Editoração Casa Civil
CEARÁ
DIÁRIO OFICIAL DO ESTADO

Fortaleza, 09 de junho de 2021 | SÉRIE 3 | ANO XIII Nº134 | Caderno 1/2 | Preço: R$ 18,73

PODER EXECUTIVO

DECRETO Nº34.098, de 08 de junho de 2021.

ALTERA O DECRETO Nº31.340, DE 5 DE NOVEMBRO DE 2013, QUE APROVA O REGULAMENTO PARA DEPRECIAÇÃO, AMORTIZAÇÃO, EXAUSTÃO, REAVALIAÇÃO E REDUÇÃO DO VALOR RECUPERÁVEL DO PATRIMÔNIO PÚBLICO DO ESTADO DO CEARÁ.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso de suas atribuições legais, com fulcro no art. 88, inciso IV e VI, da Constituição Estadual, e CONSIDERANDO o disposto no Decreto Estadual nº 21.325, de 15 de março de 1991, que versa, dentre outros, sobre o dever de transparência dos atos administrativos; CONSIDERANDO a relevância do processo de depreciação, amortização, exaustão, reavaliação e redução do valor recuperável dos bens integrantes do patrimônio do Estado do Ceará; CONSIDERANDO o impacto da pandemia da Covid-19 na execução de alguns serviços internos da Administração; CONSIDERANDO a necessidade de, em face desse cenário, alterar o prazo previsto no art. 38 do Decreto 31.340, de 05 de novembro de 2013, para ajuste do valor contábil dos bens estaduais adquiridos em exercícios anteriores a 2020, DECRETA:

Art. 1º O caput do art. 38 do Decreto 31.340, de 05 de novembro de 2013, passa a vigorar com a seguinte redação:

"Art. 38. O prazo máximo para o ajuste do valor contábil dos bens adquiridos em exercícios anteriores ao ano de 2020 será junho de 2022 para bens móveis e imóveis"

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Art. 3º Revogam-se as disposições em contrário.

PALÁCIO DA ABOLIÇÃO DO GOVERNO DO ESTADO DO CEARÁ, em Fortaleza, aos 08 de junho de 2021.

Camilo Sobreira de Santana
GOVERNADOR DO ESTADO DO CEARA

*** *** ***

DECRETO Nº34.099, de 08 de junho de 2021.

DISPENSA MEMBRO DE EQUIPE DE APOIO, NA FORMA DA LEI COMPLEMENTAR Nº65, DE 3 DE JANEIRO DE 2008, E DÁ OUTRAS PROVIDÊNCIAS.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso da atribuição prevista no Art. 88, VI, da Constituição do Estado do Ceará, CONSIDERANDO a instituição do Sistema de Licitações do Estado do Ceará, na forma da Lei Complementar nº 65, de 03 de janeiro de 2008; DECRETA:

Art. 1º Fica dispensado da função de Membro de equipe de apoio:

NOME	MATRÍCULA/CPF	A PARTIR DE
Maria Kátia Bulcão Lousada Pontes	009832-1-7	01/06/2021

Art. 2º Este Decreto entra em vigor na data de sua publicação.

PALÁCIO DA ABOLIÇÃO, DO GOVERNO DO ESTADO DO CEARÁ, aos dias do mês 08 de junho de 2021.

Camilo Sobreira de Santana
GOVERNADOR DO ESTADO DO CEARÁ

*** *** ***

DECRETO Nº34.100, de 08 de junho de 2021.

DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DOS AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC DO GOVERNO DO ESTADO DO CEARÁ E SOBRE O COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO DO ESTADO DO CEARÁ – CGSI, E DÁ OUTRAS PROVIDÊNCIAS.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso das atribuições que lhe confere o art. 88, nos incisos IV e VI, da Constituição Estadual; CONSIDERANDO a necessidade de garantir a integridade, confidencialidade e disponibilidade das informações sob gestão do Governo do Estado do Ceará e atualizar os Princípios, Diretrizes, Normas e Procedimentos que compõem a Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e Comunicação – TIC, do Governo do Estado do Ceará, a serem seguidas pelos órgãos e entidades do Poder Executivo Estatual; e CONSIDERANDO o Modelo de Governança de TIC, em conformidade com a Lei nº 13.494, de 22 de junho de 2004, alterada pela Lei nº 16.921, de 08 de julho de 2019, DECRETA:

Art. 1º Este Decreto promove a revisão da Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC), do Governo do Estado do Ceará, instituída pelo Decreto nº 29.227, de 13 de março de 2008.

Art. 2º A Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC) passa a ser a constante no Anexo Único, deste Decreto.

