CARTILHA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

COMUNICAR PARA EDUCAR

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO
GABINETE DE SEGURANÇA INSTITUCIONAL
PRESIDÊNCIA DA REPÚBLICA

Apresentação

Com o crescimento de atividades maliciosas no espaço cibernético e de ataques aos órgãos e às entidades da administração pública federal (APF), urge a necessidade de aumentar e de aprimorar as ações na área de segurança da informação. Nesse sentido, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) possui competência para elaborar e atualizar normativos, com vistas a orientar os gestores na implementação de requisitos mínimos de segurança da informação.

A segurança da informação deve ser uma prioridade da APF, a fim de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos seus ativos de informação, especialmente aqueles que, na atual conjuntura dos serviços digitais, são suscetíveis a incidentes cibernéticos.

Nesse contexto, esta Cartilha surgiu como uma demanda do Comitê Gestor de Segurança da Informação (CGSI), tendo sido elaborada pelo Departamento de Segurança da Informação (DSI) do GSI/PR, sob coordenação da Assessoria Especial de Segurança da Informação (AssESI).

Os objetivos deste documento:

Orientar os gestores de segurança da informação no desempenho de suas atribuições e competências.

Esclarecer as responsabilidades dos envolvidos no processo de segurança da informação.

Apresentar a estrutura de segurança da informação aplicável dos órgãos e entidades da APF, os normativos aplicáveis, o vocabulário utilizado, dentre outras informações relevantes.

O material está dividido em 3 capítulos:

1. Segurança da informação.
2. Responsabilidades
3. Boas práticas em segurança da informação.

Este material não pretende esgotar o assunto, possuindo apenas caráter informativo. O tema encontra-se em constante discussão e evolução, o que exige dos gestores nos diversos níveis e das demais partes interessadas flexibilidade e capacidade de adaptação para acompanhar o desenvolvimento da área de segurança da informação.

Caso persistam dúvidas ou sejam identificadas oportunidades de melhoria neste documento, a equipe do DSI coloca-se à disposição para receber sugestões e questionamentos por meio dos contatos apresentados no final desta Cartilha.

Boa leitura e bom trabalho a todos!

Gabinete de Segurança Institucional da Presidência da República

Data	Versão	Descrição	Autoria
21/12/2022	1.0	CARTILHA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO	Departamento de Segurança da Informação - GSI/PR

Sumário

1 SEGURANÇA DA INFORMAÇÃO.....6
1.1 Definição.....6
1.2 Escopo 6
1.2.1 Aspectos importantes da Política Nacional de Segurança da Informação (PNSI) e da Estratégia Nacional de Segurança Cibernética (E-Ciber) a serem considerados no planejamento da gestão da segurança da informação.....7
1.3 Estrutura da gestão da Segurança da Informação.....7
1.3.1 Gabinete de Segurança Institucional da Presidência da República (GSI/PR).....7
1.3.2 Comitê Gestor de Segurança da Informação (CGSI).....8
1.3.2.1 Composição.....9
1.3.2.2 Reuniões.....9
1.3.3 Comitê de Segurança da Informação do órgão ou da entidade.....9
1.3.3.1 Atribuições.....9
1.3.3.2 Composição.....10
1.3.3.3 Coordenação.....10
1.3.4 Gestor de Segurança da Informação.....10
1.3.5 Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).....11
1.3.5.1 Constituição.....11
1.3.5.2 Composição.....11
1.4 Glossário de Segurança da Informação.....12

2 RESPONSABILIDADES 13
2.1 Dos órgãos e Entidades.....13
2.1.1 Competências 13
2.1.2 Execução de programas, projetos e processos 14
2.1.3 Recursos orçamentários 14
2.2 Dos componentes da estrutura de gestão 14
2.2.1 Da Alta Administração - Competências.....14
2.2.2 Do Comitê de Segurança da Informação do Órgão ou da Entidade – Atribuições.....15
2.2.3 Do Gestor de Segurança da Informação – Competências:.....15
2.2.4 Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).....17
2.3 Política de Segurança da Informação.....17
2.3.1 Elaboração e Adoção.....18
2.3.2 Composição.....18

2.3.3 Revisão e atualização.....18
2.4 Avaliação de Conformidade nos aspectos de segurança da informação.....18
2.4.1 Competências específicas do Gestor de segurança da informação.....19
2.4.2 Processo de Avaliação.....19

