UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

COMITÊ DE GOVERNANÇA DIGITAL

RESOLUÇÃO NORMATIVA CGD/UFES Nº 01, DE 29 DE ABRIL DE 2025

Estabelece a Política de Segurança da Informação (Posin) no âmbito da Universidade Federal do Espírito Santo.

O COMITÊ DE GOVERNANÇA DIGITAL DA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO no uso das suas atribuições e considerando o disposto na Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD), de 14 de agosto de 2018, e no Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal, resolve:

Art. 1º. Fica instituída a Política de Segurança da Informação da Universidade Federal do Espírito Santo (Ufes), com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todos os membros da comunidade universitária.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 3º. São objetivos da Política de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;
III. estabelecer competências e responsabilidades quanto à segurança da informação;
IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;
V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da Ufes e com o arcabouço legal.

Art. 4º. Para os efeitos desta Portaria e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO II

DOS PRINCÍPIOS E DIRETRIZES

Art. 5º. As ações de segurança da informação da Ufes são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I. disponibilidade, integridade, confidencialidade e autenticidade das informações;
II. continuidade dos processos e serviços essenciais para o funcionamento da Ufes;
III. economicidade da proteção dos ativos de informação;
IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;
V. observância da publicidade como preceito geral e do sigilo como exceção;
VI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;
VII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da Ufes, assim como demais normas específicas de segurança da informação da administração pública federal;
VIII. conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e
IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação, norteando a elaboração de políticas, planos e instruções normativas no âmbito da Ufes e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º. As normas, procedimentos, manuais e metodologias de segurança da informação da Ufes devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da Ufes;
II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da Ufes;
III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV. visar à prevenção da ocorrência de incidentes.

Art. 9º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e conforme o risco de potenciais prejuízos à Ufes.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na Ufes compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional da Ufes, são passíveis de monitoramento e auditoria visando determinar o responsável por qualquer ato dentro da sua rede, respeitados os limites legais.

Art. 11. A Ufes implementará um processo de identificação e registro de informações que permita identificar as atividades realizadas pelos usuários.

§ 1º É condição para acesso aos recursos de tecnologia da informação da Ufes a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da Ufes.

§ 2º Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Art. 12. A Ufes não implementará nenhum sistema de bloqueio baseado em conteúdo para o ambiente acadêmico, mas poderá limitar a velocidade da conexão para certos tipos de serviços visando garantir a qualidade do serviço prestado.

§ 1º Poderá ser implementado um sistema de bloqueio baseado em conteúdo para o ambiente administrativo.

§ 2º Os usuários sempre são responsáveis pelas informações que distribuem ou acessam.

Art. 13. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da Ufes, devem ser divulgadas amplamente a todos os usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os usuários de informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 14. Todos os contratos de prestação de serviços firmados pela Ufes conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como de suas normas decorrentes.

CAPÍTULO III

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 15. A estrutura de Gestão de Segurança da Informação é composta por:

I. Reitoria;
II. Comitê de Governança Digital;
III. Comitê de Segurança da Informação;
IV. Gestor de Segurança da Informação;
V. Gestor de Tecnologia da Informação e Comunicação;
VI. Encarregado pelo Tratamento de Dados Pessoais;
VII. Responsável pela Unidade de Controle Interno;
VIII. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos;
IX. Unidades da Ufes; e
X. Usuários de Informação.

Art. 16. Compete à Reitoria:

I. designar um Gestor de Segurança da Informação dentre os servidores públicos ocupantes de cargo efetivo com formação ou capacitação técnica compatível;

II. instituir Comitê de Segurança da Informação (CSI) ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;

III. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da Ufes, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

IV. promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

V. instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), 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 do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

VI. coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VII. consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

VIII. aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação;

IX. promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

X. monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

XI. incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;

XII. planejar a execução de programas, de projetos e de processos relativos à segurança da informação;

XIII. estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

XIV. observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XV. implementar controles internos fundamentados na gestão de riscos da segurança da informação;

XVI. instituir um sistema de gestão de segurança da informação;

XVII. implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal;

XVIII. observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidas na legislação.

Art. 17. Compete ao Comitê de Governança Digital deliberar sobre normas internas de segurança da informação.

