Ato Normativo	Ementa / Explicação
Resolução MCTI nº 2, de 6 de outubro de 2026 DOU 1 Extra A de 09/11/2026 Visualizar medida	*"Institui **grupos técnicos permanentes** no âmbito do **Comitê Nacional de Iniciativas de Apoio a Startups e ao Empreendedorismo Inovador**."* **Explicação**: institui **dois grupos técnicos permanentes de caráter consultivo** e **propositivo** no âmbito do **Comitê Nacional de Iniciativas de Apoio a Startups e ao Empreendedorismo Inovador**. O primeiro é o **Grupo Técnico do Marco Legal**, que foca na **implementação e no aperfeiçoamento das leis e normas sobre startups e inovação**. Competirá ao grupo acompanhar a execução do Marco Legal das Startups e **identificar as necessidades de regulamentação**, além de elaborar estudos e propostas para novas medidas legislativas e decretos. Seu escopo inclui **identificar barreiras regulatórias para promover a segurança jurídica**, **harmonizar a legislação do setor com normas de outras áreas** – *como contratações públicas e mercado de capitais* – e **mapear as lacunas** que afetam as *deep techs* para propor soluções. O segundo é o **Grupo Técnico de Articulação e Avaliação**, responsável por acompanhar e aperfeiçoar as políticas, os programas e as iniciativas federais de apoio ao setor. Ele promoverá a **integração das ações**, o **compartilhamento de boas práticas entre o poder público e o ecossistema** e o **desenvolvimento de indicadores para avaliar os impactos dos instrumentos de fomento**. Além disso, executará **metodologias para o mapeamento dinâmico do ecossistema nacional**, acompanhamento das **etapas de desenvolvimento dos empreendimentos** e articulação do setor com estratégias nacionais de economia de impacto e desenvolvimento sustentável. A composição dos grupos irá reunir representantes de Ministérios, **agências de fomento**, instituições financeiras, universidades, **setor produtivo**, investidores e **organizações da sociedade civil**. Por fim, os grupos devem organizar planos de trabalho próprios e podem formar **subgrupos temáticos com prazo determinado para aprofundar temas específicos**.

Solução de Consulta RFB nº 219, de 6 de novembro de 2026

Visualizar medida

Assunto: **Contribuições Sociais Previdenciárias**

Reoneração da folha de pagamento. Período de transição (2025 a 2027). **Contribuição previdenciária sobre a receita bruta** (CPRB). Retenção na contratação de serviços. Cessão de mão de **obra**. Alíquota aplicável. Lei nº 14.973/2024.

Entre 1º de janeiro de 2025 e 31 de dezembro de 2027, no caso de **contratação de empresas que estejam legalmente sujeitas à CPRB para execução de serviços** mediante cessão de mão de obra, a empresa contratante deverá reter 3,5% do valor bruto da nota fiscal ou da fatura de prestação de serviços.

A partir de **1º de janeiro de 2028**, será de **11 % a alíquota de retenção da contribuição previdenciária incidente sobre o valor bruto da nota fiscal ou da fatura de prestação de serviços**.

Na hipótese de **não haver opção pela CPRB**, ou se a opção não for regular, a alíquota de retenção da contribuição previdenciária aplicável é de 11% incidente sobre o valor bruto da nota fiscal ou da fatura de prestação de serviços.

Portaria CADE nº 487, de 27 de outubro de 2026

Visualizar medida

*"Institui a **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR** do Conselho Administrativo de Defesa Econômica - Cade e aprova seu Regimento Interno."*

Explicação: institui formalmente a **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos** (**ETIR**) no âmbito do CADE, com a finalidade de **coordenar e executar ações de prevenção, detecção, tratamento e resposta a incidentes que possam comprometer os ativos de informação e a continuidade dos serviços do órgão**.

A equipe deverá atuar em conformidade com a Política de Segurança da Informação (**Posin**) do CADE e com as normas aplicáveis à gestão de incidentes cibernéticos na Administração Pública Federal.

O **público atendido** pela ETIR **compreende as unidades administrativas, os agentes públicos, os colaboradores, os prestadores de serviços e os demais usuários autorizados dos ativos de informação e dos serviços de tecnologia da informação e comunicação do CADE.**

Entre as principais atribuições da ETIR estão:

- **Planejar e executar atividades de prevenção, tratamento e resposta a incidentes de segurança cibernética**

- Receber, analisar e notificar eventos adversos à segurança da informação, inclusive aqueles sob suspeita, promovendo as medidas corretivas e preventivas necessárias.
- Monitorar alertas, vulnerabilidades e ameaças cibernéticas, recomendando medidas de prevenção e correção.