3 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO 20
3.1 Frameworks e normas técnicas.....20
3.2 Guias e modelos 21

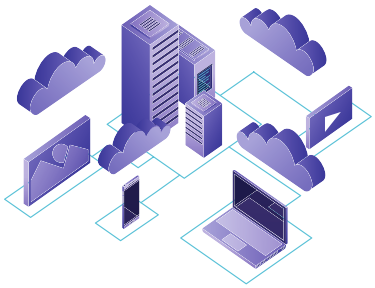
Anexo I – Contatos no Departamento de Segurança da Informação.....22

Anexo II – Legislações aplicáveis.....23

Anexo III – Legislações em revisão e consolidação no DSI, do GSI/PR.....24

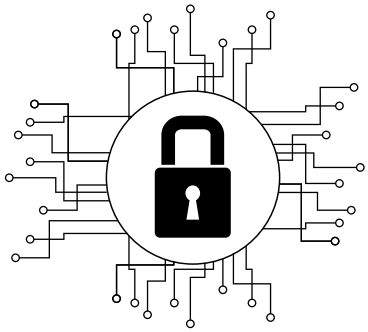
1 SEGURANÇA DA INFORMAÇÃO

1.1 Definição



Segundo o Glossário elaborado pelo Departamento de Segurança da Informação (DSI), do Gabinete de Segurança Institucional (GSI/PR), a segurança da informação "trata de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações".

A segurança da informação abrange todos os ativos de informação, que, segundo o Glossário de segurança da 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".



Dessa forma, pessoas, objetos, sistemas, plataformas, softwares, aplicativos, redes de dados ou qualquer fonte que contém, transmite ou processa dados, apresenta suas vulnerabilidades que devem ser estudadas e reduzidas utilizando mecanismos e práticas de segurança da informação.

1.2 Escopo

O Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, assim como a Instrução Normativa (IN) GSI/PR nº 1, de 27 de maio de 2020, definem que a segurança da informação abrange:

I - a segurança cibernética;[1]

II - a defesa cibernética;[2]

[1] SEGURANÇA CIBERNÉTICA - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021)

[2] DEFESA CIBERNÉTICA - ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente. (PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021)

III - a segurança física;
IV - a proteção de dados organizacionais; e
V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

1.2.1 Aspectos importantes da Política Nacional de Segurança da Informação (PNSI) e da Estratégia Nacional de Segurança Cibernética (E-Ciber) a serem considerados no planejamento da gestão da segurança da informação:

- Abrangência da segurança da informação.
- Objetivos e ações estratégicas.
- Instrumentos.
- Instituição e competências do Comitê Gestor de Segurança da Informação.
- Competências do Gabinete de Segurança Institucional da Presidência da República, do Ministério da Defesa, da Controladoria-Geral da União e dos demais órgãos e das entidades da administração pública federal.

1.3 Estrutura da gestão da Segurança da Informação

É composta pelo GSI/PR, pelo Comitê Gestor de Segurança da Informação, pelo Comitê de Segurança da Informação do órgão ou da entidade, pelo gestor de segurança da informação e pelas Equipes de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos.

1.3.1 Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

- Coordena em alto nível a atividade de segurança da informação no âmbito da administração pública federal, nela incluídas a segurança cibernética e a gestão de incidentes computacionais. [3]

[3] Art. 10, IV e V, da Lei nº 13.844, de 18 de junho de 2019.

- Estabelece normas de segurança da informação a serem incorporadas por órgãos e entidades da administração pública federal.[4]

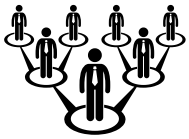
1.3.2 Comitê Gestor de Segurança da Informação (CGSI)

- Assessora o GSI/PR quanto às atividades relacionadas à segurança da informação.[5]

QR Code para acesso rápido às legislações, às atribuições e à composição do CGSI.

[4] Art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018.
[5] Art. 8º do Decreto nº 9.637, de 26 de dezembro de 2018.

1.3.2.1 Composição[6]



- 01 (um) representante titular com o respectivo suplente, indicados por cada órgão ou entidade elencados no art. 9º do Decreto nº 9.637, de 2018, e designados em ato do Ministro de Estado Chefe do GSI/PR.

  Obs.: O representante do órgão ou da entidade no CGSI não é, necessariamente, o gestor de segurança da informação do órgão ou da entidade; ele pode ser o indicado, desde que possua atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos ou entidades.[7]

1.3.2.2 Reuniões [8]

- Em caráter ordinário, semestralmente; e
- Em caráter extraordinário, por convocação do coordenador do CGSI.