§ 1º A PoSIC deve ser implementada de forma a orientar estrategicamente as ações de segurança da informação e comunicação a serem executadas pelos órgãos e entidades do Poder Executivo do Estado do Ceará, tendo por base os seguintes princípios:

I - Princípio 1 - Alinhamento estratégico: Os órgãos e entidades estaduais deverão alinhar-se com os princípios, diretrizes, normas, procedimentos e ações de segurança da informação, observando sua missão institucional e o planejamento estratégico, com vistas a viabilizar orçamentos necessários para garantir a implantação mínima e continuada de níveis de controle de segurança da informação, por meio de ações e projetos, de forma a dotar-se de recursos tecnológicos, processos e pessoal qualificado para o devido cumprimento da política de que trata a PoSIC.

II - Princípio 2 - Diversidade organizacional: A elaboração de diretrizes, normas, procedimentos e controles de Segurança Corporativa do Estado deve levar em consideração a diversidade das atividades das instituições, respeitando a natureza e finalidade de cada órgão/entidade, de forma a garantir a continuidade do seu negócio.

III - Princípio 3 - Garantia da Segurança das Informações: Deve-se sempre buscar a implantação e utilização de controles que busquem garantir a confidencialidade, disponibilidade e integridade das informações nos órgãos/entidades. Estes controles devem incluir a classificação do grau de confidencialidade, disponibilidade e criticidade, bem como uma política para acesso e manuseio das mesmas.

IV - Princípio 4 - Propriedade da informação: Toda informação produzida ou armazenada no Estado é de sua propriedade e não de seus colaboradores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição.

V - Princípio 5 - Alinhamento com os aspectos legais ("Compliance"): Devem ser cumpridas as normas legais e regulamentares de abrangência estadual e federal, as políticas e as diretrizes estabelecidas para o negócio e para as atividades do estado, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

§ 2º Compõem a PoSIC o documento a que se refere o Anexo Único, deste Decreto, e Instruções Normativas complementares, os quais deverão ficar disponíveis na Internet, no sítio eletrônico da Secretaria do Planejamento e Gestão – Seplag e da Empresa de Tecnologia da Informação do Ceará – Etice.

Art. 3º O Comitê Gestor de Segurança da Informação - CGSI, instituído pelo Decreto nº 29.227, de 13 de março de 2008, como comitê temático de Tecnologia da Informação e Comunicação - TIC, de caráter técnico, consultivo, propositivo e permanente, focado em Segurança da Informação e Comunicação, passa a ser disciplinado por este Decreto, em conformidade com o art. 5º, da Lei nº 13.494, de 22 de junho de 2004.

§ 1º O CGSI será coordenado pela Empresa de Tecnologia da Informação do Ceará – Etice, secretariado pela Secretaria de Planejamento e Gestão – Seplag e formado por técnicos representantes dos seguintes órgãos e entidades estaduais com conhecimentos em segurança da informação, mediante

indicação de um suplente para cada titular:

I - Empresa de Tecnologia da Informação do Ceará – Etice;

II - Secretaria de Planejamento e Gestão – Seplag;

III - Casa Civil - CC;

IV - Secretaria da Fazenda - Sefaz;

V - Controladoria e Ouvidoria Geral do Estado - CGE;

VI - Procuradoria Geral do Estado - PGE;

VII - Secretaria da Segurança Pública e Defesa Social – SSPDS;

VIII - Secretaria de Ciência, Tecnologia e Educação Superior – Secitece;

§ 2º A organização e o funcionamento do CGSI serão dispostos em regimento interno, definido e aprovado por maioria de seus membros.

§ 3º O representante da Empresa de Tecnologia da Informação do Ceará – Etice acumulará as funções de coordenação e membro do Comitê.

§ 4º O representante da Secretaria do Planejamento e Gestão – Seplag acumulará as funções de Secretaria Executiva e membro do Comitê;

§ 5º Representantes de outros órgãos e entidades poderão ser convidados para participar das reuniões, a critério do Comitê e por convocação da Seplag.

§ 6º Dar-se-á vacância da função de membro do Comitê Gestor de Segurança da Informação – CGSI quando este deixar de comparecer, sem justificativa, a 3 (três) reuniões consecutivas ou a 4 (quatro) intercaladas, nos últimos 12 (doze) meses.

§ 7º O funcionamento do CGSI poderá verificar-se com a presença de 4 (quatro) dos seus membros, os quais deliberarão por maioria simples, devendo ser realizado no mínimo uma reunião a cada 2 (dois) meses.