Art. 18. Compete ao Comitê de Segurança da Informação:

I. assessorar na implementação das ações de segurança da informação;
II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;
IV. avaliar as ações propostas pelo gestor de segurança da informação;
V. propor à Reitoria a inclusão de temas prioritários, no âmbito da segurança da informação, a serem contemplados no Plano Anual de Atividades de Auditoria Interna (PAINT).

Parágrafo único. O Comitê de Segurança da Informação (CSI) será coordenado pelo Gestor de Segurança da Informação e a sua composição estará em conformidade com o arcabouço legal vigente.

Art. 19. Compete ao Gestor de Segurança da Informação:

I. coordenar o Comitê de Segurança da Informação;
II. coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;
III. assessorar a Reitoria na implementação da Política de Segurança da Informação;
IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação junto à unidade responsável pela gestão de pessoas e desenvolvimento de carreiras;
V. 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;
VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;
VII. propor recursos necessários às ações de segurança da informação;
VIII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
IX. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
X. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
XI. manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. O Gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargo efetivo do órgão ou da entidade, com formação ou capacitação técnica compatível com as normas estabelecidas.

Art. 20. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, 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.

Art. 21. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709 (Lei Geral de Proteção de Dados - LGPD), de 14 de agosto de 2018, e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), 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.

Art. 22. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 23. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na Ufes;
II. monitorar as redes computacionais;
III. detectar e analisar ataques e intrusões;
IV. tratar incidentes de segurança da informação;
V. identificar vulnerabilidades e artefatos maliciosos;
VI. recuperar sistemas de informação;
VII. promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

Parágrafo único. A composição e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em instrução normativa específica.

Art. 24. Compete as unidades da Ufes:

I. Detectar e encaminhar ao Gestor de Segurança da Informação os casos de quebra da segurança da informação e das comunicações ocasionadas por riscos não identificados ou riscos que não foram tratados por usuários;

II. Realizar análise, avaliação e tratamento de riscos dos ativos de informação sob sua administração a partir das diretrizes estabelecidas em instruções normativas, legislação e orientações do Comitê de Segurança da Informação (CSI);

III. Contribuir para o processo de melhoria contínua da gestão de segurança da informação, monitorando e realizando análises críticas dos ativos do setor;

IV. Comunicar às partes interessadas os riscos dos ativos de informação sob a administração do setor; e

V. Comunicar ao Gestor de Segurança da Informação situações que comprometam a gestão de segurança da informação.

Art. 25. Compete aos usuários de informação:

I. Conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da Ufes;
II. Comunicar à chefia imediata ou à coordenação do curso, no caso de usuário estudante, situações de riscos que comprometam a segurança das informações da Universidade.

Parágrafo único. Todos os usuários de informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 26. A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação da Ufes.

Art. 27. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I. Tratamento da Informação;
II. Segurança Física e do Ambiente;
III. Gestão de Incidentes em Segurança da Informação;
IV. Gestão de Ativos;
V. Gestão do Uso dos Recursos Operacionais e de Comunicações, inclusive e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
VI. Controles de Acesso;
VII. Gestão de Riscos;
VIII. Gestão de Continuidade;
IX. Auditoria e Conformidade;
X. Segurança em Recursos Humanos;
XI. Desenvolvimento de Software Seguro;
XII. Licenciamento de Software; e
XIII. Cópias de Segurança (Backup).

§ 1º O Comitê de Governança Digital poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

§ 3º. A aplicação de cada uma das diretrizes deverá ser realizada após a elaboração e publicação das respectivas Instruções Normativas, aprovadas pelo Comitê de Governança Digital e emitidas pela Superintendência de Tecnologia da Informação.

Art. 28. As unidades organizacionais da Ufes devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 1º Todas as ações, realizadas pelas unidades da Ufes, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis a esta temática.

§ 2º As atividades, produtos e serviços desenvolvidos na Ufes devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

CAPÍTULO IV

DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 29. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela Ufes para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 30. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 31. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 32. As unidades organizacionais da Ufes devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 33. Os controles somente devem ser desconsiderados de formas pré-determinadas e seguras.

Parágrafo único. Procedimentos e controles alternativos devem existir para minimizar o nível de risco em emergências.