A ETIR ficará **vinculada institucionalmente à Coordenação-Geral de Tecnologia da Informação (CGTI), com suporte técnico e operacional do Serviço de Segurança da Informação e Comunicação (Sesic).**

Sua composição será formada pelos ocupantes dos seguintes cargos ou funções:

- Chefe do Serviço de Segurança da Informação e Comunicação (**Sesic**), como Agente Responsável pela ETIR;
- Chefe do Serviço de Infraestrutura de Redes (**Sesin**);
- Chefe do Serviço de Gestão e Governança (**Segov**);
- Chefe do Serviço de Desenvolvimento de Sistemas (**Sesis**);
- Chefe do Serviço de Dados (**Sedados**).

Estabelece o **Modelo 1 de implementação, no qual os integrantes pertencem às equipes internas de tecnologia da informação e comunicação e desempenham as atividades da ETIR** cumulativamente com suas atribuições regulares, sem dedicação exclusiva.

Os incidentes serão **classificados em quatro níveis de gravidade**: crítico, alto, médio e baixo. A classificação deverá considerar a abrangência da ocorrência, a criticidade dos ativos afetados, os impactos sobre a disponibilidade, integridade, confidencialidade e autenticidade das informações e o risco de agravamento.

Adotará o **modelo de autonomia compartilhada**, pelo qual participará do processo decisório, apresentando recomendações técnicas e atuando conjuntamente com as unidades competentes na definição das medidas de contenção, resposta e recuperação.

Em situações de crise, interrupção relevante de serviços ou impacto institucional significativo, o processo decisório deverá envolver obrigatoriamente:

- Agente Responsável pela ETIR;
- Gestor de Segurança da Informação;
- Coordenador-Geral de Tecnologia da Informação.

A decisão sobre as medidas a serem adotadas no âmbito da CGTI caberá ao Coordenador-Geral de Tecnologia da Informação. Já as medidas que ultrapassarem as competências da Coordenação ou produzirem repercussão institucional ampla serão decididas pela autoridade máxima do CADE.

A Portaria entrou em vigor na data de sua publicação. **Não estabelece prazo específico para implementação da equipe ou para adequação de terceiros.**

Portaria CADE nº 488, de 27 de outubro de 2026

Visualizar medida

*"Institui a **Política de Segurança da Informação** - Posin no âmbito do Conselho Administrativo de Defesa Econômica - Cade."*

Explicação: a política tem como objetivo **assegurar a confidencialidade, a integridade e a disponibilidade das informações institucionais**, estabelecendo regras para o tratamento, armazenamento, compartilhamento, transmissão e descarte de dados, além de **procedimentos para prevenção e resposta a incidentes de segurança da informação**.

É aplicada a **todos os ativos de informação do CADE, incluindo dados, sistemas, documentos, dispositivos, computadores e infraestrutura de redes**. Sua abrangência também alcança qualquer pessoa ou entidade que acesse, processe ou manuseie informações sob a custódia da autarquia, incluindo servidores, colaboradores, parceiros, prestadores de serviços e terceiros.

Estabelece que a **proteção das informações é uma responsabilidade compartilhada entre gestores**, usuários e demais agentes envolvidos, que devem adotar medidas técnicas e administrativas compatíveis com o grau de sensibilidade e criticidade das informações.

Todos os **colaboradores do CADE devem conhecer e cumprir integralmente a política e seus normativos complementares**.

Também torna obrigatória a participação nas ações de conscientização e capacitação sobre segurança da informação e proteção de dados promovidas pela autarquia.

Entre as principais determinações, destacam-se:

- **Prevenção de ameaças cibernéticas:** os usuários devem desenvolver capacidade de identificar ameaças como *phishing*, *spam*, engenharia social e outros artefatos maliciosos, comunicando imediatamente qualquer suspeita ao Serviço de Segurança da Informação e Comunicação (Sesic).
- **Controle de acessos:** o acesso a sistemas, informações e demais recursos institucionais deve observar o princípio do menor privilégio, concedendo aos usuários apenas as permissões necessárias ao exercício de suas funções.
- **Uso de equipamentos e softwares:** fica proibida a instalação, desinstalação ou utilização de *softwares* em equipamentos institucionais sem autorização formal prévia

da Coordenação-Geral de Tecnologia da Informação (CGTI). Também é vedada a conexão de dispositivos físicos não autorizados à infraestrutura do CADE e a modificação de hardware ou software sem homologação e autorização formal.