Art. 4º Compete ao Comitê Gestor de Segurança da Informação – CGSI:

I - Supervisionar a execução da Política de Segurança da Informação e Comunicação dos Ambientes de TIC, bem como o cumprimento de suas Instruções Normativas;

II - Analisar, monitorar, acompanhar e avaliar as ocorrências dos Incidentes de Segurança da Informação de natureza corporativa, bem como as medidas de contenção e correção adotadas;

III - Analisar, acompanhar e avaliar os projetos e as principais iniciativas de caráter corporativo dos órgãos e entidades, relativas à Segurança da Informação e Comunicação dos ambientes de TIC;

IV - Avaliar, analisar e propor para deliberação do Conselho Superior de Tecnologia da Informação e Comunicação - CSTIC, sanções de caráter técnico restritivo, no fornecimento de serviços de TIC, aos Órgãos e Entidades que descumprirem a Política de Segurança da Informação e Comunicação ou que tenham sido provocadores ou vetores de ameaças à segurança do ambiente de TIC;

V - Analisar, emitir parecer e encaminhar para deliberação do Conselho Superior de Tecnologia da Informação e Comunicação - CSTIC, os pedidos de exceção às obrigações impostas pela Política de Segurança da Informação e Comunicação dos ambientes de TIC protocolizados pelos Órgãos e Entidades;

VI - Disseminar a cultura e a Política de Segurança da Informação e Comunicação dos ambientes de TIC no âmbito do Governo do Estado do Ceará;

VII - Promover a elaboração, atualização, validação e divulgação da Política de Segurança da Informação e Comunicação dos ambientes de TIC;

VIII - Promover a elaboração e implantação de planos de contingência e recuperação de desastres;

IX - Coordenar as ações para implantação da Política de Segurança da Informação e Comunicação dos ambientes de TIC;

X - Deliberar sobre as questões que lhe tenham sido encaminhadas; e

XI - Dar ciência ao Comitê de Governança de Tecnologia da Informação e Comunicação – CGTIC sobre os assuntos e ações relacionados ao descumprimento da Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC) pelos órgãos e entidades do Poder Executivo do Estado do Ceará.

§ 1º O CGSI recomendará à Seplag e à Etice, quando necessário, a emissão de Instruções Normativas conjuntas estabelecendo procedimentos de implementação e aplicação da PoSIC, as quais estipularão prazos de adequação para suas disposições.

§ 2º Cabe ao CGSI, em conjunto com as áreas de governança de TIC da Seplag e Etice, a divulgação das Instruções Normativas complementares relacionadas à PoSIC.

§ 4º O CGSI deverá propor a revisão e atualização da Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC) e de seus documentos, no prazo máximo de 4 (quatro) anos a partir de sua vigência.

Art. 5º Compete ao Comitê de Governança de Tecnologia da Informação e Comunicação – CGTIC, instituído pelo art. 2º, da Lei nº 13.494, de

22 de junho de 2004, no âmbito da Política a que se refere este Decreto, apoiar as ações tratadas pelo Comitê Gestor de Segurança da Informação – CGSI, relacionadas à Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC), no que diz respeito aos órgãos e entidades do Poder Executivo do Estado.

Art. 6º Compete à área de governança de TIC da Secretaria do Planejamento e Gestão – Seplag:

I - Realizar o acompanhamento, no nível estratégico, da execução dos planos de ação dos órgãos e entidades estaduais, decorrentes dos pedidos de exceção, que objetivam a remoção dos impeditivos ao devido cumprimento da Política de Segurança da Informação e Comunicação dos Ambientes de TIC;

II - Avaliar o impacto das ações decorrentes da Política de Segurança da Informação e Comunicação dos Ambientes de TIC para aferir os resultados alcançados; e

III - Secretariar o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI.

Art. 7º Compete à Empresa de Tecnologia da Informação do Ceará - Etice:

I - Coordenar o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI;

II - Monitorar a ocorrência dos Incidentes de Segurança da Informação e Comunicação que possuam repercussão no ambiente corporativo de TIC do governo;

III - Manter o CGSI informado da ocorrência de Incidentes de Segurança da Informação no ambiente corporativo de TIC, bem como as ações de contenção e correção adotadas, em caráter emergencial ou definitiva;

IV - Aplicar, em caráter emergencial e temporário, medidas restritivas no fornecimento de serviços de TIC geridos pela ETICE, aos Órgãos e Entidades, nos casos de ocorrência de Incidentes de Segurança ou de detecção de falha com potencial risco de segurança para o ambiente de TIC do Governo do Estado do Ceará; e

V - Assessorar ao CGSI na elaboração, atualização e/ou revisão de normas e padrões técnicos a serem observados pelos Órgãos e Entidades, visando assegurar compatibilidade e qualidade às soluções de Segurança da Informação e Comunicação.

Art. 8º Compete à Controladoria e Ouvidoria Geral do Estado do Ceará - CGE, no que se refere à Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC), realizar auditoria nos órgãos e entidades quando solicitado pelo CGSI, respeitada a sua capacidade operacional, com o objetivo de avaliar o seu cumprimento.

