# INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 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.

**O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, e tendo em vista o disposto no art. 10, incisos IV e V, da Lei nº 13.844, de 18 de junho de 2019, no art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018, e no Decreto nº 9.668, de 2 de janeiro de 2019, resolve:

Art. 1º Aprovar os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º A presente Instrução Normativa trata dos processos relacionados à gestão de segurança da informação que devem ser observados pelos órgãos e pelas entidades da administração pública federal no planejamento e na implementação de suas ações referentes à segurança da informação.

§ 1º Os conceitos relacionados à temática dessa Instrução Normativa poderão ser consultados no glossário de segurança da informação, aprovado e atualizado por portaria do Gabinete de Segurança Institucional da Presidência da República.

§ 2º A gestão de segurança da informação deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do órgão ou da entidade.

§ 3º Os processos relacionados à gestão de segurança da informação devem estar alinhados com os controles internos de gestão do órgão ou da entidade.

Art. 3º A gestão de segurança da informação será constituída pelos seguintes processos de realização obrigatória pelos órgãos e pelas entidades da administração pública federal:

I - mapeamento de ativos de informação;

II - gestão de riscos de segurança da informação;

III - gestão de continuidade de negócios em segurança da informação;

IV - gestão de mudanças nos aspectos de segurança da informação; e

V - avaliação de conformidade de segurança da informação.

CAPÍTULO II

MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 4º O processo de mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 5º O processo de mapeamento de ativos de informação deve considerar, preliminarmente:

I - os objetivos estratégicos da organização;

II - os processos internos da organização;

III - os requisitos legais; e

IV - a estrutura do órgão ou da entidade.

Art. 6º O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:

I - os responsáveis - proprietários e custodiantes - de cada ativo de informação;

II - as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;

III - os contêineres de cada ativo de informação; e

IV - as interfaces de cada ativo de informação e as interdependências entre eles.

Art. 7º O registro de ativos de informação deverá ser homologado por meio de ato do titular do órgão ou da entidade.

Art. 8º Cabe ao gestor de segurança da informação de cada órgão ou entidade coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos do órgão ou da entidade.

Art. 9º Cabe ao agente responsável pela gestão dos ativos de informação:

I - identificar e classificar os ativos de informação por nível de criticidade;

II - identificar potenciais ameaças aos ativos de informação;

III - identificar vulnerabilidades dos ativos de informação;

IV - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

V - autorizar a atualização do relatório mencionado no inciso IV do**caput**; e

VI - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

CAPÍTULO III

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 10. O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o órgão ou entidade.

Art. 11. O processo de gestão de riscos de segurança da informação deve estar alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos do órgão ou entidade, além de considerar, preliminarmente:

I - os processos internos institucionais;

II - os requisitos legais;

III - a política de segurança da informação do órgão ou da entidade;

IV - a política de gestão de riscos institucional, caso exista; e

V - a estrutura do órgão ou da entidade.

Art. 12. O processo de gestão de riscos de segurança da informação deverá fornecer à organização os seguintes documentos:

I - plano de gestão de riscos de segurança da informação;

II - relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

III - relatório de tratamento de riscos de segurança da informação.

Art. 13. O plano de gestão de riscos de segurança da informação deverá conter, no mínimo:

I - a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento;

II - a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos;

III - os tipos de riscos;

IV - o nível de severidade dos riscos;

V - um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e

VI - um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração.

§ 1º O plano de gestão de riscos da segurança da informação deve ser regularmente revisado, a fim de manter atualizados os riscos relativos aos ativos de informação.

§ 2º O processo de implementação do plano de gestão de riscos de segurança da informação deverá considerar, dentre outros aspectos, as recomendações de mudanças em relação aos critérios de aceitação de riscos, a abrangência da atuação do plano, as ações de segurança da informação e as atividades de tratamento de riscos previstas.

Art. 14. O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser elaborado com base no modelo estabelecido pelo plano de gestão de riscos de segurança da informação e deverá conter, no mínimo:

I - os riscos associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas;

II - o grau de severidade dos riscos identificados, considerando os valores ou os níveis de probabilidade de ocorrência do risco e as consequências da ocorrência do risco (perda da integridade, disponibilidade, confiabilidade ou autenticidade nos ativos envolvidos);

III - os eventos de segurança da informação ocorridos, com a descrição das ações de segurança, e de eventuais consequências do evento para o órgão ou a entidade;

IV - as alterações nos fatores de risco; e

V - as mudanças em relação a critérios de avaliação e análise.