1.3.3 Comitê de Segurança da Informação do órgão ou da entidade

1.3.3.1 Atribuições [9]

- Assessorar a implementação das ações de segurança da informação.
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.
- Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação.
- Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação.
- Deliberar sobre normas internas de segurança da informação.

[6] Resolução GSI/PR nº 1, de 11 de setembro de 2019.
[7] Art. 9º, § 2º, do Decreto nº 9.637, de 26 de dezembro de 2018.
[8] Art. 10 do Decreto nº 9.637, de 26 de dezembro de 2018.
[9] Art. 15, §3º, do Decreto nº 9.637, de 26 de dezembro de 2018.

- Deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade.

1.3.3.2 Composição

- Um representante da Secretaria Executiva ou de unidade equivalente.
- Um representante de cada unidade finalística e do titular da unidade de tecnologia da informação.
- O gestor de segurança da informação.

1.3.3.3 Coordenação

- Pela maior autoridade designada na sua composição, tendo suas competências estabelecidas no art. 20 da Instrução Normativa (IN) GSI/PR nº 1/2020.[10]

1.3.4 Gestor de Segurança da Informação

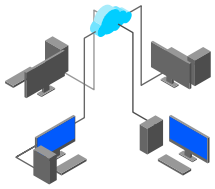
- Designado dentre os servidores públicos civis ocupantes de cargo efetivo, empregados públicos e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.[11]

  Obs.: Suas competências estão detalhadas no capítulo 2.2.3 desta Cartilha.

[10] Art. 21, parágrafo único, da IN GSI/PR nº 1, de 27 de maio de 2020

[11] Art. 15, §4º, do Decreto nº 9.637, de 26 de dezembro de 2018, e Art. 18, da IN GSI/PR nº 1, de 27 de maio de 2020.

1.3.5 Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)



- Criação obrigatória para todos os órgãos e todas as entidades que possuem a competência de administrar a infraestrutura de rede de sua organização.
- Responsável por prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade.
- Anteriormente, era chamada de Equipe de Tratamento de Incidentes de Rede, tendo-se introduzido em sua designação a palavra "prevenção"[12], seguindo a tendência internacional da comunidade de segurança cibernética de enfatizar as ações preventivas, em face dos atuais tipos de atividades e programas maliciosos, em especial o ransomware.

1.3.5.1 Constituição

- Em documento que designe suas atribuições e seu escopo de atuação.

1.3.5.2 Composição

- Preferencialmente, de servidores públicos civis ocupantes de cargo efetivo, empregados públicos ou militares de carreira, com capacitação técnica compatível com suas atividades.

[12] Decreto nº 10.641, de 2 de março de 2021, introduziu a palavra "prevenção" na denominação do CTIR Gov e da ETIR, entre outras alterações na PNSI, e a IN GSI/PR nº 2, de 24 de julho de 2020, que introduziu essa palavra na denominação da ETIR.

1.4 Glossário de Segurança da Informação

- Aprovado pela Portaria nº 93/GSI, de 18 de outubro de 2021, deve ser utilizado como referência para os trabalhos relacionados à segurança da informação.

- Atualizado, periodicamente, pelo GSI/PR, devendo os órgãos e as entidades da administração pública federal enviar, a qualquer tempo, contribuições e sugestões para seu aperfeiçoamento.[13]

QR Code para acesso rápido ao Glossário de Segurança da Informação.

[13]Arts. 6º e 7º, da IN GSI/PR nº 1, de 27 de maio de 2020.

2 RESPONSABILIDADES

A IN GSI/PR nº 1, de 27 de maio de 2020, apresenta a estrutura de gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal.

2.1 Dos Órgãos e Entidades

2.1.1 Competências[14]

- Implementar a PNSI.
- Elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo GSI/PR.
- Designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade.
- Instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI.
- Destinar recursos orçamentários para ações de segurança da informação.
- Promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação.
- Instituir e implementar equipe de prevenção, tratamento e resposta a incidentes cibernéticos, que comporá a rede de equipes dos órgãos e das entidades da administração pública federal, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) do DSI/GSI/PR.
- Coordenar e executar as ações de segurança da informação no âmbito de sua atuação.
- Consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação.
- Aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.
- Designar, pelo menos, um substituto para os cargos de segurança da informação.