O **cumprimento da política será avaliado periodicamente pelo CADE**, por meio de verificações formais de conformidade, destinadas a verificar o atendimento aos requisitos de segurança da informação e a efetividade das cláusulas de responsabilidade e sigilo previstas em contratos, convênios, acordos e instrumentos semelhantes.

O **descumprimento da política e de seus normativos complementares poderá resultar na aplicação de sanções administrativas**, sem prejuízo da apuração de responsabilidades nas esferas civil e penal. Deverão ser assegurados o contraditório e a ampla defesa.

Portaria CADE nº 489, de 27 de outubro de 2026

Visualizar medida

*"Institui a **Política de Conscientização em Segurança da Informação** no âmbito do Conselho Administrativo de Defesa Econômica - Cade."*

Explicação: institui a Política de Conscientização em Segurança da Informação no âmbito do Conselho Administrativo de Defesa Econômica (**CADE**), com a **finalidade de fortalecer a cultura institucional de segurança da informação e reduzir riscos relacionados a falhas humanas, incidentes cibernéticos e uso inadequado de informações e recursos tecnológicos.**

A política integra os **instrumentos de governança da informação do órgão e aplica-se aos agentes públicos** que exerçam atividades ou tenham acesso a informações, ambientes, sistemas ou outros ativos do CADE.

Entre seus **objetivos** estão **promover ações contínuas de sensibilização e capacitação, assegurar a compreensão das responsabilidades relacionadas à segurança da informação e fortalecer a capacidade institucional de prevenir, identificar e responder a incidentes.**

Estabelece a execução de um **Programa de Conscientização em Segurança da Informação**, que deverá ser contínuo e planejado anualmente.

O planejamento será consolidado em uma **Matriz Anual** de Conteúdos e Ações, que deverá indicar:

- Objetivos e necessidades a serem atendidos;
- Temas e conteúdos previstos;
- Ações, modalidades e públicos destinatários;
- Responsáveis e períodos de realização;

- Metas, indicadores e resultados esperados.

A matriz poderá ser atualizada ao longo do exercício em razão de riscos, incidentes ou alterações normativas, institucionais e tecnológicas.

As ações previstas poderão incluir orientações para novos servidores ou agentes que assumam novas funções, capacitações, campanhas periódicas, simulações, exercícios e divulgação de normas e orientações de segurança da informação.

A política organiza as ações de capacitação em trilhas gerais e específicas, de acordo com as atribuições e responsabilidades dos agentes públicos.
Na trilha geral, estão previstos os seguintes temas:

- Normas, responsabilidades e boas práticas de segurança da informação;
- Prevenção contra engenharia social, phishing e spam;
- Uso seguro de identidades, credenciais, correio eletrônico, internet, redes e dispositivos;
- Classificação, acesso, proteção e tramitação de documentos e informações, observando a Lei de Acesso à Informação (Lei nº 12.527/2011);
- Proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- Uso seguro, ético e responsável de ferramentas de inteligência artificial, com proteção das informações institucionais e supervisão humana;
- Prevenção, identificação e comunicação de vulnerabilidades, eventos e incidentes de segurança da informação.

Para os profissionais de Tecnologia da Informação e Comunicação (**TIC**), estão **previstas capacitações específicas sobre gestão de riscos, vulnerabilidades, acessos e incidentes; segurança de infraestrutura, aplicações, dados e serviços em nuvem; desenvolvimento seguro de software; análise de registros de segurança; continuidade e recuperação de serviços.**

A Portaria **não estabelece prazo específico** para a primeira execução das ações nem fixa um cronograma de implementação inicial.

