações. A proteção no armazenamento também deve ser considerada com ações defensivas incluindo ambientes terceirizados devidamente e explicitamente acordados.

3.9 Controle 9: Proteções de E-mail e Navegador Web

Melhorar as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto.

Por que implementar?

Navegadores Web e clientes de e-mail são pontos de entrada muito comuns para atacantes em virtude de sua interação direta com usuários dentro das instituições.

Conteúdos podem ser criados para atrair ou enganar os usuários para que revelem suas credenciais, forneçam dados sensíveis ou forneçam um canal aberto onde os atacantes obtenham acesso, aumentando assim o risco para a corporação.

Além disso, a IN GSI nº 1, de 27 de maio de 2020 prevê ações a serem observadas e implementadas neste controle.

3.9.1 *Aplicabilidade e Implicações de Privacidade*

As medidas deste controle podem ajudar a proteger os dados pessoais, e devem ser cuidadosamente consideradas para que:

- Extensões de navegador não cometam ações maliciosas ou até mesmo a coleta de informações pessoais desnecessárias.
- Filtros de *Uniform Resource Locator* - URL ajudam a impedir acessos a recursos de rede e outros tipos acessos indevidos, além de rastrear os recursos acessados ou de tentativas realizadas pelos usuários.
- Os servidores de e-mail não retenham informações por muito tempo, pois podem agravar o risco de violação de dados.
- Os Servidores de DNS - *Domain Name System* (Sistema de Nomes de Domínio) que manipulam dados de natureza sensível, sejam dados em trânsito ou dados armazenados, devem ser adequadamente protegidos.

3.10 Controle 10: Defesas Contra Malware

Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos da organização.

Por que implementar?

Os softwares maliciosos estão em constante evolução e adaptação. Os ataques ocorrem por meio de vulnerabilidades em dispositivos de usuário final e geralmente depende do comportamento inseguro do usuário, como clicar em links, abrir anexos, instalar software ou perfis, ou inserir unidade flash USB (*Universal Serial Bus*).

As defesas contra malware devem ser capazes de operar neste ambiente dinâmico por meio de automação, atualização rápida e oportuna e integração com outros processos, como gestão de vulnerabilidade e resposta a incidentes. Eles devem ser implantados em todos os possíveis pontos de entrada e ativos institucionais para detectar, impedir a propagação ou controlar a execução de software ou código malicioso.

Além disso, a IN GSI/PR nº 5, de 31 de agosto de 2021 e a NC nº 08 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.10.1 *Aplicabilidade e Implicações de Privacidade*

A implementação das medidas de segurança contra malware contidas neste controle podem evitar que um malware instalado em um sistema possa coletar informação de identificação pessoal.

Os logs e alertas do software *antimalware* defensivo devem ser armazenados em um local seguro e o acesso deve ser restrito para evitar roubo ou vazamento de dados pessoais que tenham sido coletados.

3.11 Controle 11: Recuperação de Dados

Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível.

Por que implementar?

Os órgãos precisam de muitos tipos de dados para tomar decisões de negócios e, quando esses dados não estão disponíveis ou não são confiáveis, eles podem impactar o órgão.

Quando os atacantes comprometem os ativos, fazem alterações nas configurações, adicionam contas e, frequentemente, adicionam softwares ou scripts, essas alterações nem sempre são fáceis de identificar, podendo incluir, adicionar ou alterar entradas de registro, abrir portas, desligar serviços de segurança, excluir logs ou outras ações maliciosas que tornam o sistema inseguro. Nem toda ação precisa ser maliciosa; erros humanos também podem causar os mesmos danos. Portanto, é importante ter a capacidade de ter backups ou espelhos recentes para recuperar ativos

e dados institucionais de volta a um estado confiável conhecido.

Vale ressaltar também o aumento exponencial de *ransomware*, caso em que o atacante realiza a criptografia dos dados de um órgão em uma forma de “sequestro” e em seguida exige um resgaste para restauração ou para não divulgação e venda dos dados. Nesta situação, um backup recente não comprometido seria útil para recuperar o sistema a um estado confiável, porém o risco de venda ou divulgação dos dados criptografados continuaria.

Além disso, as IN GSI/PR nº 3 de 28 de maio de 2021, nº 3 de 6 de março de 2013 e a NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.11.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle destina-se a auxiliar a instituição na preparação para a recuperação de um incidente cibernético. Existem preocupações de privacidade com muitas medidas de segurança dentro deste controle.

A equipe de TI precisará criar backups das informações corporativas como parte desse controle. Informações de identificação pessoal contidas em registros precisarão ter backup.

Testar se os backups podem realmente ser restaurados é uma parte importante do processo de recuperação de dados.

A restauração de backups durante o teste deve ser feita com cuidado. Se os dados confidenciais forem restaurados, esse sistema deve ser devidamente protegido e excluído com segurança após a conclusão do exercício.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Backup com enfoque em prover diretrizes para as políticas de backup e restauração de dados digitais que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar a construção das políticas de backup e restauração de dados digitais da instituição.

Disponível em: Modelo de Política de Backup

3.12 Controle 12: Gestão da Infraestrutura de Rede

Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Por que implementar?

A infraestrutura de rede segura é uma defesa essencial contra os ataques. Isso inclui uma arquitetura de segurança apropriada, abordando vulnerabilidades que são, muitas vezes, introduzidas com configurações padrão, monitoramento de alterações e reavaliação das configurações atuais.

Neste caso, a segurança da rede deve estar em constante mudança, o que exige uma reavaliação regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego permitidos, de forma a evitar que os atacantes tirem proveito das configurações de dispositivos de rede que se tornam menos seguras com o tempo.

Além disso, a IN GSI/PR nº 4, de 26 de março de 2020 prevê ações a serem observadas e implementadas neste controle.

3.12.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle visa a garantir que a infraestrutura de rede seja mantida e configurada adequadamente durante todo o seu ciclo de vida.

O design e a segmentação de rede inadequados podem levar a menores graus de privacidade para usuários da rede corporativa. A falha em documentar as decisões destinadas a melhorar a privacidade pode prejudicar os desenvolvimentos futuros em um programa de privacidade em expansão.

Logs relacionados a sistemas de autenticação e autorização em geral podem registrar dados privados. A coleta dessas entradas de log pode ser benéfica para os esforços de investigação durante a resposta a incidentes; no entanto, eles também podem ser usados para comprometer a privacidade. Devido a esse e outros fatores, é uma prática recomendada auditar e verificar regularmente quem tem acesso aos dados pessoais registrados em logs relacionados a sistemas de autenticação e autorização.

3.13 Controle 13: Monitoramento e Defesa da Rede

Implementar processos e ferramentas para que a organização estabeleça o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua

infraestrutura de rede e base de usuários.

Por que implementar?

Não podemos confiar que as defesas da rede sejam perfeitas. Os adversários continuam a evoluir e amadurecer à medida que compartilham ou vendem informações.

As ferramentas de segurança somente são eficazes se oferecerem suporte a um processo de monitoramento contínuo que permita à equipe ser alertada e responder rapidamente a incidentes de segurança.

Ter uma consciência situacional abrangente aumenta a velocidade de detecção e resposta, que é fundamental para minimizar um possível impacto negativo para o órgão, por exemplo, ao responder rapidamente quando um *malware* é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos.

Além disso, as IN GSI/PR nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.13.1 *Aplicabilidade e Implicações de Privacidade*

A visibilidade da rede permite entender os tipos e a frequência dos ataques enfrentados pela instituição. Para tal, as medidas de segurança e o monitoramento de rede desse controle se concentram na instalação, configuração e monitoramento de software que auxiliam nessas atividades. Essas soluções poderão ter acessos privilegiados às informações na rede que podem ter implicações de privacidade de dados pessoais.

As empresas devem garantir que as ferramentas SIEM – *Security Information and Event Management (Gerenciamento e Correlação de Eventos de Segurança)* - não estejam alertando regularmente sobre informações que contenham dados pessoais e, portanto, sejam enviados aos analistas de segurança para revisão manual. Tal configuração será diferente das soluções SIEM que alertam a TI sobre a existência de informações pessoais e senhas em texto simples.

As informações de tráfego de rede coletadas pelo IDS - *Intrusion Detection System* (Sistema de Detecção de Intrusão), IPS - *Intrusion Prevention System* (Sistema de Prevenção de Intrusão) e *softwares* de filtragem de aplicativos, juntamente com alertas gerados a partir de uma variedade de fontes, devem ser armazenadas e protegidas

adequadamente para evitar um vazamento de dados que possam conter dados pessoais.

3.14 Controle 14: Conscientização e Treinamento de Competências sobre Segurança

Implantar e manter um programa de conscientização de segurança que possa influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética da organização.

Por que implementar?

As ações das pessoas podem causar incidentes, intencionalmente ou não. É mais fácil para um atacante induzir um usuário a clicar em um link ou abrir um anexo de e-mail para instalar malware e entrar na rede de uma organização, do que fazer um *exploit* de rede diretamente. Nenhum programa de segurança pode lidar com o risco cibernético de maneira eficaz sem um meio de lidar com essa vulnerabilidade humana fundamental. Cada usuário do órgão em qualquer nível tem riscos diferentes.

Os treinamentos e conscientizações devem ser atualizados regularmente. Isso aumentará a cultura de segurança.

Além disso, a IN GSI/PR nº 6, de 23 de dezembro de 2021 e NCs nº 08 /IN01/DSIC/GSIPR, nº 17 /IN01/DSIC/GSIPR e nº 18 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.14.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle destina-se a garantir que os colaboradores recebam treinamento de segurança direcionado para suas funções e responsabilidades específicas, mas devido ao escopo deste **Guia de Framework de Privacidade e Segurança da Informação** este controle deve levar em consideração o treinamento através da lente de conscientização de privacidade.

Administradores de TI com acessos privilegiados podem tomar decisões ruins se não forem treinados sobre o uso apropriado de seus acessos e as consequências de violações de dados sigilosos e de dados pessoais.

Os usuários e provedores de serviços devem entender os requisitos de privacidade e proteção de dados pessoais exigidos pela organização e como proteger esses dados. Cabe ao controlador comunicar os requisitos de privacidade e garantir que eles sejam

atendidos.

3.15 Controle 15: Gestão de Provedor de Serviços

Com o objetivo de garantir a proteção das informações, sistemas e processos críticos da organização, estabeleça um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.

Por que implementar?

Normalmente as organizações contam com fornecedores e parceiros para ajudar a gerenciar seus dados ou contam com infraestrutura de terceiros para aplicações ou funções essenciais.

Violações de terceiros costumam impactar significativamente uma organização, como por exemplo os ataques de *ransomware* que podem ser realizados indiretamente, quando há um bloqueio de um de seus provedores de serviço, causando a interrupção nos negócios, ou diretamente, criptografando os dados da organização.

A maioria das regulamentações de segurança, privacidade e proteção de dados exigem que sua proteção seja estendida a prestadores de serviços terceirizados. A confiança de terceiros é uma função central de Governança, Riscos e *Compliance* (GRC), pois os riscos que não são gerenciados dentro da organização são transferidos para entidades fora da organização.

Além disso, as IN GSI/PR nº 3 de 6 de março de 2013, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.15.1 *Aplicabilidade e Implicações de Privacidade*

Algumas instituições utilizam os provedores de serviços em nuvem para e-mail ou armazenamento. Este controle abrange as ações que devem ser tomadas para garantir que os provedores de serviços terceirizados estejam protegendo adequadamente os dados de seus clientes e seus próprios sistemas. As medidas recomendadas para este controle incluem entender quais provedores de serviços estão em uso, quais tipos de dados eles armazenam e monitorar seu desempenho. Considere escolher fornecedores que tenham certificações de privacidade ou alguma outra auditoria independente de suas próprias práticas de privacidade.

Os provedores de serviços (operadores, conforme art. 5º, inciso VII da LGPD)

podem utilizar, vender ou compartilhar dados pessoais obtidos por meio de seus clientes.

Os dados pessoais podem ser fornecidos diretamente como parte de uma função comercial ou criados por meio do uso de um produto ou serviço, como firewalls ou outros dispositivos de rede.

Provedores de serviços ao coletar e utilizar os dados pessoais, devem declará-los claramente nos acordos de nível de serviço – SLAs *(Service Level Agreement)*. Controles de segurança relacionados aos dados pessoais também devem ser explicitamente escritos e acordados antes do uso.

3.16 Controle 16: Segurança de Aplicações

Gerenciar o ciclo de vida de segurança de todos os softwares desenvolvidos e adquiridos internamente, a fim de prevenir, detectar e corrigir falhas de segurança.

Por que implementar?

As organizações usam aplicações para gerenciar seus dados mais sensíveis e controlar o acesso aos recursos do sistema. Na ausência de credenciais, um atacante pode usar a própria aplicação para comprometer os dados, em vez de uma sequência elaborada de invasão de rede e sistema que tenta desviar dos controles e sensores de segurança da rede.

As aplicações de hoje são desenvolvidas, operadas e mantidas em um ambiente altamente complexo, diverso e dinâmico, sendo executadas em várias plataformas: web, móvel, nuvem etc., com arquiteturas de aplicações que são mais complexas do que as estruturas legadas de cliente/servidor ou servidor de banco de dados web.

As vulnerabilidades de aplicação podem estar presentes por vários motivos: design inseguro, infraestrutura insegura, erros de codificação, autenticação fraca e falha no teste para condições incomuns ou inesperadas. Os atacantes podem explorar vulnerabilidades específicas, incluindo buffer overflows, exposição à *Structured Query Language* (SQL) *injection*, *cross-site scripting*, falsificação de solicitações entre sites e *click-jacking* de código para obter acesso a dados sensíveis ou assumir o controle de ativos vulneráveis dentro da infraestrutura como um ponto de partida para novos ataques. Aplicações e sites também podem ser usados para coletar credenciais, dados ou tentar instalar malware nos dispositivos de usuários que os acessam.

Atualmente é mais comum adquirir plataformas de *Saas - Software as a Service*

(Software como um Serviço), nas quais o *software* é desenvolvido e gerenciado inteiramente por terceiros. Isso traz desafios para as organizações que precisam saber quais riscos estão aceitando na utilização do serviço.

Além disso, as IN GSI/PR nº 3 de 6 de março de 2013, nº 5 de 31 de agosto de 2021 e NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.16.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle se concentra principalmente nos esforços que desenvolvedores de software podem realizar para evitar vulnerabilidades exploráveis em seu código, que podem levar à exposição não autorizada de dados pessoais. A maioria das medidas contidas neste controle não está diretamente relacionada à proteção de dados pessoais. Bibliotecas de software de terceiros e APIs - *Application Programming Interface* (Interfaces de Programação de Aplicativos) podem coletar informações por meio de seu uso. Os dados que esses componentes de terceiros podem coletar devem ser claramente declarados nos *SLAs*. Os controles de segurança relacionados aos dados pessoais também devem ser explicitamente escritos e acordados com fornecedores de componentes de terceiros antes do uso.

Todos os desenvolvedores devem ser treinados sobre os requisitos de privacidade relativos ao tratamento de dados pessoais e como incluir privacidade no design, uma vez que bibliotecas de software de terceiros, componentes, APIs e *logs* dos sistemas podem coletar e armazenar dados pessoais. Os dados que estes componentes de terceiros podem coletar devem ser claramente indicados nos *SLAs*.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal três Guias voltados ao desenvolvimento seguro que apresentam instruções claras sobre tema.

Disponíveis em:

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para

Aplicativos Móveis

3.17 Controle 17: Gestão de Resposta a Incidentes

Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão) para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.

Por que implementar?

Um programa abrangente de segurança cibernética inclui proteções, detecções, resposta e recursos de recuperação. O objetivo principal da resposta a incidentes é identificar ameaças na organização, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos. É necessário entender todo o escopo de um incidente, como aconteceu e o que pode ser feito para evitar que aconteça novamente, com o objetivo de solucionar o incidente de forma eficiente.

Quando ocorre um incidente, se uma organização não tem um plano documentado - mesmo com boas pessoas - é quase impossível saber os procedimentos de investigação corretos, relatórios, coleta de dados, responsabilidade de gestão, protocolos legais e estratégia de comunicação que permitirão a organização entender, gerenciar e recuperar com sucesso.

Junto com a detecção, contenção e erradicação, a comunicação com as partes interessadas é fundamental. Se quisermos reduzir a probabilidade de impacto material devido a um evento cibernético, a liderança da organização deve saber qual o impacto potencial que pode haver, para que possam ajudar a priorizar as decisões de remediação ou restauração que melhor apoiem a organização. Essas decisões de negócios podem ser baseadas em conformidade regulatória, regras de divulgação, acordos de nível de serviço com parceiros ou clientes, receita ou impactos de missão.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 24 de julho de 2020, nº 3 de 28 de maio de 2021, nº 4 de 26 de março de 2020 e NCs nº 05 /IN01/DSIC/GSIPR, e seu anexo e nº 08 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.17.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle auxilia as instituições no planejamento e na resposta a um incidente cibernético. Existem dois aspectos de privacidade do controle. O primeiro é como responder a um incidente de privacidade. O segundo é como manter a privacidade de todos os indivíduos ao responder a um incidente cibernético.

As equipes de resposta a incidentes ao longo de suas funções, podem ter acesso a dados pessoais, então eles podem manipular de forma inadequada essas informações.

Os membros da equipe de resposta a incidentes coletarão informações de vários sistemas em toda a rede corporativa enquanto realizam suas funções para entender a maneira e o escopo de uma intrusão.

Todos os dados coletados durante as atividades de resposta a incidentes precisam ser protegidos, pois geralmente são dados pessoais, mas também podem ser necessários para procedimentos legais futuros.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Resposta a Incidentes de Segurança, com enfoque em incidentes que envolvam dados pessoais, que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o tratamento de incidentes cibernéticos.

Disponível em: Guia de Resposta a Incidentes de Segurança

3.18 Controle 18: Testes de Invasão

Testar a eficácia e a resiliência dos ativos institucionais por meio da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

Por que implementar?

Uma postura defensiva bem-sucedida requer um programa abrangente de políticas e governança eficazes, fortes defesas técnicas, combinadas com a ação apropriada das pessoas. Em um ambiente complexo onde a tecnologia está em constante evolução e novas técnicas dos atacantes aparecem regularmente, as organizações devem testar periodicamente seus controles para identificar lacunas e

avaliar sua resiliência. Este teste pode ser da perspectiva de rede externa, rede interna, aplicação, sistema ou dispositivo. Pode incluir engenharia social de usuários ou desvios de controle de acesso físico.

Testes de invasão independentes podem fornecer percepções valiosas e objetivas sobre a existência de vulnerabilidades em ativos institucionais e humanos, e a eficácia das defesas e controles de mitigação para proteger contra impactos adversos para a organização. Eles fazem parte de um programa abrangente e contínuo de gestão e aprimoramento de segurança. Eles também podem revelar fraquezas do processo, como gestão de configuração ou treinamento do usuário final incompletos ou inconsistentes.

3.18.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle tem como objetivo simular efetivamente as ações de um invasor externo e/ou interno em um ambiente corporativo. Isso pode incluir a exploração de uma fraqueza ou vulnerabilidade em um sistema ou rede. Muitas das medidas dentro do controle contêm impactos de privacidade de dados pessoais que podem ser mitigados por meio de políticas e acordos claramente escritos antes que qualquer teste seja realizado.

Como parte do processo de teste, informações pessoais podem ser obtidas pelos testadores de invasão.

Quaisquer dados coletados por testadores de invasão ao longo de seu envolvimento devem ser bem protegidos. Ambas as organizações devem concordar com as técnicas de descarte de dados.

Os dados obtidos por testadores de invasão não devem ser compartilhados. Caso ocorra o compartilhamento, os testadores de invasão devem notificar rapidamente a organização.

4. CONTROLES DE PRIVACIDADE

Neste capítulo serão apresentados os controles de privacidade, ressaltando a importância de sua implementação.

As medidas, em formato de pergunta, a serem aplicadas para cada controle estão detalhadas no Anexo V deste **Guia**.

4.1 Controle 19: Inventário e Mapeamento

As operações de tratamento de dados pessoais por sistemas, produtos, processos ou serviços devem ser identificadas e inventariadas.

Por que implementar?

De acordo com o art. 37 da LGPD o controlador e o operador devem manter registradas as operações de tratamento de dados pessoais que realizam, especialmente quando baseadas no legítimo interesse.

O Registro de Operações de tratamento de dados pessoais representa uma operação importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

Um modo de manter os registros de tratamento de dados pessoais é manter um inventário ou uma lista das atividades de tratamento que a organização realiza.

A atividade contempla os processos de negócio que realizam tratamento de dados pessoais, bem como o Inventário de Dados Pessoais (IDP) que aborda, por exemplo:

- agentes de tratamento (Controlador e Operador);
- encarregado;
- finalidade e hipótese do tratamento;
- compartilhamento dados pessoais;
- transferência internacional;
- propósitos para o tratamento;
- uma descrição das categorias dos dados pessoais e dos titulares de dados pessoais tratados pela instituição (por exemplo, crianças);
- o tempo de retenção dos dados pessoais;
- uma descrição geral das medidas de segurança técnica e organizacional.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Inventário de Dados Pessoais, que incentiva a adoção de registros das operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD e contém importantes instruções para que as instituições e seus colaboradores possam elaborar um inventário de dados pessoais.