Art. 34. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação.

Art. 35. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela Ufes periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 36. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas, quando couber, conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 37. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da Ufes, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 38. As exceções a esta Política deverão sempre ter aprovação superior.

Art. 39. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Política de Segurança da Informação e seus documentos.

Art. 40. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas ao Comitê de Governança Digital.

Art. 41. Esta política entra em vigor na data de sua publicação.

gov.br Documento assinado digitalmente
ANA PAULA SANTANA DE VASCONCELLOS BITT
Data: 02/06/2025 15:12:15-0300
Verifique em https://validar.iti.gov.br

ANA PAULA SANTANA DE VASCONCELLOS BITTENCOURT

Presidente do CGD

ANEXO I - REFERÊNCIAS LEGAIS E NORMATIVAS

1.1. LEIS

LEIS		
Documento	**Fonte**	**Ano**
LEI N.º 14.133, DE 1º DE ABRIL DE 2021 Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.	PR	2021
LEI N.º 14.129, DE 29 DE MARÇO DE 2021 Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei n.º 7.116, de 29 de agosto de 1983, a Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei n.º 12.682, de 9 de julho de 2012, e a Lei n.º 13.460, de 26 de junho de 2017.	PR	2021
LEI N.º 13.874 DE 20 DE SETEMBRO DE 2019 Institui a Declaração de Direitos de Liberdade Econômica.	PR	2019
LEI Nº 13.853, DE 8 DE JULHO DE 2019 Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.	PR	2019
LEI N.º 13.709 DE 14 DE AGOSTO DE 2018 Lei Geral de Proteção de Dados Pessoais (LGPD).	PR	2018
LEI N.º 13.460 DE 26 DE JUNHO DE 2017 Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.	PR	2017

LEI N.º 13.146 DE 06 DE JULHO DE 2015 Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência).	PR	2015
LEI N.º 12.965 DE 23 DE ABRIL DE 2014 Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.	PR	2014
LEI N.º 12.682 DE 9 DE JULHO DE 2012 Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.	PR	2012
LEI N.º 12.527 DE 18 DE NOVEMBRO DE 2011 Lei de Acesso à Informação (LAI).	PR	2011
LEI N.º 10.436 DE 24 DE ABRIL DE 2002 Dispõe sobre a Língua Brasileira de Sinais - Libras	PR	2002
LEI N.º 10.098 DE 19 DE DEZEMBRO DE 2000 Estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida.	PR	2000
LEI N.º 9.610 DE 19 DE FEVEREIRO DE 1998 Altera, atualiza e consolida a legislação sobre direitos autorais.	PR	1998

1.2. DECRETOS

DECRETOS		
Documento	**Fonte**	**Ano**
DECRETO Nº 12.198, DE 24 DE SETEMBRO DE 2024 Institui a Estratégia Federal de Governo Digital para o período de 2024 a	PR	2024

2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.		
DECRETO N.º 12.069, DE 21 DE JUNHO DE 2024 Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital – Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027.	PR	2024
DECRETO N.º 11.856 DE 26 DE DEZEMBRO DE 2023 Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.	PR	2023
DECRETO N.º 10,748 DE 16 DE JULHO DE 2021 Institui a Rede Federal de Gestão de Incidentes Cibernéticos.	PR	2021
DECRETO N.º 10.403 DE 19 DE JUNHO DE 2020 Altera o Decreto n.º 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.	PR	2020
DECRETO N.º 10.278 DE 18 DE MARÇO DE 2020 Regulamenta o disposto no inciso X do caput do art. 3º da Lei n.º 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei n.º 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais.	PR	2020
DECRETO N.º 10.046 DE 09 DE OUTUBRO DE 2019 Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.	PR	2019
DECRETO N.º 9.903 DE 08 DE JULHO DE 2019 Altera o Decreto n.º 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo federal, para dispor sobre a gestão	PR	2019