Art. 9º Ao gestor de tecnologia da informação e comunicação de cada órgão/entidade cabe a responsabilidade de:

I - Homologar e autorizar o uso e acesso de ativos, sistemas e dispositivos de processamento de informações em suas instalações; e

II - Realizar a gestão do acesso do usuário a recurso computacional do órgão/entidade do usuário que se desligar da instituição ou a qualquer tempo, quando evidenciados riscos à segurança da informação, e informar o incidente ao gestor máximo do órgão/entidade e ao gestor de segurança da informação e comunicação, se existir.

Parágrafo único. Nos órgãos e entidades onde não existir o responsável pela unidade de tecnologia da informação e comunicação ou função de gestão de segurança da informação e comunicação, cabe ao gestor máximo assumir as responsabilidades definidas neste artigo.

Art. 10. Ao gestor máximo de cada órgão/entidade e à chefia imediata do gestor de tecnologia da informação e comunicação cabe a responsabilidade de:

I - Disseminar permanentemente a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC); e

II - Garantir o cumprimento da PoSIC, inclusive disponibilizando recursos necessários para tanto.

Art. 11. Ao usuário de cada órgão/entidade cabe a responsabilidade de:

I - Conhecer e seguir a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC);

II - Notificar sua chefia imediata ou a qualquer membro do CGSI indício ou falha na Segurança da Informação e Comunicação; e

III - Responder por toda atividade executada por meio de sua identificação.

Art. 12. Compete aos órgãos e entidades estaduais enquadrarem-se nos termos da Política a que se refere este Decreto, cumprindo as normas aqui indicadas e reportando ao CGSI qualquer não conformidade.

Art. 13. Fica estabelecido que os órgãos e entidades estaduais devem contemplar dentro do seu Planejamento Estratégico, em caráter obrigatório, projetos relacionados à Segurança da Informação e Comunicação, que tenham como objetivo específico a adequação às recomendações estabelecidas nos controles que norteiam a PoSIC.

Art. 14. Os casos omissos e as eventuais dúvidas quanto à aplicação da Política a que se refere este Decreto serão resolvidos pelo Comitê Gestor de Segurança da Informação – CGSI.

Art. 15. Este Decreto entra em vigor na data de sua publicação.

Art. 16. Revogam-se as disposições em contrário, em especial o Decreto nº 29.227, de 13 de março de 2008.

PALÁCIO DA ABOLIÇÃO, DO GOVERNO DO ESTADO DO CEARÁ, em Fortaleza, aos 08 de junho de 2021.

Camilo Sobreira de Santana
GOVERNADOR DO ESTADO DO CEARÁ
Ronaldo Lima Moreira Borges
SECRETÁRIO EXECUTIVO DE PLANEJAMENTO E GESTÃO INTERNA,
DA SECRETARIA DO PLANEJAMENTO E GESTÃO

ANEXO ÚNICO A QUE SE REFERE O DECRETO Nº34.100, DE 08 DE JUNHO DE 2021
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

INTRODUÇÃO

A segurança da informação e comunicação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar os riscos, maximizar o retorno sobre investimentos e as oportunidades de negócio.

A segurança da informação e comunicação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atingidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

A informação e os processos de apoio, sistemas e redes de computadores são importantes ativos para os negócios de uma organização. Definir, alcançar, manter e melhorar a segurança da informação e comunicação podem ser atividades essenciais para assegurar o bom desempenho, o atendimento aos requisitos legais e a imagem da organização perante a sociedade.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação e comunicação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso e hackers estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação e comunicação é importante para os negócios, tanto do setor privado como do setor público, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação e comunicação é viabilizar os negócios como governo digital ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação e comunicação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes.

APRESENTAÇÃO DA POLÍTICA

A Secretaria de Planejamento e Gestão (SEPLAG), por meio da Empresa de Tecnologia da Informação do Ceará – ETICE, apresenta a Política de Segurança da Informação e Comunicação dos Ambientes de TIC, no cumprimento do seu papel de órgão central de definição de estratégias de Tecnologia da Informação e Comunicação (TIC), fortalecendo a gestão pública e o desenvolvimento econômico e social, por meio da Tecnologia da Informação e Comunicação (TIC). A presente política é pautada no alinhamento entre os setores de TIC com suas respectivas gestões superiores, de forma a assegurar a adequação dos preceitos norteadores da disciplina de segurança da informação e Comunicação à realidade dos órgãos e entidades, removendo impedimentos e alinhando estrategicamente as ações e projetos de segurança com as ações da própria instituição. Outro ponto fortemente considerado é a heterogeneidade da estrutura administrativa do Governo. Assim, são consideradas peculiaridades individuais de cada órgão ou entidade na exigência de requisitos de segurança, sempre maximizando a relação custo-benefício.

A Política de Segurança da Informação e Comunicação dos Ambientes de TIC definida neste documento atende à diretriz de Governo de "Rever e aplicar Políticas da Segurança da Informação e Comunicação do Estado", elaborada no Planejamento Estratégico da Função Tecnologia da Informação do Governo do Estado do Ceará.