Disponível em: Guia de Elaboração de Inventário de Dados Pessoais

4.2 Controle 20: Finalidade e Hipóteses Legais

A organização deve identificar, especificar e documentar as finalidades, hipóteses de tratamento e bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis.

Por que implementar?

A partir da promulgação da LGPD não é mais possível tratar dados pessoais com finalidades genéricas. Determinar a finalidade específica do tratamento de dados, junto com a hipótese de tratamento e as bases legais que fundamentam o tratamento, significa realizá-lo para propósitos legítimos, específicos, explícitos e informados ao titular, ou seja, os órgãos devem justificar para qual finalidade usarão cada um dos dados pessoais coletados.

O princípio da finalidade previsto no art. 6°, inciso I da LGPD estabelece que o tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja **legítima, específica, explícita e informada.** Da mesma forma, o princípio da adequação presente no art. 6°, inciso II da LGPD estabelece que o tratamento esteja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Especificar as finalidades para as quais os dados pessoais são tratados permite garantir que o processamento dos dados pessoais esteja em conformidade com a LGPD e esteja fundamentado em uma base legal permitida.

Para que o tratamento de dados pessoais possa acontecer, é necessário estar amparado em uma das hipóteses legais previstas no art. 7° e 11 da LGPD. Tais hipóteses são as diretrizes gerais que autorizam a atividade de tratamento de dados

por qualquer controlador.

Além disso, para que o órgão possa tratar os dados pessoais, a LGPD, em seu art. 7°, inciso III e art. 11, inciso II, alínea b, determina que ao executar uma política pública, esta deve estar prevista em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Importante ressaltar que a especificação da finalidade e a identificação da hipótese de tratamento e a base legal que respalda a política pública deve acontecer antes que o tratamento de dados pessoais seja realizado.

Por fim, o princípio da finalidade estabelece uma limitação ao tratamento posterior dos dados pessoais. Assim, eventual uso secundário dos dados pessoais somente pode ser realizado para uma finalidade que seja compatível com a finalidade original do tratamento desses dados.

4.3 Controle 21: Governança

A governança em privacidade estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos de impacto à privacidade e melhorias contínuas na maturidade.

Por que implementar?

A LGPD estabelece no Art. 50 que os controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que definam as condições de organização, bem como, o regime de funcionamento, procedimentos e outras ações referentes à governança em privacidade e proteção de dados pessoais.

As organizações devem implementar medidas apropriadas para estabelecer uma governança eficiente relacionada ao processamento de dados pessoais.

Para aumentar a confiança de todas as partes interessadas é necessário que os gestores do gerenciamento de segurança, proteção de dados pessoais e risco ampliem tanto a frequência quanto a amplitude da comunicação, para assim assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

Uma das ações importantes a ser observada no âmbito da governança é a implementação de um programa de governança em privacidade que demonstre o

comprometimento das partes envolvidas em adotar processos e políticas internas que assegurem o cumprimento, de normas e boas práticas relativas à proteção de dados pessoais.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Boas Práticas da LGPD e um Guia de Elaboração de um Programa de Governança em Privacidade que apresenta os principais pontos da LGPD, fornecendo os subsídios para a criação de um programa institucional de gerenciamento de privacidade.

Disponível em:

Guia de Boas Práticas da LGPD

Guia de Elaboração de um Programa de Governança em Privacidade

4.4 Controle 22: Políticas, Processos e Procedimentos

Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.

Por que implementar?

O art. 50 da LGPD prevê que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

O órgão deve desenvolver e implementar políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização que sejam compreendidos para informar a administração sobre o gerenciamento dos riscos que impactam na privacidade e proteção de dados

pessoais.

4.5 Controle 23: Conscientização e Treinamento

As pessoas envolvidas no tratamento de dados são instruídas e conscientizadas sobre privacidade, sendo treinadas para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade da organização.

Por que implementar?

Tendo como base o disposto previsto no art. 50 da LGPD, os controladores e operadores, no âmbito de suas competências, devem aplicar medidas educativas periódicas apropriadas para as pessoas que têm acesso aos dados pessoais. O programa de treinamento deve:

a) implementar e manter uma estratégia abrangente de treinamento e conscientização destinada a garantir que o pessoal entenda suas responsabilidades e procedimentos de proteção de dados pessoais;
b) criar mecanismos para manter o pessoal com responsabilidades de proteção de dados pessoais atualizado sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade pela organização;
c) administrar treinamento básico e direcionado de proteção dados pessoais com base em funções, regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente);
d) garantir que o pessoal certifique (manualmente ou eletronicamente) a aceitação das responsabilidades pelos requisitos de proteção de dados pessoais periodicamente.
e) incluir a conscientização sobre notificação de incidentes para assegurar que membros relevantes estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano reputacional ou da marca).

4.6 Controle 24: Minimização de Dados

O órgão, dentro dos limites de suas competências legais, deve implementar ações para não coletar e tratar de forma inadequada ou excessiva os dados pessoais dos

titulares de dados pessoais e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada.

Por que implementar?

Conforme estabelecido no art. 18 da LGPD, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados pessoais por ele tratados, a qualquer momento e mediante requisição, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei.

O Controlador, portanto, deve limitar a quantidade de dados pessoais tratados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, em aderência ao princípio da necessidade preconizado pelo art. 6º, inciso III da LGPD.

As organizações não devem coletar dados pessoais indiscriminadamente. Tanto a quantidade quanto o tipo de dados pessoais coletados devem ser limitados ao necessário para cumprir a(s) finalidade(s) legítima(s) especificada(s) pelo controlador.

Em qualquer tratamento de dados pessoais que seja realizado pela organização, deve-se considerar cuidadosamente quais dados pessoais serão necessários para atender à finalidade específica antes de prosseguir com o tratamento.

4.7 Controle 25: Gestão do Tratamento

A gestão do tratamento visa a limitar o uso, a retenção e a divulgação de dados pessoais ao que for estritamente necessário para cumprir propósitos específicos, explícitos e legítimos.

Por que implementar?

O princípio da necessidade, previsto no art. 6º da LGPD, estabelece que o tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

As organizações devem implementar medidas apropriadas para limitar o tratamento de dados pessoais para fins legítimos e pretendidos e reter os dados pessoais apenas pelo tempo necessário para cumprir os propósitos declarados ou para

cumprir as leis aplicáveis.

Vale ressaltar que os dados pessoais devem ser gerenciados em conformidade com a estratégia de risco da organização para proteger a privacidade dos indivíduos, aumentar a gerenciabilidade e permitir a implementação de princípios de privacidade.

4.8 Controle 26: Acesso e Qualidade

O acesso e qualidade visam a garantir que os direitos do titular, quanto ao tratamento de dados pessoais, sejam atendidos e assegurar que sejam feitos de forma exata, clara, relevante e atualizado de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Assegurar também o livre acesso aos titulares para consulta facilitada e gratuita sobre a integralidade de seus dados pessoais.

Por que implementar?

Conforme os princípios do livre acesso e qualidade dos dados estabelecido no art. 6º da LGPD e os direitos do titular de dados pessoais, previsto no art. 18, o controlador deve garantir aos titulares o acesso facilitado e gratuito a seus dados pessoais, bem como sobre a integralidade de seus dados pessoais com direito a correção de dados incompletos, inexatos ou desatualizados. E ainda, garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

A viabilização do livre acesso do titular dos dados pessoais e a adoção de práticas que visem a assegurar a qualidade do dado pessoal proporcionam que os dados coletados estejam exatos e relevantes para o cumprimento da lei.

A organização deve também implementar processos para garantir que o tratamento de dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso e implementar medidas para garantir a precisão dos dados pessoais coletados.

4.9 Controle 27: Compartilhamento, Transferência e Divulgação

Assim como ocorre com outras operações de tratamento, o compartilhamento, a transferência e a divulgação de dados pessoais devem ser realizados em conformidade com a LGPD, observando os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis.

Por que implementar?

De acordo com o art. 26 da LGPD o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. Já a comunicação ou uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado, o art. 27, deverá ser informado à autoridade nacional e dependerá de consentimento do titular.

A transferência internacional de dados pessoais está prevista na LGPD e deve ser realizada conforme os art. 33 a 36.

Ressalta-se que a organização no tocante a este controle deve, principalmente, identificar e documentar as finalidades específicas para o compartilhamento de dados pessoais.

A organização deve implementar medidas apropriadas para garantir que quaisquer compartilhamentos, transferências e divulgações de dados pessoais atendam requisitos de conformidade relevantes.

Fique Atento!

A ANPD disponibiliza em seu portal um Guia de Tratamento de Dados Pessoais pelo Poder Público que apresenta instruções claras sobre compartilhamento de dados pessoais pelo Poder Púbico.

Disponível em: Guia de Tratamento de Dados Pessoais pelo Poder Público da ANPD

4.10 Controle 28: Supervisão em Terceiros

A supervisão em terceiros visa a garantir, através de meios contratuais ou outros, como políticas internas obrigatórias, que o terceiro destinatário implemente ações previstas pelo controlador no intuito de atender aos requisitos de conformidade com as leis e regulamentos de proteção de dados em vigor e requisitos de privacidade.

Por que implementar?

O art. 39 da LGPD estabelece que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

As organizações devem implementar medidas apropriadas para garantir que contratados e processadores de dados pessoais cumpram as cláusulas contratuais previstas no momento do estabelecimento de acordo entre as partes interessadas.

Um contrato pode estabelecer as responsabilidades de cada parte diferentemente, porém, para ser consistente com este documento, convém que todos os controles sejam considerados e incluídos na informação documentada.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Requisitos e Obrigações quanto à Segurança da Informação e à Privacidade que orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de segurança e privacidade dos dados.

Disponível em: Guia de Requisitos e Obrigações quanto a Privacidade e à Segurança da Informação

4.11 Controle 29: Abertura, Transparência e Notificação

O órgão, ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas, deverá dar publicidade sobre a finalidade e a forma como o dado será tratado.

Por que implementar?

A Abertura, Transparência e Notificação buscam atender o princípio de transparência da LGPD, art. 6º, inciso VI. O referido princípio, de acordo com a lei, é a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.

O controlador, ao tratar dados pessoais, deve atender a este princípio, assegurando a disponibilização de informações claras, precisas e facilmente

acessíveis aos titulares sobre o tratamento de seus dados.

As informações exigidas pela LGPD devem ser disponibilizadas de forma adequada, ostensiva, em linguagem simples e acessível, de modo a assegurar o efetivo conhecimento do titular a respeito das atividades de tratamento realizadas pelo controlador, bem como sobre os seus direitos e a forma de exercê-lo.

Constitui uma boa prática manter as informações de forma clara e atualizada no que diz respeito à previsão legal, finalidade, procedimentos e às práticas utilizadas para a execução dessas atividades e divulgá-las em meios de fácil acesso, preferencialmente na página eletrônica dos órgãos e das entidades responsáveis.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Elaboração de Termo de Uso e Política de Privacidade que apresenta instruções claras sobre como criar um termo de uso e política de privacidade.

Disponível em: Guia de Elaboração de Termo de Uso e Política de Privacidade

4.12 Controle 30: Avaliação de Impacto, Monitoramento e Auditoria

Este controle visa a avaliar a necessidade de implementar, onde apropriado, uma avaliação de impacto à proteção de dados pessoais, quando novos tratamentos ou mudanças no tratamento existente de dados pessoais forem planejados e documentar medidas adotadas para a mitigação dos riscos identificados. Além disso, o controle visa a revisão contínua da postura de proteção de dados pessoais e privacidade da organização por meio de monitoramento e auditoria interna ou de forma independente para verificar a eficácia das medidas protetivas, políticas, processos e procedimentos implementados objetivando a conformidade com leis e regulamentos relativos à proteção de dados pessoais e privacidade.

Por que implementar?

A LGPD define o RIPD como uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Conforme previsto nos art. 4º, 10, 32 e 38, a ANPD poderá solicitar aos controladores, responsáveis pelo tratamento de dados pessoais, relatórios de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento, nos termos de regulamento, observados os segredos comercial e industrial.

As medidas para remediar uma violação de privacidade devem ser proporcionais aos riscos associados à violação, mas devem ser implementadas o mais rápido possível (a menos que proibido de outra forma, por exemplo, interferência em uma investigação legal).

O art. 50 da LGPD estabelece que sejam realizadas atualizações do programa de governança em privacidade com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas das medidas técnicas e administrativas adotadas.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Avaliação de Riscos que orienta a identificação e a mensuração de riscos de segurança e privacidade, mitigando-os com a utilização dos controles mais indicados, e um Guia de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais que orienta a elaboração de documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação.

Documentação disponível em:

Guia de Elaboração de Avaliação de Riscos

Guia de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais

4.13 Controle 31: Segurança Aplicada à Privacidade

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.

Por que implementar?

Os dados pessoais sob os cuidados e custódia do Poder Público devem ser protegidos conforme orientações previstas na LGPD em seus artigos 46, 47, 49 e 50.

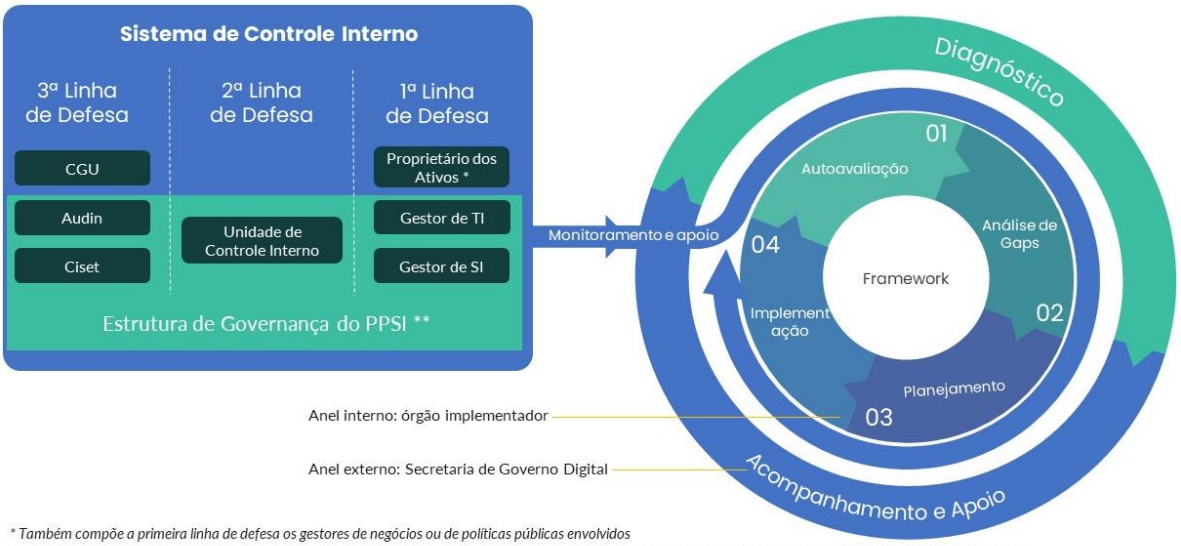
Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais devem de forma estruturada atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.

Os dados pessoais sob custódia da organização devem ser protegidos por controles apropriados, de acordo com os resultados de uma avaliação de risco de ameaça e/ou impacto na privacidade.

5. IMPLEMENTAÇÃO

Neste capítulo é descrita a metodologia de implementação deste **Framework de Privacidade e Segurança da Informação**. A metodologia adotada é composta pela atuação de um Sistema de Controle Interno (SCI) e pela execução de dois ciclos de execução de atividades, um interno e outro externo. O SCI tem a função de monitorar e apoiar a execução do ciclo interno. O ciclo externo tem a função de acompanhar e apoiar o órgão implementador do **Framework** em suas ações por meio de diagnósticos de maturidade. O ciclo interno é inspirado no ciclo PDCA[28] globalmente difundido nas instituições em diversas frentes e é executado pelo órgão implementador do **Framework**. A Figura 3 resume a metodologia de implementação a ser empregada na aplicação deste **Framework** mostrando como estão relacionados ao SCI com os principais atores e as atividades a serem executadas.

Figura 3: METODOLOGIA DE IMPLEMENTAÇÃO DO FRAMEWORK.



5.1 Sistema de Controle Interno

O SCI envolvido com a implementação deste **Framework** é dividido em três linhas de defesa, conforme o previsto pela IN nº 3, de 9 de junho de 2017 publicada pela Controladoria-Geral da União (CGU). A primeira linha de defesa é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as

[28] Disponível em: https://www.iso-9001-checklist.co.uk/learn-about-ISO-9001.htm

atividades sejam realizadas de acordo com as metas e objetivos da organização. As instâncias de segunda linha de defesa estão situadas ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada. A terceira linha de defesa é representada pela atividade de auditoria interna governamental, que presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade.

Na primeira linha de defesa atuam os Gestores de TI, os Gestores de Segurança da Informação, os Proprietários de Ativos e os Gestores do negócio ou de políticas públicas envolvidos. A segunda linha de defesa tem a atuação da Unidade de Controle Interno do órgão implementador do **Framework**. Na terceira linha de defesa, atuam a CGU, Auditoria Interna (Audin) e a Ciset[29], detalhes sobre atuação dessa linha de defesa podem ser observados na IN CGU nº 3, de 2017.

5.1.1 *Estrutura de Governança do Programa de Privacidade e Segurança da Informação (PPSI)*

A primeira e a segunda linha de defesa, citadas na introdução deste capítulo, representam a estrutura principal responsável pela governança do PPSI. A terceira linha de defesa compõe a mencionada estrutura de governança nos casos em que a Unidade de Controle Interno acumular os papéis da segunda e terceira linha de defesa.

O PPSI é constituído por um conjunto de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo das disciplinas de governança, pessoas, metodologia, tecnologia e gestão de maturidade, implementadas de forma concomitante e incremental. Tais ações são lideradas pela Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital, voltadas para aumento do grau de maturidade e de resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de TI (SISP) do Poder Executivo Federal.

A proposição deste **Framework** e sua implementação são ações resultantes do PPSI. Para saber mais sobre o PPSI visite a página sobre Segurança e Proteção de Dados mantida pela SGD/MGI.

A seguir, é destacado o realizado por cada papel da primeira e segunda linha de defesa na implementação do **Framework**.

[29] Secretarias de Controle Interno (Ciset) da Presidência da República, da Advocacia-Geral da União, do Ministério das Relações Exteriores e do Ministério da Defesa, e respectivas unidades setoriais.

- Papéis na primeira linha de defesa.

O Gestor de TI atua para planejar, implementar, melhorar e otimizar continuamente os processos e procedimentos que envolvem a área de TI.

Por sua vez, a atuação do Gestor de SI se concentra na criação e administração das métricas e indicadores da área de segurança da informação, gerencia as oportunidades de aplicação de tecnologia e interage com outras áreas de maneira a assegurar a segurança das informações da empresa.

Por fim, os Proprietários de Ativos e Gestores do negócio ou de políticas públicas são responsáveis pelos controles primários, inclusive envolvendo adoção de medidas de privacidade e proteção de dados pessoais, no que se refere à implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio.

- Papel na segunda linha de defesa.

A Unidade de Controle Interno ou estruturas equivalentes contribui no sentido de assegurar que os controles de privacidade e segurança da informação sejam executados de forma apropriada, por meio do desempenho das funções de apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa.

- Papel do Encarregado na Estrutura de Governança do PPSI.

O Encarregado desempenha o papel de fomentar e orientar o planejamento, a implementação e melhoria contínua dos controles de privacidade em serviços ou produtos que realizem o tratamento de dados pessoais ou dados pessoais sensíveis. Apoiando, no que couber, a primeira e segunda linhas de defesa.

5.2 Ciclo Externo

A implementação deste **Framework** é auxiliada pela SGD por meio das ações de diagnóstico, acompanhamento e apoio presentes no anel externo da Figura 3. O diagnóstico terá como base os controles e medidas do próprio **Framework**, e o acompanhamento e apoio se baseará nos resultados desse diagnóstico tal como o nível de maturidade do órgão implementador em privacidade e segurança da informação. Esse nível de maturidade varia conforme a execução das ações de implementação deste **Framework** representado pelo ciclo interno da Figura 3.

5.2.1 *Diagnóstico*

O diagnóstico permite que a SGD tenha uma visão do nível de maturidade dos órgãos em relação à privacidade e segurança, bem como uma visão dos controles e medidas identificados pela análise de *gaps,* etapa do ciclo interno*.* Tal análise possibilita a identificação das medidas de privacidade e segurança da informação a serem adotadas como melhorias e priorizadas em plano de ação.

5.2.2 *Acompanhamento e Apoio*

A SGD atuará no acompanhamento da implementação das melhorias priorizadas no plano de ação, etapa de implementação do ciclo interno, e fornecerá apoio com reuniões técnicas, indicação e produção de material orientativo para auxiliar na implementação dos controles e das medidas de privacidade e segurança da informação.