e os direitos de uso de dados abertos.		
DECRETO N.º 9.854 DE 25 DE JUNHO DE 2019 Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.	PR	2019
DECRETO N.º 9.756 DE 11 DE ABRIL DE 2019 Institui o portal único "gov.br" e dispõe sobre as regras de unificação dos canais digitais do Governo federal.	PR	2019
DECRETO N.º 9.723 DE 11 DE MARÇO DE 2019 Altera o Decreto n.º 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto n.º 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo da apresentação de outros documentos do cidadão no exercício de obrigações e direitos ou na obtenção de benefícios e regulamentar dispositivos da Lei n.º 13.460, de 26 de junho de 2017.	PR	2019
DECRETO N.º 9.637 DE 26 DE DEZEMBRO DE 2018 Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto n.º 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n.º 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.	PR	2018
DECRETO N.º 9.319 DE 21 DE MARÇO DE 2018 Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital.	PR	2018
DECRETO N.º 9.094 DE 17 DE JULHO DE 2017 Regulamenta dispositivos da Lei n.º 13.460, de 26 de junho de 2017, dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos, institui o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo para a apresentação de dados do cidadão no exercício de obrigações e direitos e na obtenção de benefícios,	PR	2017

ratifica a dispensa do reconhecimento de firma e da autenticação em documentos produzidos no País e institui a Carta de Serviços ao Usuário.		
DECRETO Nº 8.936 DE 19 DE DEZEMBRO DE 2016 Institui a Plataforma de Cidadania Digital e dispõe sobre a oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.	PR	2016
DECRETO Nº 8.777 DE 11 DE MAIO DE 2016 Institui a Política de Dados Abertos do Poder Executivo federal.	PR	2016
DECRETO Nº 7.724 DE 16 DE MAIO DE 2012 Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.	PR	2012
DECRETO Nº 7.579 DE 11 DE OUTUBRO DE 2011 Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal.	PR	2011
DECRETO Nº 7.174 DE 12 DE MAIO DE 2010 Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.	PR	2010
DECRETO Nº 6.949 DE 25 DE AGOSTO DE 2009 Promulga a Convenção Internacional sobre os Direitos das Pessoas com Deficiência e seu Protocolo Facultativo, assinados em Nova York, em 30 de março de 2007.	PR	2009
DECRETO Nº 5.626 DE 22 DE DEZEMBRO DE 2005 Regulamenta a Lei nº 10.436, de 24 de abril de 2002, que dispõe sobre a Língua Brasileira de Sinais - Libras, e o art. 18 da Lei nº 10.098, de 19 de dezembro de 2000.	PR	2005
DECRETO Nº 5.296 DE 02 DE DEZEMBRO DE 2004	PR	2004

Regulamenta as Leis nos 10.048, de 8 de novembro de 2000, que dá prioridade de atendimento às pessoas que especifica, e 10.098, de 19 de dezembro de 2000, que estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida, e dá outras providências.		
DECRETO-LEI Nº 200 DE 25 DE FEVEREIRO DE 1967 Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências.	PR	1967

1.3. PORTARIAS

PORTARIAS		
Documento	**Fonte**	**Ano**
PORTARIA NORMATIVA Nº 198, DE 19 DE SETEMBRO DE 2024 Código de Ética da Ufes.	Ufes	2024
PORTARIA SGD/MGI Nº 4.248, DE 26 DE JUNHO DE 2024 Estabelece recomendações para o alcance dos objetivos da Estratégia Nacional de Governo Digital para o período de 2024 a 2027.	SGD/MGI	2024
PORTARIA-TCU Nº 170, DE 31 DE OUTUBRO DE 2023 Dispõe sobre a atuação do Tribunal de Contas da União no âmbito do Programa Nacional de Prevenção à Corrupção (PNPC).	TCU	2023
PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023 Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.	SGD/MGI	2023
PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022 Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal.	GSI/PR	2022