Dessa forma, nesta política passam a figurar 03 (três) elementos principais:

1. Princípios, que são os fundamentos da Política de Segurança da Informação e Comunicação dos Ambientes de TIC;
2. Diretrizes, que são as regras de alto nível que representam os princípios básicos que o Governo do Estado do Ceará resolveu incorporar a sua gestão e

servirão como base para que as normas e os procedimentos sejam criados e detalhados; e
3. Normas e Procedimentos, que especificam no plano tático os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes e servir como base para os procedimentos no plano operacional. Posteriormente, a partir da Política traçada neste documento, os órgãos e entidades estaduais deverão desenvolver suas Políticas de Segurança da Informação e Comunicação alinhadas com o Planejamento Estratégico de suas áreas e com as estratégias de Governo definidas com foco na modernização, inclusão digital e governança. Faz-se, portanto, necessário o acompanhamento permanente da aplicação dessa política pelo CGSI, considerando também o caráter dinâmico da segurança da informação e comunicação no âmbito nacional e internacional. Ela deve servir como guia para todos os órgãos e entidades implementarem e manterem a gestão de Segurança da Informação e Comunicação nos seus ambientes de Tecnologia da Informação e Comunicação – TIC.
Objetivo
O objetivo desta Política de Segurança da Informação e Comunicação dos Ambientes de TIC é estabelecer princípios e diretrizes gerais para a gestão da segurança da informação e comunicação dos ambientes de TIC de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, posteriormente através de Instrução Normativa descrevendo as normas e procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.
Abrangência
A Política de Segurança da Informação e Comunicação dos Ambientes TIC deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes nos Órgãos/Entidades estaduais, como também às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito do Governo do Estado do Ceará ou a quem venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.
Diretrizes Gerais do Governo do Estado do Ceará para Segurança da Informação e Comunicação
Diretrizes do Princípio 1 - Alinhamento Estratégico
• Conflitos de negócios: Na existência de conflito entre os controles de segurança e uma necessidade de negócio específica, o novo cenário de controle deve ser analisado pelo CGSI e pelo órgão, a fim de viabilizar os objetivos da organização, havendo ainda a necessidade de registro da aceitação dos riscos remanescentes por parte da gestão.
• Gestão de Riscos: Os ativos, processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados do órgão/entidade devem ser submetidos a um processo formal de análise, avaliação e tratamento de riscos, visando atingir o grau de segurança adequado para o Governo do Estado.
• Gestão de Continuidade: Cada órgão/entidade deve estabelecer um conjunto de estratégias e planos de ação documentados, testados e revisados periodicamente, de maneira a garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da Instituição.
• Auditoria e Conformidade: O Governo do Estado por meio do CGSI reserva-se o direito de auditar periodicamente a prática da Política de Segurança da Informação e Comunicação dos Ambientes de TIC de forma a avaliar a conformidade das ações de seus colaboradores em relação ao estabelecido pela PoSIC da Instituição e pela legislação aplicável.
• Monitoramento: O Governo do Estado por meio do CGSI reserva-se o direito de monitorar o acesso e utilização de seus ambientes físicos, assim como dos equipamentos e sistemas tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas pro ativamente.
• Fortalecer o alinhamento estratégico: A Política de Segurança da Informação e Comunicação dos Ambientes de TIC é agenda estratégica para o Governo do Estado do Ceará, devendo ser incluídas diretrizes e metas relacionadas ao assunto no planejamento estratégico de cada órgão/entidade para fortalecer o alinhamento entre o planejamento de TIC e o planejamento estratégico da instituição e do Governo do Estado no processo de planejamento e no atingimento das metas definidas. O objetivo é promover e motivar a criação de uma cultura de segurança da informação. Com isso, a estrutura responsável pela gestão da PoSIC é um dos pilares da Governança Institucional do órgão ou entidade e deve estar vinculada à alta administração.
• Objetivos estratégicos mínimos: O planejamento estratégico de cada órgão/entidade deve conter no mínimo os objetivos estratégicos “Assegurar estruturas e práticas de segurança da informação e comunicação” e “Fortalecer o alinhamento entre o planejamento de TIC, as estratégias do órgão/entidade e do Governo do Estado”.
• Responsabilidades dos gestores de TIC e de Ativos TIC: Os gestores de TIC e de ativos de TIC são responsáveis por acompanhar e seguir as Políticas de Segurança da Informação e Comunicação dos Ambientes de TIC do órgão/entidade e do Governo do Estado do Ceará.
