03800.201568/15-11

RESOLUÇÃO CGPAR Nº 11 , DE 10 DE maio DE 2016.

A **COMISSÃO INTERMINISTERIAL DE GOVERNANÇA CORPORATIVA E DE ADMINISTRAÇÃO DE PARTICIPAÇÕES SOCIETÁRIAS DA UNIÃO – CGPAR**, no uso das atribuições que lhe conferem os arts. 3º e 7º do Decreto nº 6.021, de 22 de janeiro de 2007, e tendo em vista proposição do Grupo Executivo – GE, aprovada conforme Ata de sua 78ª Reunião Ordinária, realizada no dia 22 de junho de 2015,

RESOLVE:

Art. 1º As empresas estatais federais devem planejar, implementar e manter práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área.

§ 1º A adoção das práticas de que trata o **caput** deste artigo deve ser compatível com o porte da empresa estatal, a natureza das operações, o ambiente de negócio em que está inserida, o grau de sigilo de suas informações, a complexidade de sua estrutura organizacional e de tecnologia da informação, bem como de suas práticas de aquisição, desenvolvimento e manutenção de sistemas.

§ 2º A aplicação desta Resolução deve envolver as áreas responsáveis pelos diversos processos, alguns dos quais são relacionados, porém não subordinados, diretamente à área de TI.

Art. 2º As práticas de governança de TI devem incluir:

I – elaboração e acompanhamento de Plano Estratégico de Tecnologia da Informação (PETI), aderente ao Plano Estratégico Institucional (PEI), dando-lhe ampla divulgação, à exceção de informações classificadas como não públicas, nos termos da lei;

II – elaboração e acompanhamento de Plano Diretor de Tecnologia da Informação (PDTI), aderente ao PETI, dando-lhe ampla divulgação, à exceção de informações classificadas como não públicas, nos termos da lei;

III – definição e acompanhamento de indicadores e metas ligadas ao planejamento de TI, baseados em parâmetros de governança e nas necessidades do negócio;

IV – estabelecimento de colegiado de nível estratégico de TI, formado por representantes da alta administração, incluindo ao menos um Diretor estatutário, responsável por assegurar a adoção de práticas estabelecidas nesta Resolução, pelo direcionamento estratégico de TI, e pela avaliação de seus principais investimentos;

V – estabelecimento de colegiado de nível tático, responsável, ao menos, pela definição dos investimentos seguindo as prioridades estabelecidas pelo colegiado de nível estratégico, pelo monitoramento de projetos e solução de conflitos, e pelo monitoramento dos níveis de serviço de TI e de sua melhoria;

RATIA
PGFN/CAS

VI – definição de processos críticos de negócio, com identificação dos gestores responsáveis pelos sistemas de informação que dão suporte a esses processos;

VII – formalização de processos de gestão de serviços internos de TI, incluindo, ao menos, gestão de configuração, gestão de incidentes, gestão de mudança e gestão de continuidade de negócios;

VIII – formalização de processo de gerenciamento de projetos;

IX – formalização de processo de **software**;

X – formalização e execução de políticas de segurança da informação, incluindo, ao menos:

a) a classificação das informações pelas respectivas áreas de negócio e a disponibilização, pela TI, de ambientes com o nível de segurança necessário ao seu armazenamento;
b) o controle de acesso local e remoto às redes de dados;
c) o controle de acesso aos sistemas;
d) o controle de acesso físico aos equipamentos de TI;
e) o uso de unidades portáteis de armazenamento de dados e de computadores portáteis; e
f) a existência de rastro de auditoria (*log*) em sistemas críticos;

XI – definição dos requisitos e competências necessárias para acesso às funções de liderança na área de Tecnologia da Informação;

XII – realização periódica de avaliações qualitativas e quantitativas do pessoal da área de TI, determinando as necessidades de recursos humanos do setor e mantendo, caso necessário, plano de capacitação voltado a este tema;

XIII – estabelecimento de processo formal para contratação e gestão de soluções de TI, aderente, no que couber, às definições da IN-SLTI/MP nº 4/2014 ou de normativos que vierem a sucedê-la;

XIV – obrigatoriedade da vinculação de um processo de **software** a todos os contratos de desenvolvimento e manutenção de sistemas; e

XV – mapeamento e gestão dos riscos relevantes ligados à TI.