5.3 Ciclo Interno

O ciclo interno é composto por etapas a serem executadas pelo órgão implementador deste **Framework**, com o apoio da SGD por meio das ações que compõem o ciclo externo. O ciclo inspira-se no modelo PDCA, que é um mecanismo interativo e contínuo estruturado em quatro fases para a gestão: Planejar, Fazer, Checar e Agir.

Como nenhum processo é perfeito e sempre é possível aprimorá-lo, a abordagem do PDCA oferece condições para gerir seu funcionamento com foco na qualidade. Como ele consiste em um método cíclico de aperfeiçoamento, as instituições e profissionais que empregam um ciclo semelhante ao PDCA estão sempre em evolução usando o aprendizado de ações anteriores. Eles agregam os conhecimentos recém adquiridos no intuito de planejar novamente, eliminar falhas, desperdícios e aumentar sua competitividade.

Dessa forma, as etapas do ciclo interno de execução do **Framework** são: Autoavaliação, Análise de Gaps, Planejamento e Implementação. Tais etapas são apresentadas a seguir.

5.3.1 *Autoavaliação*

A autoavaliação terá como finalidade o autoconhecimento do órgão acerca dos controles e medidas adotados em segurança cibernética e privacidade. Para tal, será disponibilizado um questionário por meio de uma ferramenta fornecida pela SGD que

apresentará um Dashboard para auxiliar no direcionamento das ações. As questões constantes da ferramenta são as elencadas pelas medidas dos controles constantes dos Anexos III, IV e V deste documento.

A abordagem adotada para fazer essa autoavaliação será o *Control Self-Assessment* (CSA[30]) destacada pelas seções 6.2 e 6.3 deste documento.

5.3.2 *Análise de Gaps*

Esta etapa consiste, a partir das respostas fornecidas na etapa anterior, em identificar quais as falhas, lacunas ou melhorias relacionadas com privacidade e segurança da informação foram identificadas na autoavaliação. Uma vez identificados os *gaps* segue-se para a próxima etapa do ciclo interno de execução do **Framework**.

5.3.3 *Planejamento*

A etapa de planejamento tem como finalidade estabelecer um plano de ação com as medidas de privacidade e segurança da informação a serem implementadas ou melhoradas.

A priorização das medidas de privacidade e segurança da informação que constarão do plano de ação deve considerar a realidade institucional e considerar parâmetros que auxiliem na identificação de quais medidas priorizar.

Inicialmente, indica-se a priorização das medidas relacionadas com o controle de estruturação básica de gestão em privacidade e segurança da informação identificado neste **Framework** como Controle 0 - Estrutura Básica de Gestão em Privacidade e Segurança da Informação.

No âmbito da segurança cibernética, a metodologia baseada nos GIs do CIS fornece um excelente parâmetro nas escolhas ou determinação das medidas a serem implementadas ou priorizadas.

O GI1 do CIS tem foco na higiene cibernética por meio de medidas que devem ser implementadas por qualquer negócio ou instituição, pois abordam as práticas gerais que a maioria das instituições devem tomar para proteger seus sistemas dos ataques mais comuns ou impedir ataques gerais não direcionados (Figura 4).

Nesse cenário, este **Framework** propõe que as instituições públicas, independentemente da complexidade do ambiente tecnológico, devem adotar as 56 medidas do GI1 do CIS.

[30] https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles/

A adoção dos GIs 2 e 3 do CIS levará em consideração se a instituição mantém em seu ambiente tecnológico algum sistema relevante crítico, a partir de análise com base no Modelo de Avaliação de Criticidade de Sistemas apresentado pelo Anexo I.

Dessa forma, se a instituição identifica algum sistema com nível de criticidade deve-se adotar os controles dos GIs 2 e/ou 3 do CIS.

Figura 4: GRUPOS DE IMPLEMENTAÇÃO DO CIS COM DESTAQUE PARA HIGIENE CIBERNÉTICA (ADAPTADO DO CIS CONTROL v8)

Em relação à priorização das medidas de privacidade, adotou-se também a implementação por grupos. Assim como em segurança cibernética, serão 3 Grupos (GI1, GI2 e GI3).

A abordagem adotada por este **Framework** para a escolha das medidas que constarão no GI1 de privacidade se baseia nas obrigações dispostas na LGPD.

A priorização das medidas de privacidade para o GI1 neste **Framework** se baseou também, de forma complementar, na adoção das funções "Identificar-P" e "Governar-P" sugeridas pelo *NIST Privacy Framework* como método simplificado para criar ou aprimorar um programa de privacidade.

Seguindo a mesma ideia da segurança cibernética, este **Framework** propõe que as instituições públicas, independentemente da complexidade do ambiente tecnológico, devem adotar as medidas constantes no GI1 de privacidade, conforme explicado pelos parágrafos acima.

Os GI2 e GI3 de privacidade se basearam nas boas práticas estabelecidas nas

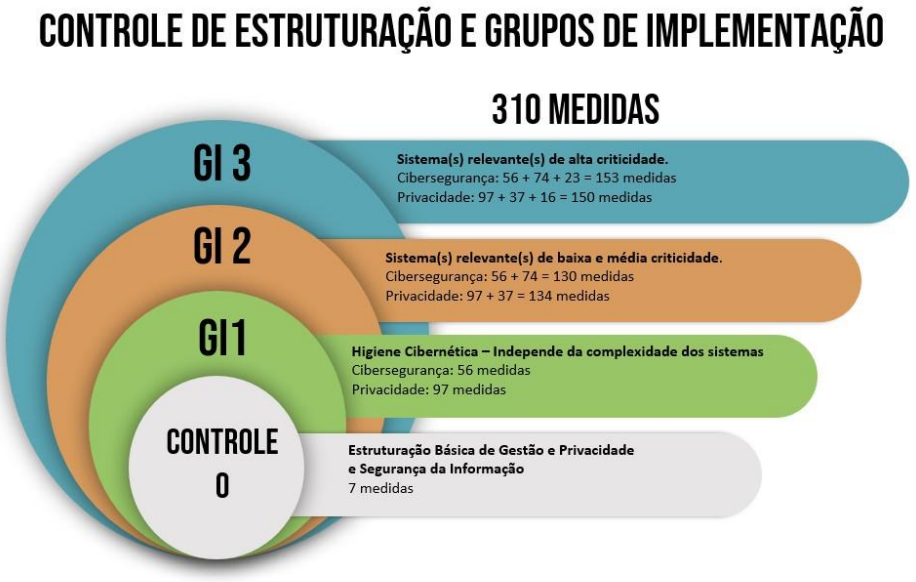
normas, frameworks e guias que fundamentaram este **Framework**, conforme capítulo 1. Assim como estabelecido na priorização das medidas de segurança cibernética, as medidas dos GI2 e GI3 de privacidade levará em consideração o nível de criticidade dos sistemas em seu ambiente tecnológico.

A tabela abaixo sintetiza os GIs que devem ser adotados na aplicação deste **Framework**.

Tabela 1: GRUPOS DE IMPLEMENTAÇÃO UTILIZADOS NESTE FRAMEWORK

Grupo de Implementação	Framework - Aplicação das medidas
GI1	Aplicável para todas as instituições e seus ambientes tecnológicos independente da complexidade do(s) sistema(s)
GI1 + GI2	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de baixa e média criticidade
GI1 + GI2 + GI3	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de alta criticidade

Figura 5: DISTRIBUIÇÃO DAS MEDIDAS NOS GRUPOS DE IMPLEMENTAÇÃO



A Figura 5 apresenta em maiores detalhes a relação entre os GIs, incluindo a quantidade agregada de medidas a serem implementadas e os requisitos para implementação em cada GI, destacando também o total de medidas do Controle 0 – Estruturação básica de gestão em privacidade e segurança da informação. Cumpre destacar que as medidas do Controle 0 devem ser implementadas pela instituição independente da complexidade dos sistemas.

Cumpre evidenciar que as medidas do Framework destacadas pela Tabela 1

e Figura 5 devem ser considerados para a aplicação em toda a cadeia de suprimentos envolvida com o sistema e ambiente tecnológico que o sustenta.

Esta etapa de Planejamento pode auxiliar no sentido de fornecer parâmetros aos gestores públicos no planejamento orçamentário prevendo contratações de bens, tais como firewall e roteadores, serviços (por exemplo, software de gestão de incidentes), licenças de antivírus, e recursos humanos especializados tais como analistas de segurança, consultores em privacidade, desenvolvedores, entre outros. Essas contratações servem para alavancar suas operações em privacidade e segurança cibernética e entregar resultados com mais efetividade, eficácia, eficiência, transparência e lisura dos entes públicos.

5.3.4 *Implementação*

Após a autoavaliação do ambiente do órgão, a análise de *gaps* e o planejamento das atividades a serem executadas para melhorar a privacidade e a segurança da informação, deve-se implementar os processos (controles e medidas) determinados na etapa anterior de acordo com as normas de proteção de dados pessoais, privacidade e segurança cibernética vigentes, para que o órgão mitigue ou aceite possíveis impactos a serem causados no negócio, devido as vulnerabilidades e ameaças de segurança cibernética.

Quando aplicável, devem ser atendidos de forma prioritária os controles e medidas recomendadas em Notas Técnicas, ou instrumentos equivalentes, a serem publicadas pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.

Além disso é necessário que o órgão eduque e treine todos os envolvidos no processo para garantir que estejam comprometidos com as atividades de conformidade e que tudo ocorra conforme o planejamento realizado na etapa anterior.

É recomendado também que órgão estabeleça e execute procedimentos de monitoramento das implementações dos controles e medidas planejados para documentar as dificuldades e os progressos durante a execução, isso permite um aprendizado necessário ao time envolvido durante todo o processo.

A realização de testes exaustivos dos controles e medidas implementados aumentam a confiabilidade no sistema em relação à segurança cibernética, à proteção de dados pessoais e à privacidade.

Finalizada esta etapa, inicia-se novamente o clico interno com nova autoavaliação

dentro do ciclo de melhoria contínua.

A SGD disponibiliza ferramenta que automatiza o ciclo interno, destacado por este capítulo, a ser realizado pelos órgãos e entidades. O capítulo 7 deste Guia apresenta informações sobre a referida ferramenta.

6. MATURIDADE

A maturidade tem foco na avaliação e gestão do grau de proteção dos sistemas no ambiente de privacidade e cibernético. Os mecanismos para medir este grau são constituídos pelos índices de maturidade em privacidade e segurança da informação do órgão, que o subsidiarão na implementação e monitoramento dos controles e medidas de privacidade e segurança cibernética.

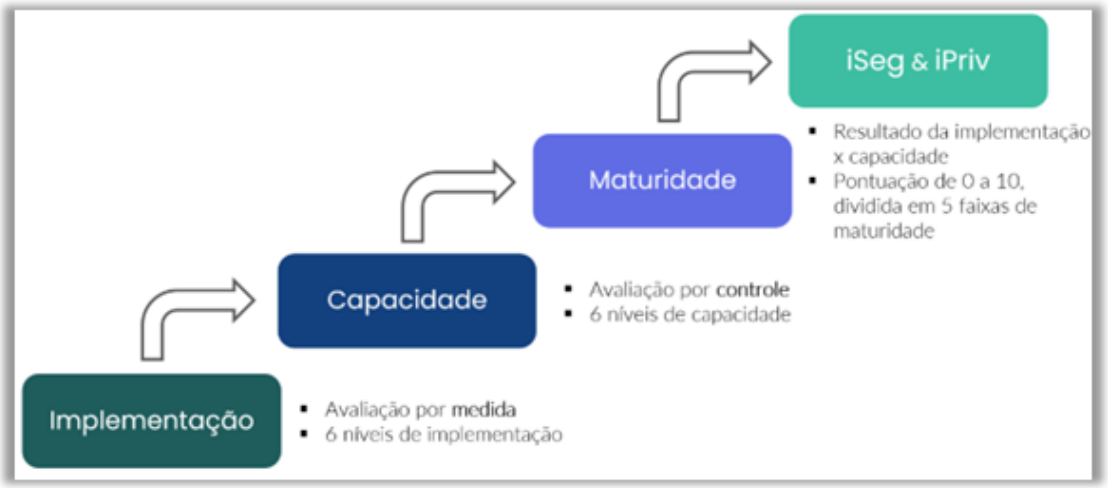
6.1 Capacidade e Maturidade

Para expressar o desempenho quanto ao atendimento dos controles previstos neste **Framework**, propõe-se realizar avaliações de capacidade e de maturidade para obtenção dos indicadores de maturidade em privacidade (iPriv) e em segurança da informação (iSeg) da sua organização.

Para isso, deverá ser adotada uma abordagem em profundidade, com avaliação do nível de implementação de cada medida, passando pela avaliação do nível de capacidade e maturidade por controle, o que resultará nos indicadores iSeg e iPriv.

A imagem a seguir demonstra todos os níveis necessários para compor a avaliação:

Figura 6: ETAPAS NECESSÁRIAS PARA REALIZAR A AVALIAÇÃO



A avaliação de maturidade consiste nas seguintes etapas:

1. Implementação: Avaliação e seleção do nível de implementação por medida.
2. Capacidade: Avaliação e seleção do nível de capacidade por controle.
3. Maturidade: Obtenção do nível de maturidade por controle.

4. iSeg & iPriv: Obtenção do índice de maturidade em segurança (iSeg) e do índice de maturidade em privacidade (iPriv) com base nas respostas fornecidas em relação à adoção das medidas de cada controle.

6.2 Quem deve executar a avaliação?

A presente avaliação poderá ser aplicada pela própria organização, considerando o método CSA, ou no que couber pela Unidade de Controle Interno da instituição.

Para avaliação da segurança da informação pela própria organização, por meio do método CSA, o responsável será o Gestor de Segurança da Informação, que deve contar com o apoio do Gestor de TI e, caso necessário, consultar o Encarregado pelo Tratamento de Dados Pessoais, bem como, os proprietários de ativos e gestores de negócios ou de políticas públicas envolvidos.

Para privacidade, o Encarregado pelo Tratamento de Dados Pessoais é quem atua na condução da avaliação, que deve contar com o apoio do Gestor de Segurança da Informação e do Gestor de TI. Também poderá ser necessário consultar os proprietários de ativos, gestores de negócios ou de políticas públicas envolvidos que tratam dados pessoais ou dados pessoais sensíveis.

Ressalta-se que, apesar das temáticas privacidade e segurança da informação possuírem forte relação, conforme exposto no framework, os indicadores iPriv e iSeg devem ser avaliados e calculados separadamente, gerando dois indicadores isolados. Dessa forma, as quatro etapas para avaliação devem ser aplicadas isoladamente tanto para os controles e medidas de privacidade quanto para os de segurança da informação.

6.3 Etapas da avaliação

6.3.1 *Implementação: Avaliação e seleção do nível de implementação por medida*

O avaliador deverá analisar cada uma das medidas listadas neste framework, individualmente, aplicando um nível de implementação para cada uma delas.

O nível de implementação expressa uma análise sobre a amplitude de implementação da respectiva medida, considerando a abrangência de ativos de informação que possuem aplicabilidade.

O avaliador deverá selecionar um dos níveis de implementação listados na tabela a seguir para cada medida:

Tabela 2: NÍVEIS DE IMPLEMENTAÇÃO A SEREM APLICADOS EM CADA MEDIDA

Nível de Implementação	Descrição	Pontuação
Adota em maior parte ou totalmente	Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente em mais de 50% ou em todos os: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	1
Adota em menor parte	Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,75
Adota parcialmente	Há decisão formal ou plano aprovado, e a medida na organização é implementada parcialmente em mais de 50% ou em todos os: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,5
Há decisão formal ou plano aprovado para implementar	Há decisão formal ou plano aprovado, porém não há na organização implementação ou está parcialmente implementado em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,25
A organização não adota essa medida	Não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.	0
Não se aplica	A medida não se aplica em nenhum ativo no caso de medida de segurança da informação ou processo/serviço no caso de medida de privacidade, por entendimento dos gestores ou considerando alguma particularidade do contexto de atuação da organização. A não aplicabilidade deverá seguir de uma motivação baseada em uma análise de riscos.	-

Considera-se que ativos de informação são meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

Importante ressaltar que, para avaliar o nível de implementação das medidas dos controles de Privacidade, devem ser considerados os serviços ou produtos que realizam

o tratamento de dados pessoais e/ou dados pessoais sensíveis.

Os níveis de implementação aplicáveis ao Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade consistem numa resposta binária de “Sim” ou “Não”.

O avaliador deverá selecionar um dos níveis de implementação listados na tabela a seguir para cada medida:

Tabela 3: NÍVEIS DE IMPLEMENTAÇÃO A SEREM APLICADOS NAS MEDIDAS DO CONTROLE 0

Nível de Implementação	Descrição	Pontuação
Sim	O papel ou instrumento foi devidamente instituído na organização.	1
Não	O papel ou instrumento não foi devidamente instituído na organização.	0

6.3.2 *Capacidade: Avaliação e seleção do nível de capacidade por controle*

Diferentemente do nível de implementação, que foca em aspectos quantitativos, o nível de capacidade foca no aspecto qualitativo, e tem como objetivo avaliar o nível de efetividade da adequação de um controle. Além disso, a avaliação é realizada por controle, e não por medida.

O avaliador deverá considerar um dos níveis de capacidade a seguir para cada controle:

Tabela 4: NÍVEIS DE CAPACIDADE POR CONTROLE

Nível de Capacidade	Descrição	Índice
0	Ausência de capacidade para a implementação das medidas do controle, ou desconhecimento sobre o atendimento das medidas.	0
1	O controle atinge mais ou menos seu objetivo, por meio da aplicação de um conjunto incompleto de atividades que podem ser caracterizadas como iniciais ou intuitivas (pouco organizadas).	20
2	O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.	40
3	O controle atinge seu objetivo de forma muito mais organizada utilizando os recursos organizacionais. Além disso, o controle é formalizado por meio de uma política institucional, específica ou como parte de outra maior.	60
4	O controle atinge seu objetivo, é bem definido e suas medidas são implementadas continuamente por meio de um processo decorrente da política formalizada.	80

Nível de Capacidade	Descrição	Índice
5	O controle atinge seu objetivo, é bem definido, suas medidas são implementadas continuamente por meio de um processo e seu desempenho é mensurado quantitativamente por meio de indicadores.	100

6.3.3 *Maturidade: Obtenção do nível de maturidade por controle*

A maturidade é obtida por meio da relação entre a avaliação quantitativa e a qualitativa, ou seja, considerando os níveis de implementação atribuídos às medidas e os níveis de capacidade atribuídos aos controles.

Dessa forma, considerando as avaliações realizadas nas etapas 1 e 2, as pontuações correspondentes dos níveis de implementação e os índices correspondentes aos níveis de capacidade deverão ser aplicados na seguinte fórmula:

$$iMC = \frac{\left(\frac{\sum PMC}{QMC - QMNAC}\right)}{2} * \left(1 + \frac{iNCC}{100}\right) \quad (1)$$

Onde:
$iMC = indicador\ de\ maturidade\ por\ controle$
$PMC = somatório\ das\ pontuações\ das\ medidas\ avaliadas\ no\ controle$
$QMC = quantidade\ de\ medidas\ do\ controle$
$QMNAC = quantidade\ de\ medidas\ não\ aplicáveis\ do\ controle$
$iNCC = índice\ do\ nível\ de\ capacidade\ do\ controle$

Além de obter o valor numérico do indicador de maturidade (iMC) por controle, este poderá ser enquadrado em uma faixa de nível de maturidade, considerando a tabela a seguir:

Tabela 5: RELAÇÃO ENTRE O INDICADOR E O NÍVEL DE MATURIDADE POR CONTROLE

iMC	Nível de Maturidade
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

6.3.4 *iSeg & iPriv: Obtenção do iSeg e/ou iPriv*

Após calculada a maturidade de todos os controles de segurança da informação ou de privacidade, os valores dos indicadores de maturidade por controle devem ser aplicados às fórmulas a seguir:

Fórmula de avaliação do iSeg

$$iSeg = \frac{(iMC_0 * 4) + \sum_{i=1}^{18} iMC_i}{22} \quad (2)$$

Onde:

$iSeg = indicador\ de\ maturidade\ de\ segurança\ da\ informação$
$i\ =\ número\ do\ controle\ avaliado, considerando\ os\ controles\ de\ 1\ a\ 18\ de\ Segurança$
$iMC = indicador\ de\ maturidade\ por\ controle$

Fórmula de avaliação do iPriv

$$iPriv = \frac{(iMC_0 * 4) + \sum_{i=19}^{31} iMC_i}{17} \quad (3)$$

Onde:

$iPriv = indicador\ de\ maturidade\ de\ privacidade$
$i\ =\ número\ do\ controle\ avaliado, considerando\ os\ controles\ de\ 19\ a\ 31\ de\ Privacidade$
$iMC = indicador\ de\ maturidade\ por\ controle$

Observa-se nas fórmulas que é considerado um indicador de maturidade por controle (iMC) com índice 0 (zero), ou seja, relativo ao Controle 0 – Estrutura Básica de Gestão em Privacidade e Segurança da Informação. Em virtude da importância quanto à instituição dos papéis e instrumentos em conformidade com a PNSI e com a LGPD, esse controle foi tratado separadamente dos demais controles, atribuindo peso 4 para tal. Tal abordagem aplica-se tanto para o iSeg quanto para o iPriv, pelo entendimento de que os papéis são essenciais para a cultura organizacional quanto às duas temáticas, e de que não há privacidade sem segurança da informação.