§ 1º O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.

§ 2º Entende-se como contextos interno e externo o conjunto de eventos que possam influenciar a capacidade da organização de atingir seus objetivos estratégicos.

Art. 15. O relatório de tratamento de riscos de segurança da informação deve ser resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação.

§ 1º O relatório de tratamento de riscos de segurança da informação deve considerar as possibilidades de tratamento para cada risco identificado.

§ 2º Para cada possibilidade de tratamento detectada em função do risco identificado, devem ser observados, no que couber:

I - a eficácia das ações de segurança da informação;

II - as restrições técnicas;

III - as restrições físicas estruturais;

IV - as restrições operacionais;

V - as restrições organizacionais;

VI - os requisitos legais; e

VII - a relação custo-benefício.

§ 3º O relatório de tratamento de riscos de segurança da informação deverá ser elaborado com base no modelo estabelecido pelo plano de gestão de riscos de segurança da informação e deverá conter, no mínimo:

I - a definição e a priorização das ações de segurança e as atividades de tratamento de riscos que deverão ser realizadas;

II - os responsáveis pela execução e pelo acompanhamento das ações de segurança e atividades de tratamento de riscos;

III - os prazos de execução das ações de segurança e das atividades de tratamento de riscos; e

IV - as opções de tratamentos de riscos priorizados.

Art. 16. Cabe ao gestor de segurança da informação de cada órgão ou entidade:

I - coordenar a gestão de riscos de segurança da informação;

II - designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do órgão;

III - aprovar o plano de gestão de riscos de segurança da informação;

IV - aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;

V - aprovar o relatório de tratamento de riscos de segurança da informação; e

VI - propor medidas preventivas à alta administração.

Art. 17. Cabe ao agente responsável pela gestão de riscos de segurança da informação elaborar:

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.

CAPÍTULO IV

GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO

Art. 18. A implementação do processo de gestão de continuidade de negócios em segurança da informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou da entidade nessa área, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 19. O processo de gestão de continuidade de negócios em segurança da informação deve ser baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio.

Art. 20. As diretrizes institucionais sobre o assunto devem ser formalizadas pelo órgão ou pela entidade, contemplando, no mínimo, os seguintes aspectos:

I - consonância com a missão do órgão ou da entidade, considerando sua estrutura, natureza do negócio e sua complexidade, a fim de que a política reflita a cultura e o ambiente institucional;

II - compromissos claros com relação às obrigações legais e regulamentares e à melhoria contínua do processo de gestão de continuidade de negócios em segurança da informação;

III - definição da abrangência e dos limites do processo de gestão de continuidade de negócios em segurança da informação;

IV - identificação de quaisquer autoridades do órgão ou da entidade e delegações necessárias, incluindo os responsáveis por continuidade de negócios na instituição;

V - critérios para o tipo e a escala dos incidentes a serem tratados;

VI - referências às normas, aos regulamentos ou às políticas que convém que o processo considere ou cumpra; e

VII - compromisso de realizar e manter a continuidade do negócio da instituição.

Art. 21. O processo de gestão de continuidade de negócios em segurança da informação deve ser composto por um plano de continuidade de negócios em segurança da informação, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio.

Art. 22. O plano de continuidade de negócios em segurança da informação tem por objetivo definir como serão realizadas a gestão dos incidentes em caso de desastres ou de outras interrupções das operações de negócios e a maneira como deverão ser recuperadas as atividades nos prazos estabelecidos.

Art. 23. O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo:

I - o objetivo;

II - as atividades críticas de negócio a serem contempladas no plano;

III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;

IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato;

V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e

VI - a definição:

a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;

b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;

c) dos parâmetros para encerramento do plano e para a volta à normalidade;

d) dos responsáveis por essas ações, incluindo seus dados de contato;

e) da forma de monitoramento desse processo; e

f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

Parágrafo único. O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação.