Portaria MTUR nº 36, de 9 de novembro de 2026

DOU 1 Extra A – 09/11/2026

Visualizar medida

"*Estabelece os **projetos e as ações prioritárias, estruturantes e de interesse nacional ou regional passíveis de financiamento** por **emendas individuais (RP 6), de bancada estadual (RP 7) e de comissão (RP 8),** bem como os critérios e as orientações para a **execução dessas programações no***

***exercício de 2027**, nas ações orçamentárias sob gestão do **Ministério do Turismo** e de suas entidades vinculadas.*"

Explicação: detalha **as ações orçamentárias elegíveis e as modalidades de emendas admitidas** (RP 6, RP 7 e RP 8), **os critérios de execução e elegibilidade dos projetos, ações e objetos financiáveis**, incluindo valores de referência, equipamentos públicos passíveis de destinação e obrigações legais aplicáveis. Também relaciona os projetos da carteira do Ministério do Turismo (**MTur**) **situados em regiões metropolitanas ou RIDEs e as obras inacabadas de exercícios anteriores consolidadas no Obrasgov.br, financiadas por emendas de bancada estadual ou de comissão.**

Estabelece **cinco eixos estratégicos** para o enquadramento dos projetos e ações financiados por emendas parlamentares no âmbito do MTur: **(i)** infraestrutura turística; **(ii)** mobilidade e conectividade; **(iii)** sustentabilidade, qualidade e responsabilidade no turismo; **(iv)** planejamento, inteligência, inovação e desenvolvimento do setor; e **(v)** promoção, comercialização e posicionamento de destinos turísticos**.**

Os projetos apoiados pelo Ministério do Turismo deverão demonstrar:

- **aderência a pelo menos um dos eixos estratégicos**;
- **alinhamento com a Política Nacional de Turismo e com o Plano Nacional de Turismo vigente**; e
- **compatibilidade do objeto com a finalidade e os atributos da ação orçamentária,** com o respectivo subtítulo e com os demais classificadores da despesa.

A execução de emendas parlamentares em projetos de investimento em obras ou serviços de engenharia, inclusive na elaboração dos respectivos projetos, **fica condicionada ao prévio registro do projeto no Cadastro Integrado de Projetos de Investimento - Obrasgov.br**.

Vincula a continuidade das obras plurianuais iniciadas com recursos de emendas de bancada estadual em exercícios anteriores à apresentação de novas emendas pela mesma bancada até sua conclusão, conforme projetos relacionados no Anexo IV, com identificação dos empreendimentos, códigos e respectivas bancadas no CIPI/ObrasGov.

Para fins de alocação das emendas de comissão, consideram-se projetos e ações de interesse:

- **nacional, aqueles que envolvam:** mais de uma região geográfica; ou o território nacional e algum país fronteiriço;
- **regional, aqueles que envolvam:** mais de uma Região Geográfica Imediata (**RGI**), nos termos da divisão regional

	estabelecida pelo IBGE; ou mais de uma Unidade da Federação. Determina que **o MTur divulgue, em seu sítio eletrônico oficial, os prazos e procedimentos para apresentação de propostas e planos de trabalho, bem como informações sobre a execução das programações**, em conformidade com as exigências de transparência e rastreabilidade da Lei Complementar nº 210/2024. Por fim, restringe a aplicação dos recursos de emendas de bancada e de comissão aos objetos aprovados, vedando despesas ordinárias sem vínculo direto com sua execução, e estabelece a aplicação da Portaria às programações orçamentárias de 2027.
Resolução CGD/IBAMA nº 9, de 29 de outubro de 2026 Visualizar medida	*"**Prorroga** a **vigência** do **Plano Diretor de Tecnologia da Informação e Comunicação** - PDTIC 2024-2026 do **Ibama até 31 de dezembro de 2026**."* **Explicação**: prorroga a vigência do Plano Diretor de Tecnologia da Informação e Comunicação (**PDTIC 2024-2026**) do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (**Ibama**), até **31 de dezembro de 2026**. Ademais, determina que a Equipe de Elaboração do PDTIC (**EqEPDTIC**) fica **responsável por concluir a elaboração do PDTIC 2027-2028 até 31 de dezembro de 2026**, observadas as diretrizes do **Guia de Elaboração do PDTIC** do Ministério da Gestão e da Inovação em Serviços Públicos (**MGI**) e demais normativos aplicáveis, de modo que o novo plano entre em vigor em **1º de janeiro de 2027**.

Ato de Pessoal	Objetivo
Portaria de Pessoal SSC/MGI nº 13.499, de 9 de novembro de 2026 Visualizar medida	**Dispensar**: Pedro Iago Carvalho Martins da função de **coordenador de Uso Responsável em Capacitação em Inteligência Artificial** da Coordenação-Geral de Governança de Inteligência Artificial da Diretoria de Estruturação de Dados e Inteligência Artificial da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (**MGI**), FCE 1.10.

Observação: É possível ter acesso aos textos das íntegras das medidas por meio do link localizado abaixo da identificação de cada ato.