Assim como o iMC, o iSeg e iPriv utilizam os níveis de maturidade da tabela a seguir:

Tabela 6: RELAÇÃO ENTRE OS INDICADORES DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO OU PRIVACIDADE E OS NÍVEIS DE MATURIDADE

iSeg / iPriv	Nível de Maturidade
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Nesse cenário, é apresentado a seguir exemplo de avaliação de capacidade e maturidade de segurança com base em simulação para os controles: “Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade”; “Controle 05 – Gestão de Contas”; e “Controle 18 – Testes de Invasão”.

Avaliação do Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 0.1	Atendido (1)	3,00	7	0	**Nível 2**	40
Medida 0.2	Não Atendido (0)					
Medida 0.3	Atendido (1)					
Medida 0.4	Atendido (1)					
Medida 0.5	Não Atendido (0)					
Medida 0.6	Não Atendido (0)					
Medida 0.7	Não Atendido (0)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[3,00 / (7-0)] / 2} * (1 + 40/100) = [(3,00 / 7) / 2] * (1 + 40/100) = (0,43 / 2) * (1 + 40/100) = 0,21 * (1 + 40/100) = 0,21 + 0,09 = **0,30**
Dessa forma, **o indicador de maturidade do Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade seria 0,30 ou nível de maturidade Básico**

Avaliação do Controle 05 – Gestão de Contas

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 5.1	Adota em maior parte ou totalmente (1)	3,00	6	0	**Nível 3**	60
Medida 5.2	Adota em maior parte ou totalmente (1)					
Medida 5.3	Adota em menor parte (0,75)					
Medida 5.4	Há decisão formal ou plano aprovado para implementar (0,25)					
Medida 5.5	A organização não adota essa medida (0)					
Medida 5.6	A organização não adota essa medida (0)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[3,00 / (6 - 0)] / 2} * (1 + 60/100) = [(3,00 / 6) / 2] * (1 + 60/100) = (0,50 / 2) * (1 + 60/100) = 0,25 * (1 + 60/100) = 0,25 + 0,15 = **0,40**
Dessa forma, **o indicador de maturidade do Controle 05 – Gestão de Contas seria 0,40 ou nível de maturidade Básico**

Avaliação do Controle 18 – Testes de Invasão

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 18.1	Adota em maior parte ou totalmente (1)	4,00	5	1	**Nível 4**	80
Medida 18.2	Adota em maior parte ou totalmente (1)					
Medida 18.3	Adota em maior parte ou totalmente (1)					
Medida 18.4	Adota em maior parte ou totalmente (1)					
Medida 18.5	Não se aplica (-)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[4,00 / (5 - 1)] / 2} * (1 + 80/100) = [(4,00 / 4) / 2] * (1 + 80/100) = (1,00 / 2) * (1 + 80/100) = 0,50 * (1 + 80/100) = 0,50 + 0,40 = **0,90**
Dessa forma, **o indicador de maturidade do Controle 18 – Testes de Invasão seria 0,90 ou nível de maturidade Aprimorado**

Nesse contexto, a avaliação do iSeg para o exemplo apresentado acima é destacada abaixo.

Avaliação do iSeg

O iSeg é composto por 19 controles, incluindo o controle 0. No entanto, para fins exemplificativos e didáticos, considera-se que serão avaliados apenas três controles para composição do iSeg, conforme já realizado acima: os controles 0, 5 e 18.

Como demonstrado, após avaliação realizada nos três controles, foram obtidos os seguintes iMC:

Controle 0 – Papéis e Instrumentos: **0,30 ou Básico**

Controle 5 – Gestão de Contas: **0,40 ou Básico**

Controle 18 – Testes de Invasão: **0,90 ou Aprimorado**

Dito isso, aplicam-se os valores na fórmula do iSeg (assumindo que trabalhemos apenas com 3 controles neste exemplo), obtendo-se o seguinte resultado arredondado para duas casas decimais:

iSeg = [(0,30 * 4) + 0,40 + 0,90] / 6 = **0,42**

Ou seja, neste exemplo o indicador de maturidade de segurança da informação (iSeg) teria 0,42 de maturidade, ou nível Básico

A SGD disponibiliza ferramenta que automatiza a implementação deste **Framework**, inclusive os cálculos de maturidade destacado por este capítulo. O capítulo 7 deste Guia apresenta informações sobre a referida ferramenta.

7. FERRAMENTA DE ACOMPANHAMENTO DA IMPLEMENTAÇÃO DO FRAMEWORK

Com a finalidade de facilitar a aplicação e acompanhamento da implementação do **Framework de Privacidade e Segurança da Informação**, a SGD desenvolveu uma ferramenta em formato de planilha na qual poderão ser obtidos e acompanhados indicadores de maturidade de privacidade e segurança da informação do órgão mediante preenchimento de diagnósticos.

Detalhes sobre o uso e funcionalidades da ferramenta podem ser observados no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/manual_ferramenta_framework.pdf

8. CONSIDERAÇÕES FINAIS

A transformação digital dos serviços públicos é uma realidade no âmbito das organizações públicas brasileiras, demandando uma estrutura de governança que permeie toda organização, com especial atenção, na elaboração de diretrizes pela alta administração, estratégias de implementação e o efetivo monitoramento da implementação dos controles de privacidade e segurança da informação.

Desse modo, o **framework** visa, principalmente, a auxiliar aos gestores da primeira linha de defesa a identificar precocemente fragilidades nas práticas de privacidade e segurança da informação que possam comprometer o desenvolvimento e execução dos serviços, dos produtos e dos processos de trabalhos internos que colaboram para o alcance dos objetivos institucionais.

Extremamente importante ressaltar que o patrocínio da alta administração do representa fator crítico de sucesso para a implementação deste **Framework** na instituição. Desse modo, é fundamental que a alta administração demonstre seu comprometimento com a adoção dos controles e medidas de privacidade e segurança da informação estabelecidos pelo **Framework** por meio de ações que assegurem:

- a estruturação básica de gestão de privacidade e segurança da informação;
- os recursos orçamentários necessários;
- a capacitação dos recursos humanos envolvidos; e
- a implementação do **framework** como parte do programa de governança em privacidade e segurança da informação do órgão ou entidade.

Diante do exposto, a adoção do **Framework de Privacidade e Segurança da Informação** pelas instituições públicas proporcionará benefícios como:

1. ampliação da confiabilidade e da proteção de sistemas informáticos contra os principais ataques que podem resultar em incidentes de segurança;
2. aprimoramento da privacidade e da proteção dos dados pessoais dos cidadãos inseridos nas bases de dados governamentais;
3. aumento da confiança da população na prestação de serviços digitais por parte do governo federal;
4. disseminação da cultura de privacidade e segurança da informação na instituição;

5. criação de uma linguagem comum de controles e de medidas de privacidade e segurança para os órgãos do SISP e demais partes interessadas; e
6. aumento da confiança mútua para compartilhamento de dados entre as instituições públicas devido a evolução dos níveis de maturidade em privacidade e segurança da informação dos ambientes tecnológicos.

Por fim, com a publicação deste Framework, a SGD segue firme no propósito de definir orientações que promovam proteção a dados pessoais e a segurança da informação no âmbito da APF, em articulação com os órgãos responsáveis por políticas públicas.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal uma série de guias operacionais, que incentiva e auxilia na conformidade de normativos vigentes sobre o tema de privacidade, proteção de dados pessoais e segurança da informação.

Disponível em: Guia Operacionais da SGD

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança dainformação - Requisitos. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles desegurança da informação. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27701:2019**: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro,2019.

_____. **ABNT NBR ISO/IEC 27184:2021**: Tecnologia da informação - Avisos de privacidade *on-line* e consentimento. Rio de Janeiro,2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Decreto nº 9.637, de 26 de dezembro de 2018. **Política Nacional de Segurança da Informação – PNSI**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm . Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. **Glossário de Segurança da Informação**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01, de 27 de maio de 2020**. Brasília, DF, GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. **Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022**. Brasília, DF, SGD/ME, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019. Acesso em: 01 mar. 2023.

BRASIL. Presidência da República. Controladoria-Geral da União. **Instrução Normativa nº 03, de 09 de junho de 2017**. Brasília, DF, CGU, 2017. Disponível em: https://wiki.cgu.gov.br/index.php/Instru%C3%A7%C3%A3o_Normativa_n%C2%BA_3,_de_9_de_junho_de_2017. Acesso em: 01 jul. 2022.

CENTER INTERNET SECURITY. **CIS Controls**, versão 8.0. Maio de 2021. Disponível em: https://www.cisecurity.org/controls. Acesso em: 01 jul. 2022.

CENTER INTERNET SECURITY. **CIS Controls v8 Privacy Companion Guide**, versão 1.0. Janeiro de 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide-portuguese-translation. Acesso em: 01 jul. 2022.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Agosto de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf . Acesso em: 01 jul. 2022.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011**: Information technology — Security techniques — Privacy framework. Genebra, 2011.

_____. **ISO/IEC 29134:2017**: Information technology – Security techniques – Guidelines for privacy impact assessment. Genebra, 2017.

_____. **ISO 9001:2015**: Quality management systems — Requirements. Genebra, 2015.

_____. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.

_____. **ISO/IEC 27018:2014**: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Genebra, 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica, versão 1.1, 2018. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em: 01 jul. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. A estrutura de privacidade do NIST: uma ferramenta para melhorar a privacidade por meio do gerenciamento de riscos corporativos, versão 1.0, 2020. Disponível em: https://www.nist.gov/privacy-framework/privacy-framework. Acesso em: 01 jul. 2022.

_____. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020. Acesso em: 01 jul. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.109/2021. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 12/05/2021. Diário Oficial da União, Brasília, DF, 12 mai. 2021. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 jul. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.768/2022. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 03/08/2022. Diário Oficial da União, Brasília, DF, 03 ago. 2022. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 set. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.889/2022. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 17/08/2022. Diário Oficial da União, Brasília, DF, 17

ago. 2021. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 set. 2022.

ANEXO I – MODELO DE AVALIAÇÃO DE CRITICIDADE DE SISTEMAS

O modelo de avaliação de criticidade busca identificar qual é o nível de criticidade de cada sistema relevante da organização em razão de sua exposição a riscos de privacidade e segurança da informação.

O modelo adotado é uma adaptação do modelo exposto pelo TCU, por meio do Acórdão 1.889/2020-TCU-Plenário, que tinha como objetivo realizar levantamento de riscos em sistemas informacionais da APF.

Para aplicação deste modelo, considera-se os seguintes conceitos:

a) **Sistema de Informação** se trata de um "conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada", conforme definição do Glossário de Segurança da Informação GSI/PR.

   Um sistema de informação também pode ser entendido como o conjunto de softwares em uso, eventualmente embarcados em hardware específico, que apoiam processos de negócio, que resultem direta ou indiretamente em serviços aos cidadãos, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações. Este entendimento foi utilizado pelo TCU em seu Acórdão, e está compatível com a definição do Glossário de Segurança da Informação;

b) **Sistemas relevantes** - são aqueles que possuem significativo grau de importância para a organização. Para classificar um sistema como relevante, podem ser utilizados critérios como lista de precedência para ser posto a funcionar em caso de desastre/recuperação e opinião dos gestores ou da equipe de TI, tratamento de dados pessoais ou dados pessoais sensíveis, entre outros.

c) **Criticidade** de um sistema pode ser entendida como uma medida de exposição a riscos em razão dos impactos decorrentes de falhas e indisponibilidades do sistema e de suas vulnerabilidades;

d) **Impacto** é a consequência de um incidente de segurança da informação (indisponibilidade ou comprometimento da integridade ou da

confidencialidade) ou de uma falha decorrente de defeitos em um sistema. Exemplo: impedimento do funcionamento de atividade finalística da organização; e

e) **Vulnerabilidade** - pode ser entendida como uma suscetibilidade do sistema ou do ambiente em que ele opera de ter sua disponibilidade, integridade ou confidencialidade comprometida.

Os impactos e as vulnerabilidades associados ao sistema ou ao ambiente em que ele opera são fatores relevantes a serem considerados na classificação dos sistemas relevantes, uma vez que possuem potencial lesivo à organização, ao cidadão ou à sociedade como um todo, sendo necessária a utilização de um fator de ponderação para cada um dos parâmetros de avaliação, visando a refletir a importância relativa dos parâmetros quando comparados.

A aplicação do modelo será realizada pela própria organização, por meio do método CSA, os responsáveis serão o Gestor de Tecnologia da Informação e Comunicação e o Proprietário do Ativo (Gestor do sistema/do negócio/da política pública).

O processo inicia com a identificação dos sistemas relevantes, considerando a definição exposta anteriormente. Cada sistema relevante deverá ter seus impactos e vulnerabilidades identificadas, individualmente, aplicando-os ao cálculo para obtenção do nível de criticidade.

Para avaliação dos impactos associados ao sistema relevante, considera-se a tabela a seguir e os respectivos pesos, bem como as possíveis respostas para cada impacto:

- Sim – 1 ponto
- Não – 0 ponto

Tabela 7: IMPACTOS ASSOCIADOS AO SISTEMA RELEVANTE

#	Descrição do Impacto	Peso
1	Perda de vidas humanas ou dano grave para a saúde humana	20,0%
2	Danos ambientais graves	15,0%
3	Degradação significativa na prestação de serviço essencial ao cidadão	6,0%

#	Descrição do Impacto	Peso
4	Danos financeiros significativos à Administração Pública (própria organização ou outro órgão/entidade) ou aos cidadãos	6,0%
5	Danos significativos à reputação ou à credibilidade da organização	2,5%
6	Impedimento do funcionamento de atividade finalística da organização	6,0%
7	Degradação significativa da produtividade dos servidores/funcionários da organização que utilizam ou dependem do sistema	2,5%
8	Degradação significativa do funcionamento de atividades ou processos com características multi-institucionais e que envolvam diferentes esferas da administração ou dos poderes	6,0%
9	Conhecimento não autorizado de informações que possa acarretar dano à soberania e à integridade territorial nacionais; a planos e operações militares; a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional; às relações internacionais do país; a programas econômicos; e a assuntos diplomáticos e de inteligência (informações secretas ou ultrassecretas)	10,0%
10	Exposição indevida de dados pessoais sensíveis e que possa causar dano ao titular	6,0%
11	Efeito negativo na execução da política econômica do Brasil (fiscal, monetária e cambial)	10,0%
12	Degradação significativa do funcionamento de atividades ou serviços relacionados às infraestruturas críticas do Brasil (definidas na Política Nacional de Segurança de Infraestruturas Críticas)	10,0%

Para avaliação das vulnerabilidades associadas ao sistema relevante, considera-se a tabela a seguir e os respectivos pesos, bem como as possíveis respostas para cada vulnerabilidade:

- Questões 16 e 20:
  a) Não – 0 ponto
  b) Sim, menos da metade do sistema/módulo – 0,33 ponto
  c) Sim, mais da metade do sistema/módulo – 0,66 ponto
  d) Sim, totalmente – 1 ponto.
- Demais questões:
  a) Não – 1 ponto
  b) Sim, menos da metade do sistema/módulo – 0,66 ponto
  c) Sim, mais da metade do sistema/módulo – 0,33 ponto
  d) Sim, totalmente – 0 ponto

Tabela 8: VULNERABILIDADES ASSOCIADAS AO SISTEMA RELEVANTE

#	Descrição da Vulnerabilidade	Peso
13	O sistema está coberto por solução de continuidade de serviços de TI (alta disponibilidade, recuperação de desastres e planos de contingência)	10,0%
14	O sistema é suportado por equipe de respostas a incidentes	8,0%
15	As vulnerabilidades e os riscos de TI relacionados ao sistema e à infraestrutura que o sustenta estão identificados, classificados, analisados e tratados	20,0%
16	O sistema possui tecnologia obsoleta ou desatualizada (hardware e software)	5,0%
17	O sistema está hospedado em sala segura ou sala cofre	10,0%
18	O sistema ou a infraestrutura que o suporta estão cobertos por processo de gestão de patches de segurança	8,0%
19	São realizados testes de invasão ou auditorias de segurança no sistema ou na infraestrutura que o sustenta	10,0%
20	O sistema é alvo de frequentes ataques	8,0%
21	O sistema possui controles para a proteção dos dados e do código (criptografia, backup, controle de acesso, trilhas de auditoria etc.)	16,0%
22	O sistema e a infraestrutura que o suporta estão incluídos em processo de gestão de ativos de TI - ITAM (*IT Asset Management*)	5,0%

É importante ressaltar que os tipos de impacto e vulnerabilidade dispostos nas tabelas devem ser considerados apenas para fins desta avaliação de criticidade de sistemas.

Considerando a avaliação dos impactos e vulnerabilidades, e as pontuações obtidas pela multiplicação entre o valor das respostas e o respectivo peso, aplica-se a seguinte fórmula:

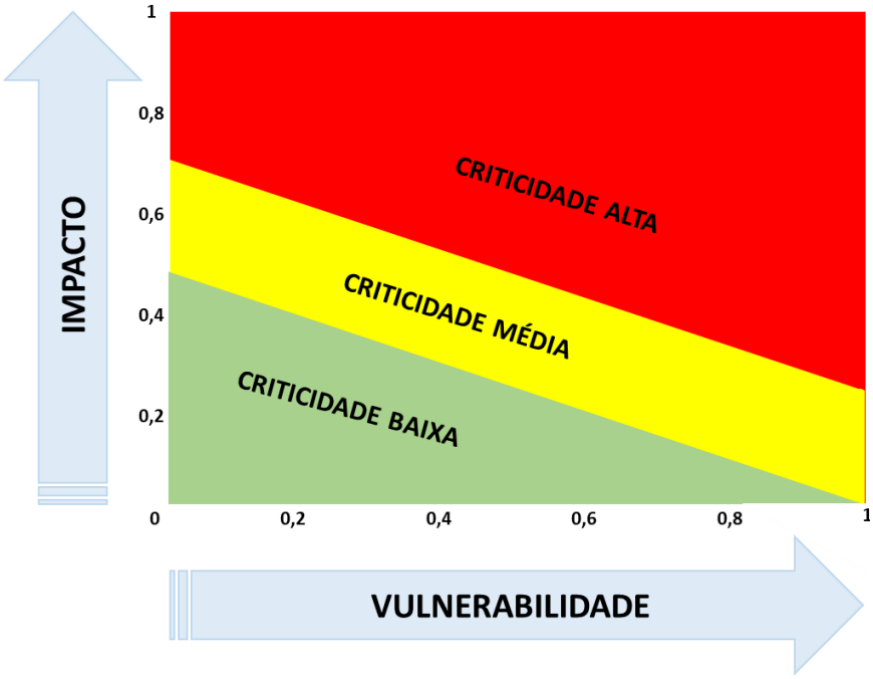
Tabela 9: NOTAS DE IMPACTO, VULNERABILIDADES E CRITICIDADE

Nota de Impacto (I)	I = Soma (pontuação de cada parâmetro de impacto x peso do parâmetro) Nota máxima = 1,00
Nota de Vulnerabilidade (V)	V = Soma (pontuação de cada parâmetro de vulnerabilidade x peso do parâmetro) Nota máxima = 1,00
Nota de Criticidade (NC)	NC = (2 x I) + V

Destaque-se que, para efeito de cálculo da nota de criticidade dos sistemas, a nota final da dimensão impacto para cada sistema foi multiplicada por dois, de forma a considerar a importância dos parâmetros nela agrupados e com potencial de afetar diretamente as estratégias e necessidades das organizações que os utilizam.

Conforme as notas obtidas, os sistemas foram classificados em três faixas de criticidade: alta, média e baixa. O resultado da nota de criticidade dos sistemas, classificados de acordo com impacto e a vulnerabilidade de cada um, podem ser dispostos graficamente tal como indicado na figura a seguir:

Figura 7: FAIXAS DE CRITICIDADE - VULNERABILIDADE x IMPACTO



A definição das faixas utilizou as seguintes premissas:

a) Um sistema com nota de impacto maior que 0,7 (de um total possível de 1), mesmo que não apresente vulnerabilidades conhecidas, deve ser objeto de um olhar prioritário e será considerado de alta criticidade (sistema crítico);

b) Um sistema com nota de impacto entre 0,5 e 0,7 (de um total possível de 1), mesmo que não apresente vulnerabilidades conhecidas, será considerado, no mínimo, como de média criticidade; e

c) Considerando-se que a criticidade é calculada como o dobro da nota impacto somado à nota de vulnerabilidade, as regiões de criticidade alta, média e baixa são separadas por retas de criticidade constante. Dessa

forma, a reta que separa as regiões de alta e média criticidade se caracteriza pela criticidade igual a 1,4 (num extremo, tem-se impacto de 0,7 e vulnerabilidade nula; no outro extremo, o impacto é de 0,2 e a vulnerabilidade é máxima). Já a reta que separa as regiões de média e baixa criticidade se caracteriza pela criticidade igual a 1 (num extremo, tem-se impacto de 0,5 e vulnerabilidade nula; no outro, o impacto é nulo e a vulnerabilidade, máxima).