• Responsabilidades da alta gestão: A alta gestão formada pelos dirigentes máximos do órgão/entidade é responsável por acompanhar e seguir as PoSIC da instituição e do Governo do Estado do Ceará, tendo como referência: Prover os recursos necessários à PoSIC; Promover o desenvolvimento de Políticas de Segurança da Informação e Comunicações dos Ambientes de TIC; Estimular a adoção de práticas de governança de segurança da informação e comunicações; Implementar práticas de gerenciamento de riscos e continuidade de negócios.
Objetivos Estratégicos relacionados às Diretrizes do Princípio 1 - Alinhamento Estratégico:
Objetivo Estratégico: Desenvolver e implantar uma Política de Segurança da Informação e Comunicação nos órgãos/entidades do Governo do Estado do Ceará.
Ações Prioritárias
1. Adotar mecanismos para promover a elaboração, revisão, atualização, divulgação, conscientização e validação dos princípios, diretrizes, normas e procedimentos da Política de Segurança da Informação e Comunicação nos órgãos/entidades estaduais;
2. Elaborar plano estratégico de segurança da informação e comunicação para viabilizar todos os recursos necessários para o cumprimento das Políticas de Segurança da Informação e Comunicação;
3. Selecionar mecanismos de segurança da informação e comunicação considerando fatores de riscos, tecnologias e custos;
4. Criar grupo responsável pela elaboração, implantação, acompanhamento, auditoria e revisão da Política de Segurança da Informação e Comunicação;
5. Criar comitê de gestão de segurança da informação para coordenar a política de segurança da informação e comunicação da instituição, e
6. Estabelecer mecanismos que possibilitem o processo de coleta, recuperação, análise e correlacionamento de dados para investigação de questões cíveis, criminais e administrativas, para proteger os usuários e recursos de TIC.
Objetivo Estratégico: Comunicar oficialmente e capacitar os usuários na Política de Segurança da Informação e Comunicação dos Ambientes de TIC adotada pelo Governo do Estado do Ceará, para garantir a conscientização e a prática.
Ações Prioritárias
1. Definir mecanismos para garantir a disseminação da cultura de segurança da informação e comunicação nos órgãos/entidades estaduais;
2. Estabelecer medidas para que a política de segurança da informação e Comunicação dos Ambientes de TIC seja cumprida de forma que as diretrizes, normas e procedimentos de segurança sejam aplicados por todos os usuários, e
3. Prover mecanismos de capacitação nos procedimentos de segurança e uso correto dos recursos de TIC para todos os usuários.
Diretrizes do Princípio 2 - Diversidade Organizacional
• Alinhamento da política de segurança da informação e comunicação: A política de segurança da informação e comunicação dos órgãos/entidades deve estar alinhada com a política de segurança da informação e Comunicação dos Ambientes de TIC do Governo do Estado do Ceara.
• Natureza e finalidade das atividades: Deve ser respeitada a natureza e finalidade das atividades de cada órgão/entidade, quanto à elaboração de Políticas, Normas, Procedimentos e controles de segurança corporativa.
• Leis e regimentos: A Política de Segurança da Informação e comunicação deve respeitar as leis e regimentos inerentes a cada órgão/entidade.
Objetivos Estratégicos relacionados as Diretrizes do Princípio 2 - Diversidade Organizacional:
Objetivo Estratégico: Desenvolver e implementar plano de contingência e respostas a incidentes, considerando a diversidade das atividades das Instituições, respeitando a natureza e finalidade de cada órgão/entidade de forma a assegurar a continuidade do negócio, bem como o seu reestabelecimento em situação de anormalidade.
Ações Prioritárias
1. Definir os processos e recursos críticos realizando análise de impacto de riscos para elaboração do plano de continuidade do negócio;
2. Estabelecer processos de proteção contra falhas e danos que comprometam as atribuições do Governo do Estado do Ceará;
3. Definir mecanismos formais e periodicamente testados para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, e
4. Definir processo e criar procedimentos para gestão de incidentes.
Diretrizes do Princípio 3 - Garantia da Segurança das Informações
• Responsabilidade e Comprometimento: Todos os colaboradores do Governo do Estado do Ceará, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos físicos, tecnológicos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, independente das medidas de segurança implementadas.
• Segurança das Comunicações: Garantir a segurança das comunicações entre os órgãos e entidades que compõem o Governo do Estado.
• Controle de Acessos: Os acessos aos ambientes físicos e computacionais devem ser controlados, registrados e monitorados, com base na necessidade de conhecer ações desenvolvidas e do privilégio de acesso mínimo para o desempenho das atividades profissionais.
• Notificação, Registro e Tratamento de Incidentes: Todos os colaboradores do Governo do Estado do Ceará, em qualquer vínculo, função ou nível hierárquico têm a obrigação de reportar imediatamente, por meio dos processos definidos no órgão/entidade, quaisquer incidentes de segurança que tomarem