[14]Art. 15, do Decreto nº 9.637, de 26 de dezembro de 2018.

2.1.2 Execução de programas, projetos e processos

Devem ser orientados para:[15]

- O aumento da resiliência dos ativos de Tecnologia da Informação e serviços estratégicos definidos pelo Governo federal;
- A contínua cooperação entre as ETIR na APF e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov);
- A priorização da interoperabilidade de tecnologias, processos, informações e dados; e
- A utilização de recursos criptográficos adequados ao grau de sigilo exigido e restrições de acesso estabelecidas.

2.1.3 Recursos orçamentários

Aos órgãos e entidades da APF, em seu âmbito de atuação compete destinar recursos orçamentários para a operacionalização dos processos de Segurança da Informação.

2.2 Dos componentes da estrutura de gestão

Como forma de estruturar a gestão da segurança da informação nos órgãos e entidades da APF, devem ser designados, ao menos, o gestor de segurança da informação, o comitê de segurança da informação ou estrutura equivalente e uma ETIR ou estrutura equivalente (art. 16, da IN GSI/PR nº 1/2020). As atribuições dessas essenciais funções são detalhadas a seguir.

2.2.1 Da Alta Administração – Competências:

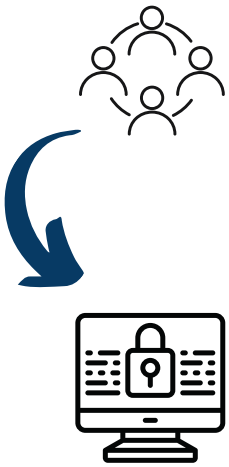
- Realizar a governança da segurança da informação, conforme competências estabelecidas no art. 17, do Decreto nº 9.637, de 2018 e no art. 41, da IN GSI/PR nº 3, de 28 de maio de 2021.
- Implantar os controles gerais de segurança da informação positivados nas normas do GSI/PR. Vale ressaltar que isto não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível das sanção prevista na Lei 8.443/1992, art.58, II (subitem II.8).[16]

[15] Art. 17, § 1º, do Decreto nº 9.637, de 26 de dezembro de 2018.

[16] Acórdão nº 1.233/2012 - TCU

- Designar ao menos um servidor efetivo, militar de carreira ou empregado público, pertencente ao respectivo órgão ou entidade, como responsável pela avaliação de conformidade de acordo com os aspectos relativos à segurança da informação.

2.2.2 Do Comitê de Segurança da Informação do Órgão ou da Entidade – Atribuições:



- Assessorar a implementação das ações de segurança da informação.
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.
- Participar da elaboração da política de segurança da informação e das normas internas de segurança da informação.
- Propor alterações à política de segurança da informação e às normas internas de segurança da informação.
- Deliberar sobre normas internas de segurança da informação.
- Deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à alta administração para aprovação o processo contendo os documentos sobre a avaliação de conformidade.

2.2.3 Do Gestor de Segurança da Informação – Competências:

- Prestar contas das atividades de segurança da informação ao Comitê de Segurança da Informação ou estrutura equivalente.
- Coordenar a elaboração da política de segurança da informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo GSI/PR e as melhores práticas sobre o assunto.
- Assessorar a alta administração na implementação da política de segurança da informação.
- Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação.
- Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade.

- Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação.
- Propor recursos necessários às ações de segurança da informação.
- Acompanhar os trabalhos da ETIR.
- Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.
- Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

- Prestar as informações necessárias para as ações da equipe de conformidade e avaliar o relatório de conformidade.
- Manter contato direto com o DSI/GSI/PR em assuntos relativos à segurança da informação.
- Designar os agentes responsáveis pela gestão de:

  - ativos de informação;
  - mudanças em aspectos de segurança da informação;
  - riscos de segurança da informação; e
  - continuidade de negócios em segurança da informação.

- Proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação.

- Coordenar os seguintes processos de realização obrigatória pelos órgãos e pelas entidades da administração pública federal: [17]

  - mapeamento de ativos de informação;
  - gestão de mudanças nos aspectos de segurança da informação;
  - gestão de riscos de segurança da informação; e
  - gestão de continuidade de negócios em Segurança da informação.

- Quanto à gestão de riscos, aprovar:

  - O plano de gestão de riscos de segurança da informação;
  - O relatório de identificação, análise e avaliação dos riscos de segurança da informação; e
  - O relatório de tratamento de riscos de segurança da informação.