Com a finalidade de facilitar a avaliação de criticidade dos sistemas relevantes, a SGD disponibiliza a título de sugestão para aqueles órgãos que não possuam uma metodologia própria, uma ferramenta em formato de planilha estruturada onde deverá ser respondido um diagnóstico com perguntas sobre as vulnerabilidades e os possíveis impactos no sistema caso haja um comprometimento.

Detalhes sobre o uso e funcionalidades da ferramenta podem ser observados no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/manual_ferramenta_framework.pdf

ANEXO II – NORMATIVOS DO GSI

GSI			
INSTRUÇÃO NORMATIVA	Instrução Normativa GSI Nº 1 - 27 de maio de 2020.	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215
	Instrução Normativa GSI Nº 2 - 24 de julho de 2020.	Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700
	Instrução Normativa GSI Nº 2 - 5 de fevereiro de 2013	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/02/2013&jornal=1&pagina=5&totalArquivos=120
	Instrução Normativa GSI Nº 3 - 28 de maio de 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172
	Instrução Normativa GSI Nº 3 - 6 de março de 2013	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=14/03/2013
	Instrução Normativa GSI Nº 4 - 26 de março de 2020	Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468
	Instrução Normativa GSI Nº 5 - 31 de agosto de 2021	Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.	https://in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684
	Instrução Normativa GSI Nº 6 - 23 de dezembro de 2021	Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-6-de-23-de-dezembro-de-2021-370081858

GSI			
NORMA COMPLEMENTAR	NC nº 05 /IN01/DSIC/GSIPR, e seu anexo	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/08/2009&jornal=1&pagina=8&totalArquivos=108
	NC nº 08 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&jornal=1&pagina=1&totalArquivos=144
	NC nº 09 /IN01/DSIC/GSIPR	**(Revisão 02)** Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=16/07/2014&jornal=1&pagina=4&totalArquivos=84
	NC nº 12 /IN01/DSIC/GSIPR	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/02/2012&jornal=1&pagina=3&totalArquivos=264
	NC nº 17 /IN01/DSIC/GSIPR	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/04/2013&jornal=1&pagina=5&totalArquivos=160
	NC nº 18 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/04/2013&jornal=1&pagina=6&totalArquivos=160
	NC nº 20 /IN01/DSIC/GSIPR	(Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=15/12/2014
	NC nº 21 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224
	NC nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas. (Publicada no DOU Nº 123, de 28 de junho de 2013 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/06/2013&jornal=1&pagina=5&totalArquivos=144

ANEXO III – TABELA DE CONTROLE e MEDIDAS DE ESTRUTURAÇÃO BÁSICA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
0.1	------	O órgão nomeou um Gestor de Tecnologia da Informação e Comunicação?	O Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.	Portaria nº 778, de 4 de abril de 2019
0.2	------	O órgão nomeou um Gestor de Segurança da Informação?	O Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação.	Art. 15, inciso I da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.3	------	O órgão nomeou um Responsável pela Unidade de Controle Interno?	O Responsável pela Unidade de Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.	Instrução Normativa CGU nº 3, de 9 de junho de 2017

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
0.4	------	O órgão instituiu um Comitê de Segurança da Informação?	Instituir um Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação.	Art. 15, inciso II da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.5	------	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Instituir e implementar Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República.	Art. 15, inciso IV da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.6	------	O órgão elaborou uma Política de Segurança da Informação - POSIN?	É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação - POSIN, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.	Art. 9º da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.7	GOVERNAR-P	O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais?	O Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os	Art. 5º, inciso VIII e Art. 41 da Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
			gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.	

ANEXO IV – TABELA DE CONTROLES e MEDIDAS DE CIBERSEGURANÇA

CIBERSEGURANÇA CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
1.1	1.1	IDENTIFICAR	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos institucionais com potencial para armazenar ou processar dado. Certificar de que o inventário registrará o endereço de rede (se estático), endereço de hardware, nome da máquina, etc. Deverá incluir ativos conectados à infraestrutura física, virtual, e remota e aqueles dentro de ambientes de nuvem. Necessário incluir também ativos mesmo que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 3/2021 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/.DSIC/GSIPR	1, 2, 3
1.2	1.4	IDENTIFICAR	O órgão usa o Dynamic Host Configuration Protocol DHCP para Atualizar o Inventários de Ativos?	Utilizar o registro (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores DHCP ou utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.3	1.3	DETECTAR	O órgão usa uma ferramenta de descoberta ativa?	Identificar ativos conectados à rede institucional através de uma ferramenta de descoberta ativa. Configurar para que essa descoberta seja executada diariamente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.4	1.5	DETECTAR	O órgão usa ferramenta de Descoberta Passiva?	Utilizar uma ferramenta de descoberta passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	3
1.5	1.2	RESPONDER	O órgão endereça ativos não autorizados?	Assegurar que exista um processo semanal para lidar com ativos não autorizados. Optar por remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
2.1	2.1	IDENTIFICAR	O órgão estabelece e mantém um inventário de software?	Estabelecer e manter um inventário detalhado de todos os softwares licenciados instalados em ativos. Revisar e atualizar o inventário de software semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 3/2021	1, 2, 3
2.2	2.2	IDENTIFICAR	O órgão assegura que o software autorizado seja atualmente suportado?	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de softwares autorizados. Softwares não suportados devem ser indicados no sistema de inventário. Revisar o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
2.3	2.5	PROTEGER	O órgão possui lista de permissões de Software autorizado?	Utilizar controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado. Reavaliar semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
2.4	2.6	PROTEGER	O órgão possuí lista de permissões de bibliotecas autorizadas?	Utilizar controles técnicos para garantir que apenas bibliotecas autorizadas (tais como *.dll, *.ocx, *.so, etc) tenham permissão para serem carregadas nos processos em execução. Impedir que bibliotecas não autorizadas sejam carregadas nos processos. Reavaliar semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2,3
2.5	2.7	PROTEGER	O órgão possuí lista de permissões de Scripts autorizados?	Utilize controles técnicos como assinaturas digitais e controle de versão para garantir que apenas scripts autorizados e assinados digitalmente (tais como *.ps1, *.py, macros etc.) tenham permissão para serem executados. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3
2.6	2.4	DETECTAR	O órgão utiliza ferramentas automatizadas de inventário de software?	Utilizar ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3

CIBERSEGURANÇA CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
2.7	2.3	RESPONDER	O órgão endereça o software não autorizado?	Assegurar que o software não autorizado seja retirado de uso em ativos institucionais ou receba uma exceção documentada. Revisar mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.1	3.1	IDENTIFICAR	O órgão estabelece e mantém um processo de gestão de dados?	Estabelecer e manter um processo de gestão de dados. No processo, tratar a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a organização. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.2	3.2	IDENTIFICAR	O órgão estabelece e mantém um inventário de dados?	Estabelecer e manter um inventário de dados, com base no processo de gestão de dados do órgão. No mínimo inventariar os dados sensíveis. Reavaliar e atualizar o inventário anualmente.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37 Art. 46 Art. 47, Art. 49 Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.3	3.7	IDENTIFICAR	O órgão estabelece e mantém um esquema de classificação de dados?	Estabelecer e manter um esquema geral de classificação de dados para o órgão, podendo ser “Sensíveis”, “Confidencial” e “Público. Revisar e atualizar o esquema de classificação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.	Art. 6º, inciso VII Art. 14, Art. 37, Art. 46, Art. 47, Art. 49 Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
3.4	3.8	IDENTIFICAR	O órgão documenta os Fluxos de Dados?	Documentar o fluxo de dados, contendo fluxos de dados do provedor de serviços, devendo ser baseada no processo de gestão de dados do órgão. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37 Art. 46 Art. 47, Art. 49 Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.5	3.3	PROTEGER	O órgão configura listas de controle de acessos a dados?	Aplicar listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, banco de dados e aplicações locais e remotos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.6	3.4	PROTEGER	O órgão aplica retenção de dados?	Reter os dados de acordo com o processo de gestão de dados da organização. A retenção deve incluir prazos mínimos e máximos.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37, Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.7	3.5	PROTEGER	O órgão descarta dados com segurança?	Descartar os dados com segurança, conforme processo de gestão de dados da organização. Certificar que o processo e método de descarte sejam compatíveis com a sensibilidade dos dados.	Art. 6º, inciso VII Art, 16, Art. 37, Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.8	3.6	PROTEGER	O órgão criptografa dados em dispositivos de usuário final?	Criptografar os dados em dispositivos de usuário final que contenham dados sensíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.9	3.9	PROTEGER	O órgão criptografa dados em mídia removível?	Criptografar os dados em removível.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.10	3.10	PROTEGER	O órgão criptografa dados sensíveis em trânsito?	Criptografar dados sensíveis em trânsito. Exemplos: Transport Layer Security (TLS) e Open Secure Shell (Open SSH)	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.11	3.11	PROTEGER	O órgão criptografa dados sensíveis em repouso?	Criptografar dados sensíveis em repouso em servidores, aplicações e banco de dados que contenham dados sensíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.12	3.12	PROTEGER	O órgão segmenta o processamento e o armazenamento de dados com base na sensibilidade?	Segmentar o processamento e armazenamento de dados com base na sensibilidade dos dados. Não processar dados sensíveis em ativos institucionais destinados a dados de menor sensibilidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.13	3.13	PROTEGER	O órgão implanta uma solução de prevenção contra perda de dados?	Implementar uma ferramenta automatizada, de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.14	3.14	DETECTAR	O órgão registra o acesso a dados sensíveis?	Registrar o acesso a dados sensíveis, incluindo modificação e descarte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
4.1	4.1	PROTEGER	O órgão estabelece e mantém um processo de configuração segura?	Estabelecer e manter um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	1, 2, 3
4.2	4.2	PROTEGER	O órgão estabelece e mantém um processo de configuração segura para a Infraestrutura de Rede?	Estabelecer e manter um processo de configuração segura para dispositivos de rede. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.3	4.3	PROTEGER	O órgão configura o bloqueio automático de sessão nos ativos?	Configurar o bloqueio automático de sessão nos ativos após um período definido de inatividade. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1,2,3
4.4	4.4	PROTEGER	O órgão implementa e gerencia um firewall nos servidores?	Implementar e gerenciar um firewall nos servidores, onde houver suporte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	1, 2, 3
4.5	4.5	PROTEGER	O órgão implementa e gerencia um firewall nos dispositivos de usuário final?	Implementar e gerenciar um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.6	4.6	PROTEGER	O órgão gerencia com segurança os ativos coorporativos e softwares?	Gerenciar com segurança os ativos e software. Exemplos de implementações incluem gestão de configuração por meio de *version controlled-infrastructure-as-code* e acesso a interfaces administrativas por meio de protocolos de rede seguros.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
4.7	4.7	PROTEGER	O órgão gerencia contas padrão nos ativos coorporativos e software?	Gerenciar contas padrão nos ativos e software, como root, administrador e outras contas de fornecedores pré-configuradas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.8	4.8	PROTEGER	O órgão desinstala ou desativa serviços desnecessários nos ativos e software?	Desinstalar ou desativar serviços desnecessários nos ativos e software, como serviço de compartilhamento de arquivo não utilizado, módulo de aplicação web ou função de serviço.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.9	4.9	PROTEGER	O órgão configura servidores DNS confiáveis nos ativos?	Implementar configuração de ativos para usar servidores DNS controlados pelo órgão e/ou servidores DNS confiáveis acessíveis externamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.10	4.11	PROTEGER	O órgão impõe a capacidade de limpeza remota nos dispositivos portáteis do usuário final?	Limpar remotamente os dados institucionais de dispositivos portáteis de usuário final de propriedade da organização quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais no órgão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.11	4.12	PROTEGER	O órgão separa os Espaços de Trabalho nos dispositivos móveis?	Certificar de que a separação de espaços de trabalho seja usada nos dispositivos móveis de usuário final, ou seja, separar aplicações e dados institucionais de aplicações e dados pessoais nos dispositivos, onde houver suporte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	3
4.12	4.10	RESPONDER	O órgão impõe o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final?	Impor bloqueio automático de dispositivos quando houver um número pré-definido de tentativas de autenticação com falha,	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2,3

CIBERSEGURANÇA CONTROLE 5: GESTÃO DE CONTAS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
5.1	5.1	IDENTIFICAR	O órgão estabelece e mantém um inventário de contas?	Estabelecer e manter um inventário de todas as contas gerenciadas na organização. O inventário deve incluir contas de usuário e administrador. Validar se todas as contas ativas estão autorizadas, trimestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
5.2	5.5	IDENTIFICAR	O órgão estabelece e mantém um inventário de contas de serviço?	Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter o departamento proprietário, data de revisão e propósito. Realizar análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	2, 3
5.3	5.2	PROTEGER	O órgão usa senhas exclusivas?	Usar senhas exclusivas para todos os ativos institucionais. Contas que usam MFA (Autenticação multifator) no mínimo senhas de 8 caracteres e uma senha de 14 caracteres para contas que não usam o MFA.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013	1, 2, 3
5.4	5.4	PROTEGER	O órgão restringe privilégios de administrador a contas de administrador dedicadas?	Restringir os privilégios de administrador a contas de administrador dedicados nos ativos institucionais. Realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	1, 2, 3
5.5	5.6	PROTEGER	O órgão centraliza a gestão de contas?	Centralizar a gestão de contas por meio de serviço de diretório ou de identidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	2, 3
5.6	5.3	RESPONDER	O órgão desabilita contas inativas?	Excluir ou desabilitar quaisquer contas inativas após um período de 45 dias de inatividade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013	1,2,3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.1	6.6	IDENTIFICAR	O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?	Estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revisar e atualizar o inventário anualmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
6.2	6.1	PROTEGER	O órgão estabelece um Processo de Concessão de Acesso?	Estabelecer e seguir um processo, de preferência automatizado, para conceder acesso aos ativos institucionais mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.3	6.2	PROTEGER	O órgão estabelece um Processo de Revogação de Acesso?	Estabelecer e seguir um processo, de preferência automatizado, para revogar o acesso aos ativos institucionais, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.4	6.3	PROTEGER	O órgão exige MFA para aplicações expostas externamente?	Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.5	6.4	PROTEGER	O órgão exige MFA para acesso remoto à rede?	Exigir MFA para acesso remoto à rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.6	6.5	PROTEGER	O órgão exige MFA para acesso administrativo?	Exigir MFA para todas as contas de acesso administrativo, em todos os ativos institucionais, sejam gerenciados no site local ou por meio de um provedor terceirizado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.7	6.7	PROTEGER	O órgão centraliza o controle de acesso?	Centralizar o controle de acesso para todos os ativos institucionais por meio de um serviço de diretório ou provedor de SSO	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013 IN nº 5/2021 NC 12 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
6.8	6.8	PROTEGER	O órgão define e mantém o controle de acesso baseado em funções?	Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas. Realizar análises de controle de acesso de ativos institucionais para validar se todos os privilégios estão autorizados, em uma programação recorrente, uma vez por ano ou com maior frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 12 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	3

CIBERSEGURANÇA CONTROLE 7: GESTÃO CONTÍNUA DE VULNERABILIDADES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
7.1	7.5	IDENTIFICAR	O órgão realiza varreduras automatizadas de vulnerabilidade em ativos institucionais internos?	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais internos trimestralmente ou com mais frequência. Realizar varreduras autenticadas e não autenticadas, usando uma ferramenta compatível com o SCAP(Security Content Automation Protocol).	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
7.2	7.6	IDENTIFICAR	O órgão realiza varreduras automatizadas de vulnerabilidade em ativos institucionais expostos externamente?	Executar varreduras de vulnerabilidade automatizadas de ativos institucionais expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Executar varreduras mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
7.3	7.1	PROTEGER	O órgão estabelece e mantém um processo de gestão de vulnerabilidade?	Estabelecer e manter um processo de gestão de vulnerabilidade documentado para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
7.4	7.3	PROTEGER	O órgão executa a gestão automatizada de patches do sistema operacional?	Realizar atualizações do sistema operacional em ativos institucionais por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
7.5	7.4	PROTEGER	O órgão executa a gestão automatizada de patches de aplicações?	Realizar atualizações de aplicações em ativos institucionais por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
7.6	7.2	RESPONDER	O órgão estabelece e mantém um processo de remediação?	Estabelecer e manter uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
7.7	7.7	RESPONDER	O órgão corrige vulnerabilidades detectadas?	Corrigir as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou com mais frequentemente, com base no processo de correção.	Art. 6º, inciso VII Art. 46, Art. 47,	------	2,3

CIBERSEGURANÇA CONTROLE 7: GESTÃO CONTÍNUA DE VULNERABILIDADES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
8.1	8.1	PROTEGER	O órgão estabelece e mantém um processo de gestão de log de auditoria?	Estabelecer e manter um processo de gestão de log de auditoria que defina os requisitos de log da organização. Tratar da coleta, revisão e retenção de logs de auditoria para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1, 2, 3
8.2	8.3	PROTEGER	O órgão garante o armazenamento adequado do registro de auditoria?	Certificar de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da organização	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1,2,3
8.3	8.4	PROTEGER	O órgão padroniza a sincronização de tempo?	Padronizar a sincronização de tempo. Configurar pelo menos duas fontes de tempo sincronizadas nos ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2,3
8.4	8.10	PROTEGER	O órgão retém os logs de auditoria?	Reter os logs de auditoria em ativos institucionais por no mínimo 90 dias.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.5	8.2	DETECTAR	O órgão coleta logs de auditoria?	Coletar logs de auditoria. Certificar de que o log, de acordo com o processo de gestão de log de auditoria da organização, tenha sido habilitado em todos os ativos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
8.6	8.5	DETECTAR	O órgão coleta logs de auditoria detalhados?	Configurar o log de auditoria detalhado para ativos institucionais contendo dados sensíveis. Incluir a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.7	8.6	DETECTAR	O órgão coleta logs de auditoria de consulta DNS?	Habilitar o registro de log de consulta do servidor DNS (Domain Name System) para detectar pesquisas de nomes de host para domínios maliciosos conhecidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.8	8.7	DETECTAR	O órgão coleta logs de auditoria de requisição de URL?	Coletar logs de auditoria de requisição de URL em ativos institucionais, quando apropriado e suportado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.9	8.8	DETECTAR	O órgão coleta logs de auditoria de linha de comando?	Habilitar o log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.10	8.9	DETECTAR	O órgão centraliza os logs de auditoria?	Centralizar a coleta e retenção de logs de auditoria nos ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.11	8.11	DETECTAR	O órgão conduz revisões de log de auditoria?	Realizar análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realizar revisões semanalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.12	8.12	DETECTAR	O órgão coleta logs do provedor de serviços?	Coletar logs do provedor de serviços. Exemplos de implementações incluem coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.	Art. 6º, inciso VII Art. 46, Art. 47,	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 9: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
9.1	9.1	PROTEGER	O órgão garante o uso apenas de navegadores e clientes de e-mail suportados plenamente?	Certificar de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na organização, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	1,2,3
9.2	9.2	PROTEGER	O órgão usa serviços de filtragem de DNS?	Usar os serviços de filtragem de DNS em todos os ativos institucionais para bloquear o acesso a domínios mal-intencionados conhecidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	1, 2, 3
9.3	9.3	PROTEGER	O órgão mantém e impõe filtros de URL baseados em rede?	Impor e atualizar filtros de URL baseados em rede para limitar um ativo institucional de se conectar a sites potencialmente maliciosos ou não aprovados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2, 3
9.4	9.4	PROTEGER	O órgão restringe extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas?	Restringir, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2, 3
9.5	9.5	PROTEGER	O órgão implementa o DMARC?	Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM)	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2,3
9.6	9.6	PROTEGER	O órgão bloqueia tipos de arquivo desnecessários?	Bloquear tipos de arquivo desnecessários que tentem entrar no gateway de e-mail do órgão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2,3
9.7	9.7	PROTEGER	O órgão implanta e mantém proteções antimalware de servidor de e-mail?	Implantar e manter proteção antimalware de servidores de e-mail, como varredura de anexos e/ou sandbox.	Art. 6º, inciso VII Art. 46, Art. 47,	IN nº 1/2020	3

CIBERSEGURANÇA CONTROLE 9: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 10: DEFESAS CONTRA MALWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
10.1	10.1	PROTEGER	O órgão instala e mantém um software antimalware?	Instalar e manter um software anti-malware em todos os ativos cibernéticos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1, 2, 3
10.2	10.2	PROTEGER	O órgão configura atualizações automáticas de assinatura antimalware?	Realizar a configuração de atualizações automáticas para as assinaturas anti-malware em todos os ativos cibernéticos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
10.3	10.3	PROTEGER	O órgão desabilita a execução e reprodução automática para mídias removíveis?	Configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1,2,3
10.4	10.5	PROTEGER	O órgão habilita funções antiexploração?	Habilitar funcionalidades "anti-exploits" tais como Data Execution Prevention (DEP) ou Address Space Layout Randomization (ASLR) que estejam disponíveis no sistema operacional, ou implantar ferramentas apropriadas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2,3
10.5	10.6	PROTEGER	O órgão gerencia o software antimalware de maneira centralizada?	Utilizar software anti-malware gerenciado centralmente para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
10.6	10.4	DETECTAR	O órgão configura a varredura antimalware automática de mídia removível?	Configure o software anti-malware para verificar automaticamente a mídia removível.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 10: DEFESAS CONTRA MALWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
10.7	10.7	DETECTAR	O órgão utiliza software antimalware baseado em comportamento?	Utilizar software anti-malware que consiga monitorar e identificar comportamentos fora do comum dos equipamentos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2,3