conhecimento, de modo que possam ser registrados, avaliados e tratados.
• Treinamento e Conscientização: Todos os colaboradores devem conhecer esta Política de Segurança da Informação e Comunicação dos Ambientes de TIC e serem capacitados regularmente por meio de campanhas de conscientização e treinamentos, de acordo com suas funções, garantindo assim maior efetividade e eficácia das ações de segurança da Informação e comunicação.
• Revisão e análise crítica: Os conjuntos de documentos que compõem a Política de Segurança da Informação e Comunicação dos Ambientes de TIC devem passar por revisões e análises críticas periódicas em no máximo 4 (quatro) anos, ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada.
• Proteção Física: Toda proteção física deve ser compatível com o risco identificado.
• Ameaças Externas: Deve ser estabelecida também a proteção contra ameaças externas e do meio ambiente, como proteção contra incêndios e enchentes ou outras formas de desastres naturais.
• Cópias de Segurança: Gerar no mínimo cópias de segurança dos dados classificados como críticos e sua respectiva restauração em tempo aceitável, a fim de não prejudicar o bom andamento das atividades do órgão/entidade com uso preferencial do ambiente de nuvem.
• Suporte jurídico: A implantação de uma PoSIC deve contar com suporte jurídico ou de profissionais qualificados sobre os aspectos legais e seus requisitos.
Objetivos Estratégicos relacionados as Diretrizes do Princípio 3 - Garantia da Segurança das Informações:
Objetivo Estratégico: Definir procedimentos de rotina para a execução de cópias de segurança e disponibilização dos recursos de reserva.
Ações Prioritárias
1. Implantar rotina de backup (cópias), armazenamento, testes de integridade e recuperação de dados (restore) preferencialmente utilizando o ambiente de nuvem;
2. Implantar normas e responsabilidades sobre o controle das mídias de software.
Objetivo Estratégico: Garantir de forma segura o acesso e manuseio das informações no âmbito do Governo do Estado do Ceará.
Ações Prioritárias
1. Definir normas e procedimentos de acesso a dados, informações e conhecimentos por pessoas do próprio órgão/entidade, por outros órgãos/entidades e terceiros.
Objetivo Estratégico: Assegurar que os sistemas de processamento em operação e em implantação possuam documentação suficiente para garantir sua manutenibilidade, instalação e utilização.
Ações Prioritárias
1. Definir e implantar metodologias de desenvolvimento de sistemas implementando requisitos de segurança.
2. Implantar a cultura de documentação de sistemas de processamento como manuais técnicos e operacionais, e
3. Definir procedimentos para controle de liberação de ativos de TIC.
Objetivo Estratégico: Garantir que apenas pessoas autorizadas tenham acesso a funcionalidades e informações dos sistemas de processamento.
Ações Prioritárias
1. Manter controle de acesso a todos os sistemas utilizando identificação de uso pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;
2. Prever trilhas de auditoria nos sistemas de processamento críticos, e
3. Definir controles para que usuários detenham acesso apenas aos recursos necessários e imprescindíveis ao desenvolvimento do seu trabalho.
Diretrizes do Princípio 4 - Propriedade da informação
• Uso de Correio: Assegurar que o uso do Correio Eletrônico institucional seja disciplinado, ficando claro para os usuários o conceito de não privacidade no seu uso, sendo utilizado preferencialmente serviços em nuvem.
• Uso da internet: Assegurar que o acesso à Internet, provido pelo Governo do Estado, seja disciplinado, ficando claro para os usuários o conceito de não privacidade no seu uso.
• Proprietários e Ativos de TIC: Os ativos de TIC devem ser identificados, assim como seus respectivos proprietários. Aos proprietários desses ativos deve ser atribuída a responsabilidade pela manutenção da sua segurança.
• Informações sensíveis: Funcionários com acesso a informações sensíveis devem ser adequadamente analisados antes da liberação de acesso.
• Direitos de Acesso: Deve ser prevista também uma forma de retirar direitos de acesso e de devolução de ativos, caso o vínculo empregatício do colaborador (funcionário, terceirizado ou comissionado) seja encerrado.
• Informações Críticas: O processamento de informações críticas ou sensíveis deve ser mantido em áreas seguras, com controle de acesso apropriado, preferencialmente em ambiente de nuvem.
• Acessibilidade, Disponibilidade e Integridade: Garantir a acessibilidade, disponibilidade e integridade das informações para o acesso público.
• Interoperabilidade: Viabilizar a interoperabilidade e acessibilidade entre os órgãos e entidades que compõem o Governo do Estado.
• Certificação Digital: Incentivar e apoiar o estudo e implantação de soluções de segurança e certificação digital, observando o cumprimento de requisitos de segurança mínimos e a interoperabilidade entre todos os órgãos e entidades que compõem o Governo do Estado, sendo essas soluções baseadas preferencialmente em código aberto quando aplicável.