[17] IN GSI/PR nº 3, de 28 de maio de 2021.

- Quanto à gestão de mudanças, analisar o documento de avaliação e aprovação de mudança para apreciação e aprovação da alta administração
- Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação, bem como acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).
- Manter contato direto com o DSI/GSI/PR em assuntos relativos à segurança da informação.
- Quanto à avaliação de conformidade nos aspectos de segurança da informação:

- Fornecer, ao(s) agente(s) responsável(is) pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação.
- Emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação.
- Adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração.

2.2.4 Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

São regidas por normativos padrões e procedimentos técnicos exarados pelo CTIR Gov, sem prejuízos das demais metodologias e padrões conhecidos. A comunicação com a ETIR ocorrerá por formatos e procedimentos padronizados pelo CTIR Gov.[18]

2.3 Política de Segurança da Informação

Deve ser implementada a partir da formalização e aprovação da autoridade máxima da instituição, buscando estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação, garantindo recursos necessários à sua execução.[19]

[18]Art. 22, § 3º e §4º, da IN GSI/PR nº 1, de 27 de maio de 2020.

[19]Art. 9º da IN GSI/PR nº 1/2020.

2.3.1 Elaboração e Adoção

- Evidencia o comprometimento da alta administração com a gestão de segurança da informação em sua organização.

- Leva em consideração a natureza e a finalidade do órgão ou da entidade e deve estar alinhada ao planejamento estratégico[20] do órgão ou da entidade, contendo, no mínimo, os itens, estabelecidos no art. 12 da IN GSI/PR nº 1/2020.

2.3.2 Composição[21]

- Escopo, conceitos e definições, diretrizes, competências, penalidades e política de atualização.

2.3.3 Revisão e Atualização[22]

- Deve ser revista e atualizada num prazo máximo de 4 (quatro) anos, sendo complementada, quando necessário, por normas, metodologias e procedimentos adequados.

2.4 Avaliação de Conformidade nos aspectos de segurança da informação[23]

Proporciona adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis. As atribuições relacionadas à avaliação de conformidade para a alta administração e para os agentes responsáveis pela avaliação estão descritas nos arts. 41 e 43 da IN GSI/PR nº 3, de 28 de maio de 2021.

[20] Art. 11, da IN GSI/PR nº 1/2020, de 27 de maio de 2020.

[21] Art. 12, da IN GSI/PR nº 1/2020, de 27 de maio de 2020.

[22] Art. 12, §1º e §2º, da IN GSI/PR nº 1, de 27 de maio de 2020.

[23] Art. 37, da IN GSI/PR nº 3, de 28 de maio de 2021.

2.4.1 Competências específicas do Gestor de segurança da informação:[24]

- Coordenar a avaliação de conformidade nos aspectos relativos à segurança da informação;
- Fornecer, aos agentes responsáveis pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação;
- Emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação;
- Adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração; e
- Após a aprovação do processo de avaliação de conformidade pela alta administração, deverá adotar as ações cabíveis aprovadas.

2.4.2 Processo de Avaliação[25]

- Deve ser composto, no mínimo, pelos seguintes documentos:

  I - O plano de gestão de riscos de segurança da informação;
  II - O relatório de identificação, análise e avaliação dos riscos de segurança da informação; e
  III - O relatório de tratamento de riscos de segurança da informação.

Obs: os requisitos mínimos para elaboração do plano de verificação de conformidade e do relatório de avaliação de conformidade encontram-se descritos nos arts. 39 e 40, da IN GSI/PR nº 3, de 28 de maio de 2021.

[24]Art. 42, da IN GSI/PR nº 3, de 28 de maio de 2021.

[25]Art. 11, da IN GSI/PR nº 1/2020, de 27 de maio de 2020.