CIBERSEGURANÇA CONTROLE 11: RECUPERAÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
11.1	11.3	PROTEGER	O órgão protege os dados de recuperação?	Garantir que os dados de recuperação sejam protegidos adequadamente por meio de segurança física ou criptografia quando são armazenados, bem como quando são movidos pela rede. Isso inclui backups remotos e serviços em nuvem. Devem ser estabelecidos controles que garantam que os dados de recuperação sejam equivalentes aos dados originais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021	1, 2, 3
11.2	11.1	RECUPERAR	O órgão estabelece e mantém um processo de recuperação de dados?	Estabelecer e manter um processo de recuperação de dados. Tal processo deve descrever em seu escopo as atividades de recuperação de dados, priorização da recuperação e a atividade de segurança dos dados de backup. Periodicamente, deve ser realizada uma revisão e/ou atualização deste processo, assim como em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 NC 09 /IN01/DSIC/GSIPR	1, 2, 3
11.3	11.2	RECUPERAR	O órgão executa backups automatizados?	Garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizadas automaticamente e de forma regular.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
11.4	11.4	RECUPERAR	O órgão estabelece e mantém uma instância isolada de dados de recuperação?	Criar e manter pelo menos uma instância isolada dos dados de recuperação. Alguns exemplos deste tipo de implementação são controle de versão de destinos de backup por meio de sistemas e serviços off-line (backup off-line, não acessível por meio de uma conexão de rede), em nuvem, ou em datacenter separado do site local.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
11.5	11.5	RECUPERAR	O órgão testa os dados de recuperação?	Realizar o teste de integridade dos dados na mídia de backup regularmente, executando um processo de restauração de dados para garantir que o backup esteja funcionando corretamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3

CIBERSEGURANÇA CONTROLE 12: GESTÃO DA INFRAESTRUTURA DE REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
12.1	12.4	IDENTIFICAR	O órgão elabora e mantém diagramas de arquitetura?	Elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deve ser realizada de forma periódica ou quando ocorrerem mudanças que possam impactar tais artefatos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.2	12.1	PROTEGER	O órgão garante que a infraestrutura de rede está atualizada?	Garantir que a infraestrutura de rede da organização esteja sempre atualizada. Deve ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
12.3	12.2	PROTEGER	O órgão garante níveis de segurança para a arquitetura de rede?	Garantir que a arquitetura de rede se mantenha segura. É interessante buscar implementar políticas de segurança como segmentação de rede, privilégio mínimo e níveis básicos de disponibilidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.4	12.3	PROTEGER	O órgão gerencia a infraestrutura de rede e segurança?	Implementar e gerenciar com segurança a infraestrutura de rede da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2,3
12.5	12.5	PROTEGER	O órgão centraliza a autenticação, autorização e auditoria de rede (AAA)?	Implementar a centralização de (AAA) de rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.6	12.6	PROTEGER	O órgão utiliza protocolos de comunicação e gestão de rede seguros?	Implementar protocolos de comunicação e rede seguros.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2,3

CIBERSEGURANÇA CONTROLE 12: GESTÃO DA INFRAESTRUTURA DE REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
12.7	12.7	PROTEGER	O órgão garante que os dispositivos remotos utilizem uma VPN e se conectem em uma infraestrutura AAA segura da organização?	Fazer com que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela organização antes de acessar os dispositivos e recursos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
12.8	12.8	PROTEGER	O órgão utiliza e mantém recursos cibernéticos dedicados para todo o trabalho administrativo?	Habilitar a coleta de Netflow e registros de log em cada um dos dispositivos existentes para a execução de tarefas administrativas, utilize e mantenha recursos cibernéticos dedicados, estes devem estar fisicamente ou logicamente separados e seguros. É importante que tais recursos sejam segmentados da rede primária da organização, e não deve ser permitido o acesso a rede externa da organização. fronteiras da rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3

CIBERSEGURANÇA CONTROLE 13: MONITORAMENTO E DEFESA DA REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
13.1	13.4	PROTEGER	O órgão realiza filtragem de tráfego entre os segmentos de rede?	Realize a filtragem de tráfego entre os segmentos de rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.2	13.5	PROTEGER	O órgão aplica o gerenciamento de controle de acesso em ativos remotos?	Aplique o gerenciamento de controle de acesso em ativos que se conectam remotamente a organização. Determine a quantidade de acesso aos recursos da organização utilizando softwares antimalware devidamente atualizados, processos de configuração segura de ativos e certifique-se que os sistemas operacionais e demais aplicações estejam sempre atualizados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2,3
13.3	13.7	PROTEGER	O órgão implanta soluções para prevenção de intrusão baseada em host?	Implante uma solução para prevenção de intrusão baseada em host e ativos institucionais, preferencialmente com suporte do fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.4	13.8	PROTEGER	O órgão implanta soluções para prevenção de intrusão de rede?	Implante uma solução para prevenção de intrusão baseada em rede, preferencialmente com suporte do fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.5	13.9	PROTEGER	O órgão implanta controle de acesso a nível de porta?	Implante o controle de acesso em nível de porta. Tal controle utiliza o protocolo 802.1x ou soluções semelhantes como certificados, também podem ser utilizadas ferramentas para autenticação de usuário e/ou dispositivo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.6	13.10	PROTEGER	O órgão realiza a filtragem de camada de aplicação?	Realize a filtragem de camada de aplicação. Exemplos de implementações são proxy de filtragem, firewall desta camada ou gateway.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 13: MONITORAMENTO E DEFESA DA REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
13.7	13.1	DETECTAR	O órgão centraliza alertas de eventos de segurança?	Centralize os alertas de eventos de segurança em ativos institucionais para que a organização consiga realizar a correlação e análise do log. Uma boa prática é o uso de um SIEM que inclua alertas de correlação de eventos definidos pelo fornecedor. Outra boa prática é a adoção de uma plataforma de análise de log configurada com aletas de correlação relevantes para a segurança cibernética.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.8	13.2	DETECTAR	O órgão implanta soluções de detecção e intrusão baseada em host?	Implante soluções para detecção de intrusão baseada em host em ativos institucionais	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.9	13.3	DETECTAR	O órgão implanta soluções de detecção e intrusão baseada em rede?	Implante soluções para detecção de intrusão de rede em ativos institucionais	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.10	13.6	DETECTAR	O órgão coleta logs de fluxo e tráfego de rede?	Realize a coleta dos logs de fluxo e tráfego de rede com o objetivo de checar e alertar sobre dispositivos de rede que estejam com comportamento que fujam do padrão. em sua necessidade de acesso como parte de suas responsabilidades.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.11	13.11	DETECTAR	O órgão ajusta limites de alertas de eventos de segurança?	Ajuste periodicamente os limites dos alertas de eventos de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
14.1	14.1	PROTEGER	O órgão implanta e mantém um programa de conscientização de segurança?	Criar programa de conscientização de segurança para que todos os membros da força de trabalho o realizem regularmente com o objetivo de garantir que eles entendam e exibam os conhecimentos e comportamentos necessários para ajudar a garantir a segurança da instituição. O programa de conscientização de segurança da instituição deve ser comunicado de maneira contínua e envolvente.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.2	14.2	PROTEGER	O órgão treina colaboradores para reconhecer ataques de engenharia social?	Treinar os colaborares sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes de telefone e chamadas realizadas por impostores.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.3	14.3	PROTEGER	O órgão treina os colaboradores nas melhores práticas de autenticação?	Treinar os colaboradores sobre a importância de habilitar utilizar as melhores práticas de autenticação segura como MFA (Multi-factor Authentication – Autenticação de múltiplos fatores), composição de senha e gestão de credenciais.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.4	14.4	PROTEGER	O órgão treina os colaboradores nas Melhores Práticas de Tratamento de Dados?	Treinar os membros da força de trabalho sobre como identificar e armazenar, transferir, arquivar e destruir informações sensíveis (incluindo dados pessoais) adequadamente. Isto também inclui o treinamento sobre práticas recomendadas de mesa e tela limpas, (não deixar senhas expostas nas mesas de trabalho e bloquear a tela da estação de trabalho ao se ausentar), apagar quadros físicos e virtuais após reuniões e armazenar dados e ativos com segurança.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.5	14.5	PROTEGER	O órgão treina os colaboradores sobre as causas da exposição não intencional de dados?	Treinar os membros da força de trabalho para estarem cientes das causas de exposições de dados não intencionais, como perder seus dispositivos móveis ou enviar e-mail para a pessoa errada devido ao preenchimento automático de e-mail.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
14.6	14.6	PROTEGER	O órgão treina os colaboradores sobre como Reconhecer e Relatar incidentes de Segurança?	Treinar os colaboradores para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de relatar tal incidente.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.7	14.7	PROTEGER	O órgão treina os colaboradores sobre como identificar e comunicar se os seus ativos institucionais estão desatualizados em relação a segurança?	Treine os colaboradores para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. É importante incluir nesse treinamento a etapa de notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas que estejam ocorrendo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1,2,3
14.8	14.8	PROTEGER	O órgão treina os colaboradores sobre os perigos de se conectar e transmitir dados institucionais em redes inseguras?	Treine os colaboradores sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a organização tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.9	14.9	PROTEGER	O órgão conduz treinamento de competências e conscientização de segurança para funções específicas?	Para colaboradores que atuem em funções específicas, realize o treinamento de conscientização de segurança e de competências específicas para estas funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP e treinamento avançado de conscientização de engenharia social para funções de níveis estratégico da organização	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 15: GESTÃO DE PROVEDOR DE SERVIÇOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
15.1	15.1	IDENTIFICAR	O órgão cria e gerencia o inventário de provedores de serviços?	Crie e gerencie o inventário de provedores de serviços. Este inventário deve listar todos os provedores de serviços da organização, incluir classificações, e conter contatos institucionais para cada provedor de serviço. Deve ser realizada uma revisão e/ou atualização deste inventário anualmente ou quando ocorrerem mudanças significativas do provedor que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	1, 2, 3
15.2	15.2	IDENTIFICAR	O órgão cria e gerencia uma política de gestão de provedores de serviços?	Crie e gerencie uma política de gestão de provedores de serviços. Faça com que tal política trate de classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores e provedores de serviço da organização. Deve ser realizada uma revisão e/ou alteração desta política periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	2, 3
15.3	15.3	IDENTIFICAR	O órgão classifica provedores de serviços?	Realize a classificação de provedores de serviços. Para que seja realizada a classificação podem ser levadas em consideração uma ou mais característica do provedor, como a sensibilidade dos dados e informações que este provedor opera/gerencia, volume destes dados e informações, regulamentações aplicáveis, requisitos de disponibilidade e classificação de risco. Deve ser realizada uma revisão e/ou alteração desta classificação periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização e forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021	2, 3
15.4	15.5	IDENTIFICAR	O órgão avalia provedores de serviços?	Realizar a avaliação de provedores de serviços da organização. O escopo da avaliação deve levar em consideração as diretrizes contidas na política de gestão de provedores de serviços além de classificações e relatórios de avaliação padronizados, questionários, e processos rigorosos aplicáveis. A avaliação de provedores de serviço deve ser realizada de forma periódica e na medida em que novos contratos estipulados ou renovados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 4/2020 IN nº 5/2021 NC 09 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 15: GESTÃO DE PROVEDOR DE SERVIÇOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
15.5	15.4	PROTEGER	O órgão garante que os contratos dos provedores de serviços contenham requisitos mínimos de segurança?	Fazer com que os contratos do provedor de serviços contenham requisitos de segurança, alguns exemplos destes requisitos de segurança são, requisitos mínimos de segurança do software, resposta a incidentes de segurança, criptografia e descarte de dados. Tais requisitos mínimos devem ser concisos com a política de gestão de provedores da organização. Deve ser realizada uma revisão dos contratos de provedores de forma periódica com o objetivo de atualizar e garantir que os requisitos de segurança estão sendo cumpridos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	2, 3
15.6	15.7	PROTEGER	O órgão encerra de forma segura o contrato com o provedor de serviços?	Realizar de forma segura o encerramento de contrato de provedores e prestadores de serviço. Algumas ações que possam ser utilizadas para realizar o encerramento de contratos ou desligamento de prestadores são, desativação de contas de usuário e serviço utilizadas durante o contrato, encerramento de fluxo de dados e descarte seguros de dados e informações corporativas em sistemas dos provedores de serviço.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	3
15.7	15.6	DETECTAR	O órgão monitora provedores de serviço?	Realizar a monitoração de provedores de acordo com a política de gestão dos provedores de serviços. Tal monitoração pode incluir a avaliação periódica do provedor, monitoração de artefatos entregues pelo provedor	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021	3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.1	16.1	PROTEGER	O órgão estabelece e mantém um processo de desenvolvimento de aplicações?	Estabelecer e manter um processo de desenvolvimento de aplicações seguro. Este processo deve tratar de itens como padrões de design seguro de aplicações (Security by Design), práticas de codificação seguras, treinamentos para desenvolvedores, gestão de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.2	16.2	PROTEGER	O órgão estabelece e mantém um processo para aceitar e endereçar vulnerabilidades de software?	Estabelecer e manter um processo de aceitação e tratamento de informações sobre vulnerabilidades de software, incluindo mecanismos para que entidades externas contatem o grupo de segurança da instituição. É importante que o processo inclua itens como: Política de tratamento de vulnerabilidades identificadas e relatadas, equipe ou profissional responsável por analisar os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e testes de correção. Como parte deste processo, é importante rastrear as vulnerabilidades, classificar a gravidade e atribuir métricas capazes de medir o tempo de identificação, análise e correção das vulnerabilidades. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.3	16.3	PROTEGER	O órgão executa análise de causa raiz em vulnerabilidades de segurança?	Executar a análise de causa raiz em vulnerabilidades de segurança. A análise da causa raiz é a tarefa capaz de avaliar os problemas subjacentes que criam vulnerabilidades no código da aplicação e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.4	16.4	PROTEGER	O órgão estabelece e gerencia um inventário de componentes de software de terceiros?	Estabelecer e gerenciar um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de “lista de materiais”, bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar a organização. Deve ser realizada uma revisão e/ou alteração deste inventário periodicamente, com o objetivo de identificar quaisquer mudanças ou atualização nesses componentes e validar a compatibilidade do mesmo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.5	16.5	PROTEGER	O órgão usa componentes de software de terceiros atualizados e confiáveis?	Utilizar apenas componentes de terceiros atualizados e confiáveis. Quando possível, escolher bibliotecas e estruturas pré-estabelecidas e comprovadas que forneçam a segurança adequada. É importante adquirir tais componentes de fornecedores e fontes confiáveis ou realizar a avaliação de vulnerabilidades do software antes de usar/adquirir.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 09 /IN01/DSIC/GSIPR	2,3
16.6	16.6	PROTEGER	O órgão estabelece e mantém um processo para a classificação de severidade de vulnerabilidades?	Estabelecer e manter um processo para a classificação de gravidade de vulnerabilidades capaz de facilitar a priorização na medida em que as vulnerabilidades descobertas são corrigidas. Esse processo deve incluir a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. A classificação de gravidade deve trazer uma forma sistemática de triagem de vulnerabilidades que venha a melhorar a gestão de riscos e ajuda a garantir que os bugs mais graves sejam priorizados. Revise o processo o e a classificação de vulnerabilidade periodicamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.7	16.7	PROTEGER	O órgão usa modelos de configurações de segurança padrão para infraestrutura de aplicações?	Utilizar modelos de configuração de segurança padrão (Segurança by Default) recomendados pela equipe de segurança em componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de Security as a Service (SaaS). Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.8	16.8	PROTEGER	O órgão separa sistemas de produção e não produção?	Manter ambientes separados para sistemas de produção e não produção.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.9	16.9	PROTEGER	O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?	Garantir que todos os responsáveis pelo desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento deve incluir princípios gerais de segurança e práticas padrão de segurança para aplicações. O treinamento deve ser realizado periodicamente, é interessante estabelecer uma cultura de segurança entre os desenvolvedores.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.10	16.10	PROTEGER	O órgão aplica princípios de design seguro em arquiteturas de aplicações?	Aplicar princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de “nunca confiar nas entradas do usuário”. Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.11	16.11	PROTEGER	O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?	Aproveitar módulos ou serviços controlados para componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria de logs. O uso de recursos para plataforma em funções críticas de segurança deve reduzir a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
				mecanismos para criar e manter logs de auditoria seguros.			
16.12	16.12	PROTEGER	O órgão implementa verificações de segurança em nível de código?	Utilizar ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo utilizadas na organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3
16.13	16.13	PROTEGER	O órgão realiza teste de invasão de aplicação?	Realizar testes de invasão em aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de codificação e de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente uma aplicação como um usuário autenticado e não autenticado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3
16.14	16.14	PROTEGER	O órgão realiza a modelagem de ameaças?	Realizar a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um desenho, antes que o código seja criado. É conduzido por profissionais especialmente treinados que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender todos os pontos fracos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.1	17.1	RESPONDER	O órgão designa os colaboradores para gerenciar o tratamento de incidentes?	Designar os responsáveis para gerenciar o processo de tratamento de incidentes da organização. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes, esta equipe pode formada por colaboradores internos, terceirizados ou pode contar com os dois tipos de colaborares. Casos em que a equipe for composta somente por funcionários terceirizados, a organização deve designar pelo menos um colaborador interno para supervisionar qualquer ação terceirizada.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2020 IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	1, 2, 3
17.2	17.2	RESPONDER	O órgão estabelece e mantém informações de contato para relatar incidentes de segurança?	Estabelecer e manter as informações de contato das pessoas que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos periodicamente para garantir que as informações estejam atualizadas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo	1, 2, 3
17.3	17.3	RESPONDER	O órgão estabelece e mantém um processo institucional para relatar incidentes?	Estabelecer e manter um processo institucional para a colaborares relatarem incidentes de segurança. O processo inclui cronograma de relatórios, pessoal responsável por para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. É importante certificar que o processo está publicamente disponível para todos os colaboradores da organização. Deve ser realizada uma revisão periódica deste processo ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	1, 2, 3
17.4	17.4	RESPONDER	O órgão estabelece e mantém um processo de resposta a incidente?	Estabelecer e manter um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.5	17.5	RESPONDER	O órgão atribui funções e responsabilidades?	Atribuir funções e responsabilidades chave para resposta a incidentes, incluindo equipe jurídica, TI, segurança da informação, instalações, relações s públicas, recursos humanos, equipe de resposta a incidentes, conforme aplicável. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.6	17.6	RESPONDER	O órgão define mecanismos de comunicação durante a resposta a incidente?	Determinar quais mecanismos primários e secundários serão usados para relatar um incidente e se comunicar durante um incidente de segurança. Os mecanismos podem incluir ligações, e-mails ou cartas. Lembre-se de que certos mecanismos, como e-mails, podem ser afetados durante um incidente de segurança. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.7	17.7	RECUPERAR	O órgão conduz exercícios de resposta a incidentes regularmente?	Planejar e conduzir exercícios e cenários rotineiros de resposta a incidentes para a equipe envolvida na resposta a incidentes, de forma a manter a conscientização e tranquilidade no caso de resposta a ameaças reais. Os exercícios devem testar os canais de comunicação, tomada de decisão e recursos técnicos da equipe de resposta a incidentes, contemplando a utilização das ferramentas e dados disponíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.8	17.8	RECUPERAR	O órgão realiza análises pós-incidente?	Realizar análises pós-incidente. As análises pós-incidente ajudam a prevenir a recorrência do incidente por meio da identificação de lições aprendidas e ações de acompanhamento.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.9	17.9	RECUPERAR	O órgão estabelece e mantém limites de incidentes de segurança?	Estabelecer e manter limites de incidentes de segurança, incluindo, no mínimo, a diferenciação entre um incidente e um evento. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, ameaça de segurança, violação de dados, incidente de privacidade etc. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2020 IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 18: TESTES DE INVASÃO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
18.1	18.1	IDENTIFICAR	O órgão elabora e mantém um programa de teste de invasão?	Estabelecer um programa para testes de invasão adequado ao tamanho, complexidade e maturidade da organização. O programa de teste de invasão deve levar em consideração o escopo do teste como rede, aplicação web, API, controles de instalações físicas e etc.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.2	18.2	IDENTIFICAR	O órgão realiza testes de invasão externos periódicos?	Conduzir testes de invasão e externos regularmente. A teste de invasão externo deve ser reconhecido pela organização e deve ser capaz de detectar informações exploráveis que possam impactar a segurança da organização. Tal teste deve ser realizado por profissionais qualificados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.3	18.5	IDENTIFICAR	O órgão realiza testes de invasão internos periódicos?	Realize testes de invasão internos periódicos com base nos requisitos do programa de testes de invasão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3
18.4	18.3	PROTEGER	O órgão corrige os resultados dos testes de invasão?	Corrigir as descobertas do teste de invasão com base na política da organização para o escopo e a priorização de correção de vulnerabilidades.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.5	18.4	PROTEGER	O órgão valida as medidas de segurança?	Validar as medidas de segurança após cada teste de invasão. Se necessário, modificar os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3