§ 1º Para o cumprimento do estabelecido nos incisos VIII e IX, as empresas podem optar pela adoção das metodologias mantidas pelo Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Governo Federal.

§ 2º Para o cumprimento do estabelecido no inciso XIV, as empresas podem optar pela vinculação de processo de **software** utilizado por seu fornecedor, desde que adequadamente detalhado e formalizado em contrato.

Art. 3º Devem ser estabelecidos procedimentos de controles internos, abrangendo os diversos níveis da organização, visando mitigar os riscos ligados, ao menos, aos seguintes processos:

I – Planejamento Estratégico Institucional (PEI);

KÁTIA
PGFN/CAS

II – Planejamento Estratégico de TI (PETI);

III – Plano Diretor de TI (PDTI);

IV – funcionamento de comitês e fóruns ligados a TI;

V – processo orçamentário de TI;

VI – processo de **software**;

VII – gerenciamento de projetos de TI;

VIII – gerenciamento de serviços de TI;

IX – segurança da informação;

X – gestão de pessoal de TI;

XI – contratação e gestão de soluções de TI;

XII – monitoramento do desempenho da TI organizacional.

Parágrafo único. Os controles internos devem ser periodicamente revisados e atualizados, de forma a serem incorporadas medidas relacionadas a riscos novos ou anteriormente não abordados.

Art. 4º No caso de empresas estatais pertencentes a um mesmo grupo, as práticas de governança de TI e os controles internos relacionados poderão ser definidos e mantidos:

I – individualmente, no âmbito de cada empresa; ou

II – total ou parcialmente centralizados em uma das empresas que compõe o grupo, desde que não haja perda de efetividade.

Parágrafo único. A faculdade estabelecida no inciso II do **caput** deverá ser exercida, preferencialmente, pela empresa controladora do grupo ou por empresa especializada em tecnologia da informação, e esta deverá ter ascendência sobre as demais empresas que compõem o grupo em relação aos processos que centraliza.

Art. 5º As práticas de governança de TI e os controles internos relacionados deverão ser implementados até:

I – 1 (um) ano, após a publicação desta Resolução, no caso das empresas Petrobras, Eletrobrás, Banco do Brasil, Caixa Econômica Federal, BNDES, Banco da Amazônia, Banco do Nordeste do Brasil, Serpro e Dataprev, bem como das empresas controladas direta ou indiretamente por elas; e

II – 2 (dois) anos, após a publicação desta Resolução, no caso das demais empresas estatais federais.

KÁTIA
GFN/CAS

Art. 6º A Auditoria Interna das empresas estatais federais e os órgãos de controle e fiscalização da Administração Federal deverão incluir, no escopo de seus trabalhos, no que couber, a verificação quanto à observância pelas empresas desta Resolução.

Art. 7º Fica o Departamento de Coordenação e Governança das Empresas Estatais (DEST) autorizado a baixar normas complementares a esta Resolução, incluindo a alteração do cronograma estabelecido no art. 5º.

Art. 8º Esta Resolução entra em vigor na data de sua publicação.

Brasília, 20 de maio de 2016; 195º da Independência e 128º da República.

VALDIR MOYSÉS SIMÃO
Ministro de Estado do Planejamento, Orçamento e Gestão
Presidente

NELSON BARBOSA
Ministro de Estado da Fazenda
Membro

EVA MARIA CELLA DAL CHIAVON
Ministra de Estado Chefe da Casa Civil da Presidência da República, Substituta
Membro

GABINETE DO MINISTRO - MP
PUBLICAÇÃO: DOU DE 12/5/2016
SEÇÃO/EDIÇÃO: 1 PÁGINA: 189
ASS.:

KÁTIA
PGFN/CAS