PORTARIA MCOM Nº 2.382 DE 9 DE ABRIL DE 2021 Aprova o Guia de Estilo para o novo Portal Institucional denominado "gov.br".	MCOM	2021
PORTARIA Nº 1.915 SEI-MCOM DE 28 DE JANEIRO DE 2021 Aprova o Guia de Transformação Digital para o Portal "gov.br".	MCOM	2021
PORTARIA Nº 1.914 SEI-MCOM DE 28 DE JANEIRO DE 2021 Aprova o Manual de Uso da Marca "gov.br".	MCOM	2021
PORTARIA Nº 540 DE 8 DE SETEMBRO DE 2020 Disciplina a implantação e a gestão do Padrão Digital de Governo dos órgãos e entidades do Poder Executivo federal.	PR	2020
PORTARIA Nº 485 DE 28 DE AGOSTO DE 2020 Aprova o Manual de SEO - Otimização de Mecanismos de Buscas, para o novo Portal Institucional denominado Gov.Br.	MCOM	2020
PORTARIA Nº 484 DE 28 DE AGOSTO DE 2020 Aprova o Manual de Migração que trata da transferência do conteúdo dos portais do Governo federal para o novo Portal Institucional denominado Gov.Br.	MCOM	2020
PORTARIA Nº 483 DE 28 DE AGOSTO DE 2020 Aprova o Manual de Diretrizes para a padronização dos portais do Governo federal no novo Portal Institucional denominado Gov.Br.	MCOM	2020
PORTARIA Nº 482 DE 28 DE AGOSTO DE 2020 Aprova o Manual de Publicação que trata das ferramentas de administração e publicação de conteúdos no âmbito do Portal Institucional do Governo Federal.	MCOM	2020
PORTARIA Nº 15.543, DE 2 DE JULHO DE 2020 Divulga o Manual de Conduta do Agente Público Civil do Poder Executivo Federal.	ME	2020

PORTARIA Nº 13.420 DE 2 DE JUNHO DE 2020 Revoga a Portaria n.º 58, de 23 de dezembro de 2016, da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão, que dispõe sobre procedimentos complementares para o compartilhamento de bases de dados oficiais entre órgãos e entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União.	SGD/MGI	2020
PORTARIA Nº 11.551 DE 8 DE MAIO DE 2020 Subdelega competência para publicação de resoluções do Comitê Central de Governança de Dados - CCDG à Secretaria de Governo Digital da Secretaria Especial de Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.	ME	2020
PORTARIA Nº 41 DE 3 DE SETEMBRO DE 2019 Declara a alteração e a revogação de atos normativos, para fins do disposto no art. 9º do Decreto n.º 9.759, de 11 de abril de 2019 (Revoga a Coordenação do Modelo de Acessibilidade em Governo Eletrônico – e-MAG e a Comissão de coordenação dos Padrões de Interoperabilidade de Governo Eletrônico - e-PING).	SGD/MGI	2019
PORTARIA Nº 39 DE 9 DE JULHO DE 2019 Dispõe sobre procedimentos para a unificação dos canais digitais e define regras para o procedimento de registro de endereços de sítios eletrônicos na internet e de aplicativos móveis do Governo Federal.	ME	2019
PORTARIA Nº 778 DE 4 DE ABRIL DE 2019 Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.	ME	2019
PORTARIA Nº 23 DE 4 DE ABRIL DE 2019 Dispõe sobre diretrizes, competências e condições para adesão à Rede Nacional de Governo Digital.	ME	2019
PORTARIA CONJUNTA Nº 6 DE 14 DE MARÇO DE 2019	ME	2019

Institui o Programa de Desenvolvimento de Capacidades para Transformação Digital no Poder Executivo federal.		
PORTARIA INTERMINISTERIAL Nº 176 DE 25 DE JUNHO DE 2018 Dispõe sobre a vedação de exigência de documentos de usuários de serviços públicos por parte de órgãos e entidades da Administração Pública federal.	MPDG	2018
PORTARIA INTERMINISTERIAL Nº 1 DE 12 DE JANEIRO DE 2017 Dispõe sobre procedimentos para a elaboração e a publicação dos relatórios circunstanciados, previstos no art. 120 da Lei n.º 13.146, de 6 de julho de 2015, sobre a situação de acessibilidade em sítios, portais, sistemas e serviços mantidos na internet pelos órgãos do governo pertencentes à Administração Pública Federal e as devidas providências a serem adotadas para melhoria da acessibilidade desses ambientes digitais.	MJC-MPDG	2017
PORTARIA SLTI-MPOG Nº 92 DE 24 DE DEZEMBRO DE 2014 Institui a ePING	SLTI	2014
PORTARIA Nº 11 SLTI DE 30 DE DEZEMBRO DE 2008 Estratégia Geral de Tecnologia da Informação 2008.	SLTI	2008
PORTARIA Nº 3 DE 7 DE MAIO DE 2007 Institucionaliza o Modelo de Acessibilidade em Governo Eletrônico – e-MAG no âmbito do Sistema de Administração dos Recursos de Informação e Informática – SISP.	SLTI	2007
PORTARIA NORMATIVA Nº 5 DE 14 DE JULHO DE 2005 Institucionaliza os Padrões de Interoperabilidade de Governo Eletrônico - e-PING, no âmbito do Sistema de Administração dos Recursos de Informação e Informática – SISP, cria sua Coordenação, definindo a competência de seus integrantes e a forma de atualização das versões do Documento.	SLTI	2005