Art. 24. A revisão do plano de continuidade de negócios deverá ser realizada:

I - uma vez ao ano, no mínimo;

II - em função dos resultados dos testes de funcionamento realizados, uma vez comprovada a perda da validade e eficácia das medidas adotadas diante de novas situações; ou

III - após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

Art. 25. O gestor de segurança da informação coordenará o processo de gestão de continuidade de negócios em segurança da informação nos seus respectivos órgãos ou entidades, bem como designará um agente responsável pela referida gestão, dentre os servidores efetivos do órgão.

Art. 26. Cabem aos responsáveis pelo processo ou aos titulares das unidades em que forem identificadas atividades críticas as seguintes atribuições:

I - propor as diretrizes a serem contempladas no plano de continuidade de negócios em segurança da informação;

II - elaborar o plano de continuidade de negócios em segurança da informação;

III - realizar os testes de funcionamento desse plano;

IV - avaliar e aprimorar este plano a partir dos resultados dos testes de funcionamento;

V - gerenciar a contingência quando ocorrer a interrupção de atividades, com base nesse plano desenvolvido; e

VI - propor os recursos necessários para a implementação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes de funcionamento deste plano.

Art. 27. Cabe ao agente responsável pela gestão de continuidade de negócios em segurança da informação:

I - assessorar os responsáveis pelo processo ou os titulares das unidades em que forem identificadas atividades críticas nas atribuições descritas no art. 26;

II - avaliar o plano de continuidade de negócios em segurança da informação e propor mudanças, quando aplicável;

III - supervisionar a implementação, os testes de funcionamento e a atualização desse plano;

IV - propor melhorias na implementação de novos controles relativos ao plano de continuidade de negócios em segurança da informação;

V - participar da elaboração da análise de impacto nos negócios; e

VI - propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação.

CAPÍTULO V

GESTÃO DE MUDANÇAS NOS ASPECTOS DE SEGURANÇA DA INFORMAÇÃO

Art. 28. A implementação do processo de gestão de mudanças nos aspectos de segurança da informação tem por objetivo preparar e adaptar os órgãos e as entidades da administração pública federal para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências.

§ 1º O processo de gestão de mudanças nos aspectos de segurança da informação deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos de segurança da informação e no relatório de tratamento de riscos de segurança da informação.

§ 2º O processo mencionado no **caput**, além de promover o controle das mudanças planejadas, deve considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

Art. 29. Para efeito desta Instrução Normativa, a mudança será classificada como:

I - emergencial: mudança não prevista de alto impacto e que ocorre, geralmente, em função de:

a) incidente grave ou modificação nos fatores de risco com alto impacto para os processos da organização;

b) alteração normativa de aplicação imediata;

c) necessidade de modificação significativa imediata nos ativos de informação; e

d) outros eventos similares;

II - rotineira: mudança em que a equipe técnica já possui elevado grau de conhecimento e discernimento necessário para realizar a atividade e que ocorre, geralmente, em função de:

a) atualização da infraestrutura de tecnologia da informação;

b) serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança; e

c) outros eventos similares;

III - proativa: mudança em que se busca trazer maior eficiência para a organização e que ocorre geralmente em função de:

a) ampliação do parque computacional;

b) obsolescência prevista de equipamentos e processos;

c) necessidade de adoção de novas tecnologias; e

d) outros eventos similares.

Art. 30. O processo de gestão de mudanças de segurança da informação deve ser constituído, no mínimo, pelos seguintes instrumentos:

I - documento de descrição de mudança; e

II - documento de avaliação e aprovação de mudança.

Art. 31. O documento de descrição de mudança tem o objetivo de identificar o tipo de alteração pretendida, de forma a adequar a organização às transformações nos contextos interno e externo.

Parágrafo único. Os titulares das unidades demandantes da mudança são responsáveis pela elaboração e aprovação do documento mencionado no **caput**, o qual deverá ser remetido ao agente responsável pela gestão de mudanças nos aspectos de segurança da informação.

Art. 32. O documento de descrição de mudança deverá conter, no mínimo:

I - agente demandante;

II - unidade de origem;

III - descrição da mudança;

IV - tipo de mudança;

V - objetivo(s) da mudança com os fatores que levaram a esta necessidade; e

VI - benefícios esperados.