ANEXO V – TABELA DE CONTROLES e MEDIDAS DE PRIVACIDADE

PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
19.1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P1	1, 2, 3
19.2	IDENTIFICAR-P	O órgão mapeia os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P2	1, 2, 3
19.3	IDENTIFICAR-P	O órgão documenta as fases do tratamento em que o operador atua?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P2 NIST ID.IM-P4	1, 2, 3
19.4	IDENTIFICAR-P	O órgão mapeia os fluxos ou ações do tratamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P8	1, 2, 3
19.5	IDENTIFICAR-P	O órgão mapeia o escopo (abrangência ou área geográfica) dos tratamentos de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.6	IDENTIFICAR-P	O órgão documenta a natureza (fonte) dos dados pessoais tratados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.7	IDENTIFICAR-P	A organização registra as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis?	Art. 7º Art. 11 Art. 23 Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2) ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.8	IDENTIFICAR-P	O órgão inventaria as categorias dos dados pessoais e dados pessoais sensíveis objetos dos tratamentos realizados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P6	1, 2, 3
19.9	IDENTIFICAR-P	O órgão registra o tempo de retenção de dados pessoais tratados conforme a finalidade de cada processamento?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P4	1, 2, 3
19.10	IDENTIFICAR-P	O órgão inventaria as categorias dos titulares de dados pessoais utilizados no tratamento?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P3	1, 2, 3
19.11	IDENTIFICAR-P	O órgão registra os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?	Art. 26 Art. 27 Art. 37	ABNT NBR ISO/IEC 29151:2017 (item A.7.4) ABNT NBR ISO/IEC 27701:2019 (item 7.5.3 e 7.5.4)	NIST CM.AW-P4	1, 2, 3

PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
				ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)		
19.12	IDENTIFICAR-P	O órgão mapeia os ambientes (ex: interno, nuvem, terceiros, etc) em que os dados pessoais objetos dos tratamentos são processados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P7	1, 2, 3
19.13	IDENTIFICAR-P	O órgão registra as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados e a quem?	Capítulo V Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.5.3 e 7.5.4) ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.14	IDENTIFICAR-P	O órgão mapeia os contratos estabelecidos/firmados com terceiros operadores responsáveis pelos tratamentos de dados pessoais?	Art. 37 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 20: FINALIDADE E HIPÓTESES LEGAIS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
20.1	IDENTIFICAR-P	O órgão identifica as finalidades específicas antes da realização dos tratamentos de dados pessoais?	Art. 6º, I e II Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.1)	NIST ID.IM-P5	1, 2, 3
20.2	IDENTIFICAR-P	O órgão identifica as hipóteses de tratamento antes da realização dos processamentos de dados pessoais?	Art. 7º Art. 11	ABNT NBR ISO/IEC 27701:2019 (item 7.2.1)	N/A	1, 2, 3
20.3	IDENTIFICAR-P	A organização identifica as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis antes da realização do tratamento?	Art. 7º Art. 11 Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2)	N/A	1, 2, 3
20.4	CONTROLAR-P	O órgão prioritariamente realiza tratamento de dados pessoais apenas para o atendimento de finalidade específica, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?	Art. 23	ISO/IEC 29151:2017 (item A.4.1)	N/A	1, 2, 3
20.5	CONTROLAR-P	O órgão trata dados pessoais sensíveis para executar políticas públicas previstas apenas em leis e regulamentos?	Art. 11, inciso II, alíneas a, b	N/A	N/A	1, 2, 3
20.6	CONTROLAR-P	O órgão ao realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, restringe o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária?	Art. 11, inciso II, alínea f	N/A	N/A	1, 2, 3
20.7	CONTROLAR-P	O órgão adota mecanismos para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais?	Art. 13, § 1º	N/A	N/A	1, 2, 3
20.8	CONTROLAR-P	O órgão, ao realizar estudos em saúde pública, trata os dados pessoais exclusivamente dentro da instituição, mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, e estritamente para a finalidade de realização de estudos e pesquisas?	Art. 13	N/A	N/A	1, 2, 3
20.9	CONTROLAR-P	O órgão mantém processo contínuo de gerenciamento das hipóteses legais de tratamento, incluindo o desenvolvimento de capacidades para cumprimento de obrigações decorrentes da definição da hipótese legal de tratamento, tais como: gerenciamento do consentimento, elaboração de Avaliação de Legitimo Interesse, etc?	Art. 7° Art. 8° Art. 10 Art. 11 Art. 12 Art. 13	N/A	N/A	1, 2, 3

PRIVACIDADE CONTROLE 20: FINALIDADE E HIPÓTESES LEGAIS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
20.10	CONTROLAR-P	O órgão, ao realizar compartilhamento de dados pessoais, adota medidas que assegurem a compatibilidade do propósito geral da finalidade original informada ao titular?	Art. 6, inciso I	N/A	N/A	1, 2, 3
20.11	CONTROLAR-P	O órgão ao coletar cookies identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for caso, cumprimento de obrigações ou atribuições legais?	Art. 6º, inciso VI; Art. 7° Art. 9º Art. 11 Art. 18	ISO/IEC 29184 (item 5.3.15)	NIST CM.AW-P1	1, 2, 3
20.12	CONTROLAR-P	O órgão ao coletar cookies permite, no banner de segundo nível, a obtenção do consentimento específico de acordo com as categorias identificadas, observados o disposto na LGPD?	Art. 8º Art. 14 Art. 18	ISO/IEC 29184 (item 5.4.1) ISO/IEC 29151 (item A.3)	NIST CM.AW-P1 NIST CM.AW-P8 NIST CT.PO-P1	1, 2, 3
20.13	CONTROLAR-P	O órgão mantém o fornecimento do serviço quando os titulares de dados pessoais se recusam a fornecer o consentimento para cookies não necessários?	Art. 7º Art. 8º Art. 9º Art. 11	ISO/IEC 29151 (item A.3)	NIST CM.AW-P8 NIST CT.PO-P1	1, 2, 3
20.14	CONTROLAR-P	O tratamento de dados pessoais de crianças e adolescentes é realizado no seu melhor interesse com base em hipótese legal prevista pela LGPD e, no que couber, conforme preconizado pelo art. 14 da LGPD?	Art. 7º Art. 11 Art. 14 Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 21: GOVERNANÇA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
21.1	GOVERNAR-P	O órgão adota medidas para adequar seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos de privacidade e proteção de dados vigentes?	Art. 50 § 2º inciso I	ABNT NBR ISO/IEC 27701:2019 (item 5.2.1) ABNT NBR ISO/IEC 27701:2019 (item 5.4)	NIST GV.PO-P	1, 2, 3
21.2	GOVERNAR-P	O órgão já elaborou e divulgou o seu Programa Institucional de Privacidade de Dados, conforme estabelecido no art.50 da LGPD?	Art. 50, § 2º, inciso I	ABNT NBR ISO/IEC 27701:2019 (item 5)	NIST GV.PO-P2	1, 2, 3
21.3	GOVERNAR-P	As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas?	Art. 50	N/A	NIST GV.PO-P3 NIST GV.AT-P1 NIST GV.AT-P2 NIST GV.AT-P3 NIST GV.AT-P4	1, 2, 3
21.4	GOVERNAR-P	O órgão disponibiliza para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?	Art. 50	ISO/IEC 29151 (item A.11.1)	N/A	1, 2, 3
21.5	GOVERNAR-P	O órgão determina as responsabilidades e respectivos papéis para o tratamento de dados pessoais com o(s) controlador(es) conjunto(s) envolvido(s)?	Art. 50	ABNT NBR ISO/IEC 27701:2019 (item 7.2.7)	NIST GV.PO-P3	2, 3
21.6	GOVERNAR-P	O órgão divulga a seus colaboradores internos e externos as políticas e procedimentos operacionais relacionados à proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.1, f)	NIST GV.PO-P1 NIST GV.PO-P4	1, 2, 3
21.7	GOVERNAR-P	Os requisitos legais, regulatórios e contratuais relativos à privacidade são compreendidos e direcionados por meio regras de boas práticas e de governança publicadas pela instituição?	Art. 50	N/A	NIST GV.PO-P5	1, 2, 3
21.8	GOVERNAR-P	No âmbito das operações de tratamento de dados pessoais, existe uma tolerância ao risco organizacional definida, claramente expressa e informada às partes interessadas do órgão?	Art. 50	N/A	NIST GV.RM-P2 NIST GV.RM-P3	2, 3
21.9	GOVERNAR-P	Foram definidos indicadores que serão utilizados para medir os resultados e desempenho do órgão na implementação do Programa Institucional de Privacidade de Dados?	Art. 50	N/A	NIST GV.MT-P	2, 3

PRIVACIDADE CONTROLE 21: GOVERNANÇA

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
21.10	GOVERNAR-P	O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?	Art. 46	ABNT NBR ISOIEC 27701:2019 (item 6.9.6.1)	NIST PR.PO-P10	2, 3

PRIVACIDADE CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
22.1	GOVERNAR-P	A organização revisou e adequou a Política de Segurança da Informação ou instrumento similar à LGPD?	Art. 6º, inciso VII Art. 46 Art. 50 § 2º, inciso I, alíneas “a” e “d"	ABNT NBR ISO/IEC 27701:2019 (itens 5.3.2 e 6.2)	NIST PR.PO-P NIST GV.MT-P2	1, 2, 3
22.2	GOVERNAR-P	Há uma política vigente ou documento equivalente que dispõe sobre diretrizes de proteção de dados pessoais?	Art. 6º Art. 46 Art. 50, § 2º, inciso I, alíneas “a” e “d”	ABNT NBR ISO/IEC 29151:2017 (Item A.2) ABNT NBR ISO/IEC 27701:2019 (item 6.2)	NIST PR.PO-P	1, 2, 3
22.3	GOVERNAR-P	As políticas, processos e procedimentos de gerenciamento de risco de privacidade do tratamento de dados pessoais são identificados, estabelecidos, avaliados, gerenciados e acordados pelas partes interessadas organizacionais, e seu progresso medido e comunicado?	Art. 6, X Art. 38 Art. 46 Art. 50, § 2º, inciso I, alíneas 'a'; 'd'; 'f'	N/A	NIST ID.DE-P1 NIST GV.MT-P4	2, 3
22.4	GOVERNAR-P	Os instrumentos convocatórios (editais licitatórios) estão adequados à LGPD?	Art. 39 Art. 50	ISO/IEC 29151:2017 (Item 15.1.2)	NIST GV.PO-P5	1, 2, 3
22.5	GOVERNAR-P	O órgão fornece um processo para monitorar as leis e políticas de privacidade com o objetivo de identificar alterações que afetem o programa de proteção de dados pessoais?	Art. 50, § 2º, inciso I, alínea “h”	ISO/IEC 29151 (item A.13)	NIST GV.MT-P3	1, 2, 3
22.6	CONTROLAR-P	A instituição estabelece um processo formal para a concessão de direitos de acesso privilegiado para o processamento de dados pessoais?	Art. 6º, inciso VIII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.4)	NIST CT.PO-P1	1, 2, 3
22.7	CONTROLAR-P	O órgão estabelece procedimento ou metodologia para assegurar que os princípios da LGPD estão sendo respeitados desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?	Art. 6º Art. 46 § 2º Art. 47 Art. 49	ISO/IEC 29151:2017 (Item 14.2.10) ABNT NBR ISO/IEC 27701:2019 (item 7.4)	NIST GV.PO-P2 NIST CT.DM-P10	1, 2, 3
22.8	CONTROLAR-P	A instituição implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	Art. 6º, inciso I, II e V Art. 23, inciso I	ISO/IEC 29151:2017 (item A.8)	N/A	1, 2, 3
22.9	CONTROLAR-P	O órgão estabelece políticas, procedimentos e adota mecanismos documentados para o descarte de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.7.1, A.7.2)	NIST CT.PO-P2	2, 3

PRIVACIDADE CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
22.10	CONTROLAR-P	A organização adequou seu Plano de Resposta a Incidentes (ou documento similar) à LGPD de forma a tratar violações relativas à privacidade dos titulares de dados pessoais?	Art. 50, § 2º, inciso I, alínea "g"	ABNT NBR ISO/IEC 27701:2019 (item 6.13)	NIST PR.PO-P7	1, 2, 3
22.11	CONTROLAR-P	A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?	Art. 48 Art. 50, § 2º, inciso I, alínea "g"	ABNT NBR ISO/IEC 27701:2019 (6.13.1.5)	N/A	1, 2, 3
22.12	CONTROLAR-P	O órgão revisa periodicamente as políticas, processos, planos e procedimentos de proteção de dados pessoais?	Art. 50, § 2º, inciso I, alínea "h"	ISO/IEC 29151 (item 5.1.3)	NIST GV.MT-P2 NIST GV.MT-P3	2, 3

PRIVACIDADE CONTROLE 23: CONSCIENTIZAÇÃO E TREINAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
23.1	GOVERNAR-P	O órgão implementa e mantêm uma estratégia abrangente de treinamento e conscientização a fim de garantir que a força de trabalho compreenda sobre suas responsabilidades e procedimentos de proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.5 a)	GV.AT-P	1, 2, 3
23.2	GOVERNAR-P	O plano de desenvolvimento de pessoas do órgão contempla treinamento adequado sobre a temática de privacidade e de proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.5 a)	GV.AT-P	1, 2, 3
23.3	GOVERNAR-P	As ações de treinamento e conscientização realizadas pela instituição visam a manter os colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade da organização?	Art. 50	ISO/IEC 29151 (item A.11.5 c)	GV.AT-P	1, 2, 3
23.4	GOVERNAR-P	O órgão executa regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente) treinamento básico e direcionado de proteção de dados pessoais conforme as funções das pessoas envolvidas com o tratamento?	Art. 50	ISO/IEC 29151 (item A.11.5 c)	GV.AT-P	1, 2, 3

PRIVACIDADE CONTROLE 24: MINIMIZAÇÃO DE DADOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
24.1	CONTROLAR-P	O órgão avalia e classifica os dados pessoais a serem coletados em obrigatórios e opcionais a fim de priorizar somente a coleta dos dados obrigatórios para a prestação do serviço?	Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	2, 3
24.2	CONTROLAR-P	O órgão restringe ao máximo a coleta de dados de forma que seja suficiente para atender a finalidade específica do tratamento?	Art. 18, inciso IV	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	1, 2, 3
24.3	CONTROLAR-P	O órgão, ao realizar o tratamento de dados pessoais, aplica o princípio da minimização de dados para restringir a quantidades de dados pessoais ao estritamente necessário para atendimento da finalidade específica?	Art. 6º - III Art. 18, inciso IV	ISO/IEC 29151:2017 (Item A.5 e A.6) ABNT NBR ISO/IEC 27701:2019 (item 7.4.1)	NIST CT.DP-P	1, 2, 3
24.4	CONTROLAR-P	O órgão adota medidas para assegurar que as configurações de privacidade sejam aplicadas por padrão (Privacy by Default) nos serviços fornecidos?	Art. 6º - III Art. 46, § 2º	ABNT NBR ISO/IEC 27701:2019 (item 7.4)	N/A	2, 3
24.5	CONTROLAR-P	O órgão adota o princípio 'need-to-how', em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos colaboradores?	Art. 46	ISO/IEC 29151 (item A.6)	NIST CT.DP-P	2, 3
24.6	CONTROLAR-P	O órgão adota como padrão, sempre que possível, interações e transações que não envolvam a identificação dos titulares?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P1 NIST CT.DP-P2	3
24.7	CONTROLAR-P	O órgão adota mecanismos para limitar a vinculação dos dados pessoais coletados?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P1 NIST CT.DP-P2	3
24.8	CONTROLAR-P	As referências de atributos são substituídas por valores de atributos? Por exemplo, para o atributo "aniversário", um valor de atributo poderia ser "1/12/1980" e uma referência de atributo seria "nascido em dezembro".	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	N/A	NIST CT.DP-P5	3

PRIVACIDADE CONTROLE 24: MINIMIZAÇÃO DE DADOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
24.9	CONTROLAR-P	Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passam por um processo de anonimização?	Art. 6º, inciso VII Art. 12, § 3º Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (Item 12.1.5)	NIST CT.DP-P	2, 3
24.10	CONTROLAR-P	O órgão realiza revisão periódica dos dados pessoais tratados para que continuem a ser o mínimo necessários para cumprir com a finalidade?	Art. 6º, inciso I, II e III Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	3
24.11	CONTROLAR-P	O órgão determina e desidentifica os dados pessoais que necessitam ser anonimizados de acordo com o tratamento e exigências estabelecidas por leis aplicáveis?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	2, 3
24.12	CONTROLAR-P	Ao fornecer a base de informações para órgãos de pesquisa ou para realização de estudos em saúde pública, os dados pessoais são, sempre que possível, anonimizados ou pseudoanonimizados?	Art. 7º, inciso IV Art. 11, inciso II alínea c Art. 13	ISO/IEC 29151:2017 (item A.6)	NIST CT.DP-P	1, 2, 3
24.13	CONTROLAR-P	O órgão ao coletar cookies disponibiliza botão de fácil visualização, no banner de primeiro e de segundo nível, que permita rejeitar todos os cookies não-necessários?	Art. 6º, incisos III VI Art. 8º Art. 9º Art. 18	ISO/IEC 29184 (item 5.4.6) ABNT NBR ISO/IEC 27701:2019 (item 7.4.1) ISO/IEC 29151 (item A.5 e A.6)	CM.AW-P1 CM.AW-P2	1, 2, 3
24.14	CONTROLAR-P	O órgão ao coletar cookies desativa, no banner de primeiro nível, cookies baseados no consentimento por padrão (opt-in)?	Art. 6º, incisos III e VI Art. 8º Art. 9º Art. 18	ABNT NBR ISO/IEC 27701:2019 (item 7.4.1)	CM.AW-P1 CM.AW-P2	1, 2, 3
24.15	CONTROLAR-P	O órgão ao coletar cookies classifica os cookies em categorias no banner de segundo nível?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29184 (item 5.4.6) ISO/IEC 29151 (item A.5 e A.6)	CM.AW-P1 CM.AW-P2	1, 2, 3

PRIVACIDADE CONTROLE 25: GESTÃO DO TRATAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS			GRUPOS DE IMPLEMENTAÇÃO
			LGPD	ISO	NIST - PF	
25.1	CONTROLAR-P	O órgão configura os sistemas para registrar a data em que os dados pessoais são coletados, criados, atualizados, excluídos ou arquivados?	Art. 50	ISO/IEC 29151 (item A.7)	NIST CT.DM-P8	2, 3
25.2	CONTROLAR-P	O órgão limita a quantidade de processamento sobre os dados pessoais sob sua custódia?	Art. 6º, inciso III	ISO/IEC 29151 (item A.7)	NIST CT.DM-P	1, 2, 3
25.3	CONTROLAR-P	O órgão define e documenta os objetivos da minimização do tratamento sobre os dados pessoais sob sua custódia?	Art. 6º, inciso III	ABNT NBR ISO/IEC 27701:2019 (item 7.4.4)	NIST CT.DM-P	3
25.4	CONTROLAR-P	Os dados são mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?	Art. 25	N/A	NIST ID.DE-P4	1, 2, 3
25.5	CONTROLAR-P	Há procedimentos para garantir que quando há o término do tratamento de dados do titular no órgão, este segue as hipóteses previstas no artigo 15 da LGPD?	Art. 15	N/A		1, 2, 3
25.6	CONTROLAR-P	A instituição utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 8.3.3, A.7.1 "b" e A.7.2) ABNT NBR ISO/IEC 27701:2019 (itens 7.4.6, 7.4.8, 8.4.1 e 8.4.2)	NIST CT.PO-P2 NIST CT.DM-P4 NIST CT.DM-P5	2, 3
25.7	CONTROLAR-P	A organização avalia se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	Art. 6º, inciso I e III Art. 16	ABNT NBR ISO/IEC 27701:2019 (item 7.4.7) ISO/IEC 29151:2017 (item A.7.1 a)	N/A	1, 2, 3
25.8	CONTROLAR-P	O órgão implementa no serviço a detecção da expiração do período de retenção e aviso automático de que deve ser avaliada a possibilidade de exclusão dos dados pessoais após o cumprimento das finalidades?	Art. 6º Art. 15 Art. 16	ISO/IEC 29151 (item A.7.1)	NIST CT.DM-P	3
25.9	CONTROLAR-P	O órgão bloqueia e adota medidas de proteção para isentar de processamento adicional os dados pessoais quando os propósitos informados ao titular são atingidos, mas a retenção for exigida pelas leis aplicáveis?	Art. 6º Art. 15 Art. 16	ISO/IEC 29151 (item A.7.1)	NIST CT.DM-P	3