3 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Estão disponíveis diversos frameworks e guias para implantação de controles de Segurança da Informação. Tendo por base o utilizado pelo DSI, bem como nas auditorias realizadas pelo Tribunal de Contas da União (TCU) e pela Controladoria-Geral da União (CGU), sugere-se a utilização dos seguintes documentos:

3.1 Frameworks, referências e normas técnicas

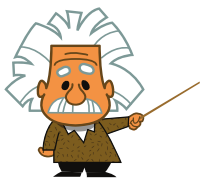
- Framework do Center for Internet Security (CIS), versão 8;
- The NIST Cybersecurity Framework;
- Norma ABNT NBR ISO/IEC 27.001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos;
- Norma ABNT NBR ISO/IEC 20.000-2:2008 – Tecnologia da Informação- Gestão de serviço – Parte 2: Orientação para aplicação de sistemas de gestão de serviço;
- Norma ABNT NBR ISO/IEC 27.005:2008 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação;
- Norma ABNT NBR ISO/IEC 27.002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação;

- Boletins Informativos Mensais do DSI; e
- Itens da biblioteca de referência em estrutura de Tecnologia da Informação da Information Technology Infrastructure Library (ITIL v3 ou ITIL v4).

3.2 Guias e modelos

Guias e modelos de Segurança e Proteção de Dados da SGD/ME.

FIM



“Uma pessoa inteligente resolve um problema, um sábio previne-o.”

(Albert Einstein)

ANEXO I

CONTATOS NO DSI

Setor	Contato
Departamento de Segurança da Informação (DSI)	dsi@presidencia.gov.br 3411-4253
Coordenação-Geral de Gestão de Segurança da Informação (CGGSI)	cggsi@presidencia.gov.br 3411-3978

ANEXO II

LEGISLAÇÃO APLICÁVEL

I.Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI).
II.Lei nº 13.844, de 18 de junho de 2019. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, nela incluídas as competências do GSI/PR
quanto à segurança cibernética e da informação.
III.Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei de Acesso à Informação.
IV.Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
V.Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação (PNSI) e o Comitê Gestor da Segurança da Informação (CGSI), entre outras disposições.
VI.Decreto nº 9.668, de 2 de janeiro de 2019. Aprova a Estrutura Regimental do GSI/PR, entre outras disposições.
VII.Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber), com validade no quadriênio 2020-2023.
VIII.Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
IX.Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 (com as alterações dadas pela Instrução Normativa nº 2, de 24 de julho de 2020 e pela Instrução Normativa nº 7, de 29 de novembro de 2022). Dispõe sobre a estrutura de gestão da segurança da informação nos órgãos e nas entidades da administração pública federal.
X.Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. (com as alterações dadas pela Instrução Normativa nº 7, de 29 de novembro de 2022) Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
XI.Portaria nº 93 GSI/PR, de 18 de outubro de 2021. Aprova o Glossário de Segurança da Informação.
XII.Instrução Normativa GSI/PR nº 4, de 26 de março de 2020 - Requisitos mínimos de Segurança Cibernética no estabelecimento das redes 5G.
XIII.Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021 - Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
XIV.Instrução Normativa GSI/PR Nº 6, 23 de dezembro de 2021. (com as alterações dadas pela Instrução Normativa nº 7, de 29 de novembro de 2022) - Diretrizes de segurança da informação para uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

ANEXO III

Legislação a ser revisada e consolidada pelo GSI/PR

I. Instrução Normativa nº 2, de 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.

II. Instrução Normativa nº 3, de 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.

III. Norma Complementar nº 01/IN02/NSC/GSIPR. Disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas.

IV. Norma Complementar nº 05/IN01/DSIC/GSIPR. Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da administração pública federal.

V. Norma Complementar nº 07/IN01/DSIC/GSIPR. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

VI. Norma Complementar nº 08/IN01/DSIC/GSIPR. Estabelece as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal.

VII. Norma Complementar nº 09/IN01/DSIC/GSIPR. Estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações, nos órgãos ou entidades da administração pública federal direta e indireta.

VIII.Norma Complementar 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 direta e indireta.

IX.Norma Complementar nº 16 /IN01/DSIC/GSIPR. Estabelece as diretrizes para o desenvolvimento e obtenção de software seguro nos órgãos e entidades da administração pública federal direta e indireta.

X.Norma Complementar 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 nas entidades da administração pública federal.

XI.Norma Complementar nº 18/IN01/DSIC/GSIPR. Estabelece as Diretrizes para as atividades de ensino em Segurança da Informação e Comunicações (SIC) nos órgãos e nas entidades da administração pública federal.

XII.Norma Complementar nº 19/IN01/DSIC/GSIPR. Estabelece padrões mínimos de segurança da informação e comunicações para os sistemas estruturantes da administração pública federal direta e indireta.

XIII.Norma Complementar nº 20/IN01/DSIC/GSIPR. 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 direta e indireta.

XIV.Norma Complementar 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 nas entidades da administração pública federal direta e indireta.