1.4. RESOLUÇÕES

RESOLUÇÕES		
Documento	**Fonte**	**Ano**
RESOLUÇÃO Nº 3 DE 13 DE OUTUBRO DE 2017 Aprova as normas sobre elaboração e publicação de Planos de Dados Abertos, conforme disposto no Decreto nº8.777, de 11 de maio de 2016.	MPDG	2017
RESOLUÇÃO Nº 2 DE 24 DE MARÇO DE 2017 Aprova os Termos de Uso do Portal Brasileiro de Dados Abertos.	MPDG	2017

1.5. INSTRUÇÕES NORMATIVAS

INSTRUÇÕES NORMATIVAS		
Documento	**Fonte**	**Ano**
INSTRUÇÃO NORMATIVA SGD-ME Nº 128 DE 28 DE DEZEMBRO DE 2020 Dispõe sobre as condições a serem observadas pelas empresas públicas e sociedades de economia mista para a adesão ao Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, nos termos do art. 1º, parágrafo único, do Decreto n.º 7.579, de 11 de outubro de 2011.	SGD/ME	2020
INSTRUÇÃO NORMATIVA SGD-ME Nº 202 DE 18 DE SETEMBRO DE 2019 Altera a Instrução Normativa n.º 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.	SGD/SEDGGD/ME	2019
INSTRUÇÃO NORMATIVA Nº 8 DE 27 DE NOVEMBRO DE 2018 Altera a Instrução Normativa SECOM-PR nº 08, de 19 de dezembro de 2014.	PR	2018

INSTRUÇÃO NORMATIVA Nº 5 DE 18 DE JUNHO DE 2018 Estabelece orientações para a atuação das unidades de ouvidoria do Poder Executivo federal para o exercício das competências definidas pelos capítulos III e IV da Lei n.º 13.460, de 26 de junho de 2017.	MTCG/OGG	2018
INSTRUÇÃO NORMATIVA SEGES-MP Nº 5 DE 26 DE MAIO DE 2017 Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.	MPDG	2017
INSTRUÇÃO NORMATIVA SECOM-PR Nº 8 DE 19 DE DEZEMBRO DE 2014 Disciplina a implantação e a gestão da Identidade Padrão de Comunicação Digital das propriedades digitais dos órgãos e entidades do Poder Executivo Federal e dá outras providências.	SECOM	2014
INSTRUÇÃO NORMATIVA Nº 4 DE 13 DE ABRIL DE 2012 Institui a Infraestrutura Nacional de Dados Abertos – INDA.	SLTI	2012
INSTRUÇÃO NORMATIVA Nº 3 DE 27 DE MARÇO DE 2012 Dispõe sobre as condições a serem observadas pelas empresas públicas e sociedades de economia mista para a adesão ao Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp, nos termos do art. 1º, parágrafo único, do Decreto n.º 7.579, de 11 de outubro de 2011.	SLTI	2012
INSTRUÇÃO NORMATIVA Nº 1 DE 17 DE JANEIRO DE 2011 Dispõe sobre os procedimentos para o desenvolvimento, a disponibilização e o uso do Software Público Brasileiro – SPB.	SLTI	2011
INSTRUÇÃO NORMATIVA Nº 1 DE 19 DE JANEIRO DE 2010 Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.	SLTI	2010
INSTRUÇÃO NORMATIVA 01-2009 GSI DE 13 DE JUNHO DE 2008 Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras	PR	2008

providências.		

1.6. NORMAS COMPLEMENTARES

NORMAS COMPLEMENTARES		
Documento	**Fonte**	**Ano**
NORMA COMPLEMENTAR 04-2009 DE 14 DE AGOSTO DE 2009 Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.	PR	2009