PRIVACIDADE CONTROLE 26: ACESSO E QUALIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
26.1	CONTROLAR-P	Há um canal de comunicação ativo, seguro e autenticado com um ponto de contato para receber e responder a reclamações e requisições do titular sobre o tratamento de dados pessoais?	Art. 41, § 2º, inciso I Art. 46	ISO/IEC 29151:2017 (Item A.10.3)	NIST CM.PO-P	1, 2, 3
26.2	CONTROLAR-P	O órgão adota meios para verificar a validade e exatidão das solicitações de correção realizadas por parte do titular de dados pessoais?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.8 e)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.3	CONTROLAR-P	O órgão fornece meios para que o titulares de dados pessoais possam solicitar as correções dos dados pessoais ou contestar a exatidão e integridade dos dados pessoais com direito a confirmação de recebimento da solicitação?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	1, 2, 3
26.4	CONTROLAR-P	O órgão fornece, na medida do possível, as respostas ao titular de dados pessoais de forma equivalente àquela em que a solicitação foi realizada?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.5	CONTROLAR-P	O órgão adota mecanismos de rastreamento para garantir que todas as petições e reclamações recebidas dos titulares de dados pessoais sejam analisadas e tratadas adequadamente em tempo hábil?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.3)	NIST CT.DM-P NIST CT.PO-P2	1, 2, 3
26.6	CONTROLAR-P	São utilizados padrões técnicos, principalmente os definidos pela ANPD, que facilitem o controle pelos titulares dos seus dados pessoais?	Art. 51	N/A	N/A	2, 3
26.7	CONTROLAR-P	O órgão implementa meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.8	CONTROLAR-P	O órgão confirma, na medida do possível, a exatidão, relevância e integridade dos dados pessoais na coleta?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.8)	NIST CT.DM-P NIST CT.PO-P2	3

PRIVACIDADE CONTROLE 26: ACESSO E QUALIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
26.9	CONTROLAR-P	A instituição implementa medidas que visam a garantir e maximizar a exatidão, qualidade e completude dos dados pessoais coletados?	Art. 6º, inciso V Art. 18, inciso III	ISO/IEC 29151:2017 (item A.8 g)	NIST CT.PO-P2 NIST CT.DM-P	1, 2, 3
26.10	CONTROLAR-P	O órgão revisa periodicamente e corrige, conforme necessário, os dados pessoais imprecisos ou desatualizados?	Art. 6º, inciso V Art. 18, inciso III	ISO/IEC 29151 (item A.8 f)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.11	COMUNICAR-P	O órgão fornece informações ao titular de dados pessoais sobre o andamento de suas solicitações?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.10.1 h)	N/A	2, 3
26.12	COMUNICAR-P	O órgão comunica qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados?	Art. 6º Art. 18 Art. 39	ISO/IEC 29151 (item A.10.2)	NIST CT.DM-P NIST CT.PO-P2 NIST CM.AW.P5	1, 2, 3

PRIVACIDADE CONTROLE 27: COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
27.1	IDENTIFICAR-P	O órgão identifica os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Art. 26 e 27	N/A	CM.AW-P4	1, 2, 3
27.2	IDENTIFICAR-P	O órgão identifica as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Art. 33 Art. 34 Art. 35 Art. 36	N/A	CM.AW-P4	1, 2, 3
27.3	CONTROLAR-P	O órgão, ao compartilhar dados pessoais, adota um processo de formalização e registro, identificando objeto e finalidade, base legal e duração do tratamento?	Art. 25 Art. 26 Art. 27 Art. 30	N/A	CT.PO-P2	1, 2, 3
27.4	CONTROLAR-P	O órgão solicita descrição formal das medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais?	Art. 25 Art. 26 Art. 27 Art. 30	N/A	CT.PO-P2	2, 3
27.5	CONTROLAR-P	O órgão observa o disposto pelo art. 33-36 da LGPD para a realização de transferência internacional de dados pessoais?	Art. 33 Art. 34 Art. 35 Art. 36	ABNT NBR ISO/IEC 29151:2017 (item A.13.2) ABNT NBR ISO/IEC 27701:2019 (item 7.5.1, 7.5.2, 8.5.1 e 8.5.2)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 28: SUPERVISÃO EM TERCEIROS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
28.1	CONTROLAR-P	O órgão estabelece as funções e responsabilidades do operador envolvido no tratamento de dados pessoais, principalmente a notificação em caso de violação de dados pessoais?	Art. 39	ISO/IEC 29151 (item A.11.3 c)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.2	CONTROLAR-P	São estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais controlados pelos órgãos?	Art. 39	ISO/IEC 29151:2017 (Item 13.2.5)	NIST GV.PO-P4 NIST GV.PO-P5	1, 2, 3
28.3	CONTROLAR-P	O órgão estabelece no contrato que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador?	Art. 23 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 8.2.2)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.4	CONTROLAR-P	O órgão determina por contrato o assunto e o prazo do serviço a ser prestado, a extensão, a forma e a finalidade do tratamento de dados pessoais pelo operador, bem como os tipos de dados pessoais processados?	Art. 39	ISO/IEC 29151 (item A.11.3 d)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.5	CONTROLAR-P	O órgão documenta no contrato de nível de serviço os requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender?	Art. 39	ISO/IEC 29151 (item A.11.3 a)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.6	CONTROLAR-P	O órgão adota meios para garantir que os sistemas do operador de dados pessoais tenham mecanismos de proteção de dados implementados?	Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.2.6)	NIST GV.PO-P4 NIST GV.AT-P4	3
28.7	CONTROLAR-P	O órgão instrui ao operador que implemente meios práticos para permitir que os titulares exerçam seu direito de gerenciamento dos dados pessoais?	Art. 6º, incisos IV e V Art. 8º § 5º Art. 9º § 2º Art. 18 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.3.4, 7.3.5, 7.3.6, 7.3.9 e 8.3)	NIST GV.PO-P4 NIST GV.AT-P4	2, 3
28.8	CONTROLAR-P	O órgão exige do operador o cumprimento de todas as cláusulas estipuladas em contrato sobre divulgação de dados pessoais, a menos que proibido por lei?	Art. 39	ISO/IEC 29151 (item A.7.3 e A.11.3 g) ABNT NBR ISO/IEC 27701:2019 (item 8.5.4 e 8.5.5)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.9	CONTROLAR-P	O órgão exige que o operador o informe sobre assuntos envolvendo o tratamento de dados pessoais para que o controlador esteja em conformidade com suas obrigações, principalmente em casos de solicitações juridicamente vinculativas para divulgação de dados pessoais, violação de dados pessoais, sobre alterações relevantes ao serviço?	Art. 39 Art. 44 Art. 45	ISO/IEC 29151 (item A.11.3 i) ABNT NBR ISO/IEC 27701:2019 (item 8.2.4, 8.2.5 e 8.5.4)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3

PRIVACIDADE CONTROLE 28: SUPERVISÃO EM TERCEIROS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
28.10	CONTROLAR-P	O órgão especifica as condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador?	Art. 15 Art. 16 Art. 39 Art. 46	ISO/IEC 29151 (item A.11.3 e) ABNT NBR ISO/IEC 27701:2019 (item 7.4.8 e 8.4.2)	NIST GV.PO-P NIST GV.AT-P4 NIST CT.PO-P2	3
28.11	CONTROLAR-P	O órgão especifica no contrato entre controlador e operador sobre o uso de subcontratados para processar dados pessoais?	Art. 39	ISO/IEC 29151 (item A.7.5) ABNT NBR ISO/IEC 27701:2019 (item 8.5.6, 8.5.7 e 8.5.8)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.12	CONTROLAR-P	O órgão monitora e inspeciona a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores?	Art. 39	ISO/IEC 29151 (item A.11.3 b)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.13	CONTROLAR-P	O órgão realizou revisão das cláusulas contratuais em vigência com os operadores terceiros para adequá-los à LGPD?	Art. 39	ISO/IEC 29151:2017 (Item 15.1.2, A.7.5 e A.11.3) ABNT NBR ISO/IEC 27701:2019 (item 7.2.6)	NIST GV.PO-P5 NIST GV.PO-P4 NIST GV.AT-P4	1, 2, 3

PRIVACIDADE CONTROLE 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
29.1	CONTROLAR-P	O órgão adota meios para apresentar as informações de tratamento de dados pessoais de forma clara para que possam ser compreendidas por uma pessoa que não esteja familiarizada com as tecnologias da informação, internet ou jargões jurídicos?	Art. 6º, inciso VI; Art. 8º, § 1º Art. 9º Art. 18, inciso I, VII e VIII	ISO/IEC 29151 (item A.9.1 e) ABNT NBR ISO/IEC 27701:2019 (item 7.3.3)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.2	CONTROLAR-P	O órgão adota meios para disponibilizar a política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1)	NIST CM.AW-P1 NIST CM.AW-P2	2, 3
29.3	CONTROLAR-P	O órgão adota algum mecanismo, sempre que possível, para comprovar que o titular de dados pessoais obteve acesso à política de privacidade fornecida?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1 i)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.4	CONTROLAR-P	O órgão revisa a política de privacidade, cookies e outras aplicáveis ao tratamento de dados pessoais, antes ou assim que possível, para refletir mudanças realizadas no tratamento?	Art. 6º, inciso VI; Art. 8º, § 1º Art. 9º Art. 18, inciso I, VII e VIII	ISO/IEC 29151 (item A.9.1 c)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.5	COMUNICAR-P	O órgão destaca na Política de Privacidade informações sobre os dados pessoais que a organização coleta e a(s) finalidade(s) do tratamento para a qual a coleta é realizada, hipóteses e bases legais?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.6	COMUNICAR-P	A identidade e as informações de contato do encarregado estão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?	Art. 41, § 1º	ABNT NBR ISO/IEC 27701:2019 (item 6.3.1)	NIST CM.PO-P1 NIST CM.PO-P2	1, 2, 3
29.7	COMUNICAR-P	O órgão fornece informações aos titulares sobre como é realizado o tratamento de dados pessoais, tais como o período de retenção dos dados pessoais coletados, entre outras ações de tratamento?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1 a) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.8	COMUNICAR-P	Os titulares de dados são informados quando há alterações na forma de tratamento dos dados pessoais?	Art. 6º, inciso VI; Art. 8º Art. 9º	ISO/IEC 29151:2017 (item A.9.1)	NIST CM.AW-P1 NIST CM.AW-P5	1, 2, 3
29.9	COMUNICAR-P	O órgão fornece orientações ao titular sobre a forma e meios utilizados de gerenciamento aos dados pessoais?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9)	NIST CM.AW-P1 NIST CM.AW-P2	2, 3

PRIVACIDADE CONTROLE 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
				ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)		
29.10	COMUNICAR-P	O órgão informa se a organização compartilha dados pessoais com entidades externas, os dados pessoais compartilhados e a finalidade para tal compartilhamento?	Art. 6º, inciso VI; Art. 8º **Art. 9º, inciso V** Art. 18	ISO/IEC 29151 (item A.9.1 a) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2 NIST CM.AW-P4	1, 2, 3
29.11	COMUNICAR-P	O órgão fornece informações sobre a proteção e descarte seguro dos dados pessoais coletados?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	**ISO/IEC 29151 (item A.9.1 a)** ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1	2, 3
29.12	COMUNICAR-P	O órgão fornece, quando solicitado por instituição competente, informações relativas a violações de privacidade dos titulares, juntamente com quaisquer ações associadas que o solicitante possa tomar para mitigar os riscos adicionais decorrentes da violação?	Art. 48	**ISO/IEC 29151 (item A.9.2 j)**	NIST CM.AW-P1	1, 2, 3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.1	GOVERNAR-P	O órgão observa o conteúdo mínimo a ser inserido no Relatório de Impacto à Proteção de Dados Pessoais - RIPD conforme o disposto no Art. 38, parágrafo único da LGPD?	Art. 5º XVII Art. 38	ABNT NBR ISO/IEC 29134:2017 (Item 5, 6 e 7 e Anexos A,B,C e D) ABNT NBR ISOIEC 27701:2019 (5.6.2, 5.6.3 e 7.2.5)	NIST ID.RA-P NIST CM.AW-P1	1, 2, 3
30.2	GOVERNAR-P	O órgão estabelece processo para avaliar o impacto na privacidade ao fornecer serviços que tratam dados pessoais?	Art. 4º, § 3º Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P NIST GV.MT-P	1, 2, 3
30.3	GOVERNAR-P	A organização avalia os riscos dos processos de tratamento de dados pessoais que foram identificados?	Art. 4º, § 3º Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29134:2017 (item 6.4.4)	NIST ID.RA-P	1, 2, 3
30.4	GOVERNAR-P	O órgão documenta os riscos de privacidade oriundos da avaliação de impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3
30.5	GOVERNAR-P	O órgão documenta as medidas de proteção de dados pessoais adotadas para mitigação do impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.6	GOVERNAR-P	O órgão realiza e documenta os resultados de uma avaliação de impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3
30.7	GOVERNAR-P	O órgão desenvolve, divulga (no que couber) e atualiza relatórios (por exemplo, relatórios sobre violações, investigações, auditorias), a fim de demonstrar responsabilidade e conformidade com leis e regulamentos de proteção de dados pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.6)	NIST ID.RA-P	3
30.8	CONTROLAR-P	O órgão monitora e audita regularmente as operações de tratamento de dados pessoais, especialmente aquelas envolvendo dados pessoais sensíveis, para garantir que estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 a)	NIST GV.MT-P	2, 3
30.9	CONTROLAR-P	Os controles de proteção de dados pessoais são monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com normas e regulamentos internos e externos, quando aplicável, a organização?	Art. 6º, incisos VII, VIII e X Art. 39 Art. 46 Art. 47 Art. 49 Art. 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 b)	NIST GV.PO-P NIST GV.MT-P NIST ID.DE-P5	3
30.10	CONTROLAR-P	O órgão implementa medidas apropriadas para monitorar e auditar periodicamente os controles de privacidade e a eficácia da política de privacidade interna (política de proteção de dados pessoais) da instituição?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4)	NIST GV.PO-P NIST GV.MT-P	3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.11	CONTROLAR-P	O órgão assegura que as auditorias sejam conduzidas por partes qualificadas e independentes (internas ou externas à organização)?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 c)	NIST GV.PO-P NIST GV.MT-P	3
30.12	CONTROLAR-P	O órgão produz um relatório anual detalhando as ações tomadas para conformidade e um resumo das ações pendentes?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.13.1 a)	NIST GV.PO-P NIST GV.MT-P	3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.1	PROTEGER-P	A organização adota medidas de segurança, técnicas e administrativas, testadas e avaliadas, aptas a proteger dados pessoais de acordo com os resultados de uma avaliação de riscos ou impacto de proteção de dados pessoais?	Art. 6º, inciso VII Art. 44 Art. 46 Art. 47 Art. 48, §1° inciso VI Art. 49	ISO/IEC 29151 (item A.12 “c” e “e”)	NIST PR. P	1, 2, 3
31.2	PROTEGER-P	O órgão submete os controles de privacidade e segurança da informação adotados a revisão e reavaliação periódicas resultantes da avaliação de impacto na privacidade?	Art. 46 Art. 47 Art. 49 Art. 50	ISO/IEC 29151 (item A.12 f)	NIST PR.PO-P NIST PR.AC-P NIST PR.DS-P NIST PR.MA-P NIST PR.PT-P	2, 3
31.3	PROTEGER-P	A organização implementa processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ABNT NBR ISO/IEC 27701:2019 (itens 6.6.2.1 e 6.6.2.2) ISO/IEC 29151:2017 (item 9.2.2 e 9.2.3)	NIST PR.AC-P1 NIST PR.AC-P4 NIST PR.AC-P6	1, 2, 3
31.4	PROTEGER-P	A instituição considera o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.3)	NIST PR.AC-P4	1, 2, 3
31.5	PROTEGER-P	Meios fortes de autenticação são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD)?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.3)	NIST PR.AC-P	2, 3
31.6	PROTEGER-P	O acesso físico aos dados e dispositivos é gerenciado?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49 Art. 50	N/A	NIST PR.AC-P2	1, 2, 3
31.7	PROTEGER-P	O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança (Exemplo: https://www.ssllabs.com/ssltest/)?	Art. 6º, inciso VII Art. 30, Art. 34, inciso IV Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 29151:2017 (item 13.2.2)	NIST PR.DS-P2	2, 3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.8	PROTEGER-P	Os dados pessoais armazenados/retidos possuem controles de integridade permitindo identificar se os dados foram alterados sem permissão?	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 29151:2017 (item A.12 a)	NIST PR.DS-P6	2, 3
31.9	PROTEGER-P	O órgão adota mecanismos para restauração de dados pessoais?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.3) ABNT NBR ISO/IEC 27701:2019 (item 6.9.3.1)	NIST PR.PO-P NIST PR.DS-P NIST PR.PT-P	1, 2, 3
31.10	PROTEGER-P	O órgão restringe e controla a impressão de documentos que contenha dados pessoais encaminhados para as impressoras corporativas?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.2)	NIST PR.PT-P	1, 2, 3
31.11	PROTEGER-P	O órgão descarta materiais impressos de forma segura?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.7)	NIST PR.PO-P NIST PR.DS-P	1, 2, 3
31.12	PROTEGER-P	As medidas de mitigação de riscos resultantes do RIPD são consideradas no processo de desenvolvimento de sistemas?	Art. 32 Art. 38 Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 14.1.2) ABNT NBR ISO/IEC 27701:2019 (item 5.6.2 e 7.2.5)	NIST ID.RA-P NIST GV.MT-P1 NIST PR.DS-P	2, 3
31.13	PROTEGER-P	A manutenção e reparação dos ativos organizacionais são realizadas e registradas, com ferramentas aprovadas e controladas?	Art. 6º, inciso VII Art. 46 Art. 50	N/A	NIST PR.MA-P1	2, 3
31.14	PROTEGER-P	A manutenção remota dos ativos organizacionais é aprovada, registrada e executada de forma a impedir o acesso não autorizado?	Art. 6º, inciso VII Art. 46 Art. 50	N/A	NIST PR.MA-P2	2, 3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.15	PROTEGER-P	A organização ao realizar registros de eventos (logs), considerando o princípio de minimização de dados, grava o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49 Art. 50	ABNT NBR ISO/IEC 27701:2019 (item 6.9.4.1)	NIST CT.DM-P8	3
31.16	PROTEGER-P	A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?	Art. 48 Art. 50, § 2º, inciso I, alínea “g”	ABNT NBR ISO/IEC 27701:2019 (itens 6.13.1.4 e 6.13.1.5)	NIST PR.DS-P5	2, 3
31.17	PROTEGER-P	A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	Art. 46 Art. 47 Art. 49 Art. 50, § 2º, inciso I, alínea “g”	ABNT NBR ISO/IEC 27701:2019 (item 6.13.1.1)	NIST PR.PO-P7	1, 2, 3
31.18	PROTEGER-P	A organização comunica à Autoridade Nacional de Proteção de Dados sobre a ocorrência de incidente de segurança e proteção de dados pessoais?	Art. 48	N/A	NIST CMAW-P7	1, 2, 3

ANEXO VI – MUDANÇAS DAS VERSÕES

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia do Framework de Privacidade e Segurança da Informação.

Mudanças da Versão 1.1.3

A mudança inserida nesta versão em comparação com a anterior visa a ajustar a fórmula do Indicador de Maturidade por Controle (iMC), conforme descrito na página 84, em alinhamento ao estabelecido na Ferramenta do Framework disponibilizada aos órgãos para diagnóstico e avaliação da maturidade em Privacidade e Segurança da Informação.

Importante destacar que o ajuste desta fórmula nesta versão do presente Guia não impacta nos resultados dos indicadores de maturidade obtidos nos ciclos de implementações já realizados uma vez que a fórmula ajustada já estava implementada na ferramenta.

Ademais, os exemplos apresentados imediatamente após a referida expressão foram adaptados de acordo com as alterações mencionadas.

Mudanças da Versão 1.1.2

A mudança inserida nesta versão em comparação com a anterior visa a padronizar o termo “**Unidade de Controle Interno**” em alinhamento ao estabelecido pela Portaria SGD/MGI nº 852/2023 que dispõe sobre o PPSI.

Além disso, foi atualizada a Figura 5 com o objetivo de contemplar as medidas do controle 0 que trata da Estruturação Básica de Gestão em Privacidade e Segurança da Informação.

Mudanças da Versão 1.1.1

A mudança inserida nesta versão em comparação com a anterior visa o ajuste da redação da medida 31.2, conforme destaque em negrito apresentado a seguir:

- O órgão submete os controles **de privacidade e segurança da informação adotados** a revisão e reavaliação periódicas **resultantes da avaliação de impacto na privacidade**?

Mudanças da Versão 1.1

As mudanças inseridas nesta versão em comparação com a anterior visam principalmente a revisão das referências das medidas de privacidade constantes do Anexo V, mais especificamente as referências ABNT NBR ISO/IEC 27701, ISO/IEC 29151, ISO/IEC 27018, ISO/IEC 29134, ABNT NBR ISO/IEC 29184.

Além disso, foram realizados ajustes como as remoções das seguintes citações: termo “operador” na página 20 e na medida 0.7 do Controle 0 (Anexo III); e termos “primário” e “secundário” nas medidas 0.1 e 0.2 do Controle 0 (Anexo III).

Por fim, o termo “autoridade máxima de Tecnologia da Informação” foi substituído em todo o Guia pelo termo “Gestor de Tecnologia da Informação e Comunicação” em alinhamento ao estabelecido pela Portaria SGD/MGI nº 852/2023.