Art. 33. O documento de avaliação e aprovação de mudança tem o objetivo de:

I - analisar as mudanças demandadas;

II - recomendar quais mudanças devem ser aprovadas; e

III - sugerir as alternativas para a implementação das mudanças.

Art. 34. O documento de avaliação e aprovação de mudança deverá conter, no mínimo:

I - alternativas para implementação da mudança, com a descrição básica dos procedimentos necessários para sua execução;

II - recomendações, em ordem de prioridade, das alternativas a serem adotadas;

III - relação entre a mudança pretendida e outras alterações que, eventualmente, possam ocorrer simultaneamente;

IV - análise de risco dos ativos de informação que serão afetados pela mudança;

V - avaliação do impacto do adiamento da realização da mudança;

VI - definição da alternativa a ser implementada ou indeferimento da mudança proposta pela alta administração do órgão ou da entidade; e

VII - análise crítica das consequências de mudanças não previstas e de ações propostas para mitigação das eventuais consequências negativas.

Art. 35. Cabe ao gestor de segurança da informação, com relação ao processo de gestão de mudanças nos aspectos de segurança da informação:

I - coordenar a gestão de mudanças;

II - designar o agente responsável pela gestão de mudança, dentre os servidores efetivos do órgão;

III - analisar e encaminhar o documento de avaliação e aprovação de mudança para apreciação da alta administração do órgão, à qual cabe a decisão de aprovar ou indeferir a mudança; e

IV - 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.

Art. 36. Cabe ao agente responsável pela gestão de mudança nos aspectos de segurança da informação:

I - recomendar à alta administração a instituição de um grupo técnico de mudança, composto por servidores das áreas afetadas e da área de segurança da informação para a elaboração do documento de avaliação e aprovação de mudança;

II - elaborar, juntamente com o grupo técnico de mudança, o documento de avaliação e aprovação de mudança e submetê-lo à análise do gestor de segurança da informação;

III - acompanhar, juntamente com o grupo técnico de mudança, os testes da mudança aprovada pelo documento de avaliação e aprovação de mudança;

IV - acompanhar, juntamente com o grupo técnico de mudança, a implementação da solução aprovada no documento de avaliação e aprovação de mudança;

V - assegurar, juntamente com o grupo técnico de mudança, registro de auditoria contendo todas as informações relevantes relacionadas com a mudança; e

VI - informar ao gestor de segurança da informação sobre o andamento e a conclusão do processo.

CAPÍTULO VI

AVALIAÇÃO DE CONFORMIDADE NOS ASPECTOS DE SEGURANÇA DA INFORMAÇÃO

Art. 37. A avaliação de conformidade nos aspectos de segurança da informação consiste em proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

Art. 38. O processo de avaliação de conformidade nos aspectos de segurança da informação deve ser composto, no mínimo, pelos seguintes documentos:

I - plano de verificação de conformidade; e

II - relatório de avaliação de conformidade.

Art. 39. O plano de verificação de conformidade deverá conter, no mínimo:

I - as unidades a serem abrangidas;

II - os aspectos a serem observados para verificação da conformidade;

III - as ações e atividades a serem realizadas;

IV - os documentos necessários para fundamentar a verificação de conformidade; e

V - as responsabilidades.

Art. 40. O relatório de avaliação de conformidade deverá conter, no mínimo:

I - o detalhamento das ações e das atividades realizadas com a identificação do responsável pela análise;

II - o parecer de conformidade; e

III - as recomendações.

§ 1º As não conformidades identificadas no relatório de avaliação devem ser tratadas em procedimento que propicie o acompanhamento das soluções adotadas e que seja definido pelo órgão ou pela entidade.

§ 2º O processo citado no § 1º pode ser parte integrante da gestão de riscos de segurança da informação citada no Capítulo III desta Instrução Normativa, caso as não conformidades identificadas sejam consideradas como um risco para a instituição.

Art. 41. Cabe à alta administração do órgão ou da entidade:

~~I - apreciar e aprovar o relatório de avaliação de conformidade e encaminhá-lo ao gestor de segurança da informação; e~~

I - aprovar o processo de avaliação de conformidade disposto no artigo nº 38 e devolvê-lo ao Comitê de Segurança da Informação para adoção das providências cabíveis; (Redação dada pela Instrução Normativa nº 7, de 2022)

~~II - promover ações de capacitação para os agentes responsáveis pela avaliação de conformidade, visando ao aperfeiçoamento de seus conhecimentos sobre a legislação vigente relativa à segurança da informação.~~

II - promover ações de capacitação para os agentes responsáveis pela avaliação de conformidade, visando ao aperfeiçoamento de seus conhecimentos sobre a legislação vigente relativa à segurança da informação; e (Redação dada pela Instrução Normativa nº 7, de 2022)

III - designar ao menos um servidor efetivo, militar de carreira ou empregado público, lotado no respectivo órgão ou entidade, como responsável pela avaliação de conformidade de acordo com os aspectos relativos à segurança da informação. (Incluído pela Instrução Normativa nº 7, de 2022)

Parágrafo único. A designação a que se refere o inciso III do **caput** deste artigo não poderá recair sobre membros da equipe de gestão de segurança da informação do órgão ou da entidade. (Incluído pela Instrução Normativa nº 7, de 2022)

Art. 42. Cabe ao gestor de segurança da informação, com relação à avaliação de conformidade nos aspectos de segurança da informação:

~~I - coordenar a avaliação de conformidade nos aspectos relativos à segurança da informação;~~ (Revogado pela Instrução Normativa nº 7, de 2022)

~~II - designar, dentre os servidores efetivos do órgão, um ou mais agentes responsáveis pela avaliação de conformidade, de acordo com os aspectos relativos à segurança da informação, não podendo ser nenhum dos membros da equipe de gestão de segurança da informação do órgão ou da entidade;~~ (Revogado pela Instrução Normativa nº 7, de 2022)

III - 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;

~~IV - analisar o relatório de avaliação de conformidade e encaminhá-lo para apreciação e aprovação da alta administração; e~~

IV - emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação; e (Redação dada pela Instrução Normativa nº 7, de 2022)

V - adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração.

Art. 43. Cabe ao(s) agente(s) responsável(is) pela avaliação de conformidade:

I - elaborar o plano de verificação de conformidade;

~~II - elaborar o relatório de avaliação de conformidade e remetê-lo à alta administração do órgão; e~~

II - elaborar o relatório de avaliação de conformidade e remetê-lo ao gestor de segurança da informação; e (Redação dada pela Instrução Normativa nº 7, de 2022)

III - verificar a adequação dos procedimentos de segurança da informação de acordo com as recomendações descritas no relatório de avaliação de conformidade.

CAPÍTULO VII

DISPOSIÇÕES GERAIS

Art. 44. Os processos mencionados nesta Instrução Normativa devem estar em conformidade com a Instrução Normativa nº 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República.

Art. 45. Os órgãos e as entidades da administração pública federal devem adotar os processos descritos na presente Instrução Normativa, bem como contemplar em seu planejamento estratégico institucional a gestão de segurança da informação.

Parágrafo único. Para o cumprimento do previsto no **caput**, os órgãos e as entidades da administração pública federal devem definir seus próprios planos de ação, com atividades, prazos e responsáveis pela implementação dos processos de gestão de segurança da informação, conforme descrito nesta Instrução Normativa.

Art. 46. Cabe aos órgãos e às entidades da administração pública federal:

I - designar, pelo menos, um substituto nos cargos previstos nesta Instrução Normativa, para que possam atuar em caso de impedimentos ou de ausência do titular; e

II - destinar recursos orçamentários para executar as ações de Segurança da Informação previstas nesta Instrução Normativa.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 47. Ficam revogados os seguintes atos normativos do Gabinete de Segurança Institucional da Presidência da República, conforme estabelece o art. 7º, inciso I, do Decreto nº 10.139, de 28 de novembro de 2019:

I - Portaria nº 62, de 19 de novembro de 2009;

II - Portaria nº 7, de 7 de fevereiro de 2012;

III - Portaria nº 9, de 7 de fevereiro de 2012;

IV - Portaria nº 10, de 7 de fevereiro de 2012; e

V - Portaria nº 2, de 15 de fevereiro de 2013.

Art. 48. Esta Instrução Normativa entra em vigor no dia 1º de julho de 2021.

**AUGUSTO HELENO RIBEIRO PEREIRA**