Objetivos Estratégicos relacionados as Diretrizes do Princípio 4 - Propriedade da informação:
Objetivo Estratégico: Estabelecer que as condições e termos de licenciamento de softwares e direitos de propriedade intelectual devam ser respeitados.
Ações Prioritárias
1. Definir normas para instalação de softwares com objetivo de combater o uso de cópia ilegal;
2. Garantir o controle das licenças de softwares utilizados pelo órgão/entidade;
3. Adotar procedimentos para que a instalação e uso de softwares e sistemas computacionais, devam ser homologados e autorizados pelo setor competente do órgão/entidade, e
4. Definir mecanismos para cessão de softwares e sistemas computacionais no âmbito do Governo do Estado do Ceará.
Objetivo Estratégico: Adotar critérios relacionados ao uso de ativos de TIC no Governo do Estado do Ceará.
Ações Prioritárias
1. Manter os ativos de TIC críticos em áreas seguras e adequadas, protegidos contra perigos ambientais e com implantação de controles de acesso, preferencialmente utilizando o ambiente de nuvem;
2. Inventariar os ativos, classificando-os quanto à importância, prioridade e nível de proteção;
3. Proteger os ativos de TIC de roubo e modificação, definindo controles de forma a minimizar a perda ou dano;
4. Adotar controles de acesso físico e lógico para uso de ativos no âmbito do Governo do Estado do Ceará;
5. Estabelecer processos de aquisição de bens e serviços baseados em preceitos legais;
6. Aprimorar e/ou definir critérios de seleção, movimentação ou desligamento de pessoal que impactam na segurança da informação e comunicação, e
7. Implementar mecanismos de registro de históricos dos ativos de TI, garantindo a sua rastreabilidade.
Objetivo Estratégico: Estabelecer responsabilidades e requisitos básicos de utilização da Internet e correio eletrônico no âmbito do Governo do Estado do Ceará.
Ações Prioritárias
1. Elaborar plano de comunicação para conscientização de que o uso da internet e correio eletrônico não é um direito e sim uma concessão;
2. Disseminar o conceito de não privacidade do uso da Internet e correio eletrônico.
Objetivo Estratégico: Assegurar que todos os usuários ao utilizarem esses serviços deverão fazê-los no estrito interesse dos órgãos e entidades mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.
Ações Prioritárias
1. Implantar mecanismos de autenticação e monitoramento, que determinem a titularidade de todos os acessos à Internet e correio eletrônico, e
2. Criar mecanismos de controle da demanda e da disponibilidade, garantindo a qualidade do serviço.
Diretrizes do Princípio 5 - Alinhamento com os aspectos legais
• Conformidade Legal – Aderência às leis: Assegurar que os órgãos e entidades, cumpram e façam cumprir as leis que vigoram no país, em especial as leis de combate à pedofilia, preconceito racial, pirataria de software e do direito autoral.
• Conformidade Legal - A gestão da segurança da informação e comunicação: Deve atender aos requisitos legais dos órgãos regulatórios de segurança da informação e comunicação do Governo Municipal, Estadual e Federal, assim como, às normas ABNT de segurança da informação, aplicáveis ao negócio da instituição.
• Conformidade Legal - Cumprimento do decreto estadual vigente: Devem ser adotadas medidas para o cumprimento do decreto estadual vigente, que estabelece a Política de Segurança da Informação e Comunicação dos Ambientes de TIC para o Governo do Estado do Ceará.
• Conformidade Legal - Aderência às normas técnicas e boas práticas: Deve-se buscar aderência às normas técnicas e boas práticas que regem a Gestão da Segurança da Informação e Comunicação. Devem ser consideradas as legislações específicas de cada setorial.
• Classificação e Tratamento da Informação: Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificados de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida. A Classificação de Informação como sigilosa

ou reservada será solicitada por meio dos Comitês Setoriais de Acessos à Informação de cada órgão ou entidade e deliberadas pelo Comitê Gestor de Acesso à Informação (art.11 do Decreto Estadual nº 31.199, de 30 de abril de 2013).
• Acesso às informações de TIC: O acesso às informações de TIC deverá ser fornecido mediante pedido formal, e seu andamento deverá estar em conformidade com a Lei de Acesso à Informação (LAI).
• Pedidos de acesso a informações de TIC: Não serão atendidos pedidos de acesso a informações de TIC classificadas como sigilosas.
• As informações classificadas como sigilosas: As informações classificadas como sigilosas para o acesso do cidadão, podem ser fornecidas em casos de auditoria (§ 1º, inciso II, art. 3°, da Lei n° 13.325, de 14.07.03).
• Especificações técnicas de sistemas informatizados: As informações referentes a especificações técnicas de sistemas informatizados, diretórios de rede, servidores, bancos de dados e redes (por ex.: casos de uso, código-fonte, diagramas de banco de dados, dicionário de dados etc) são classificadas como sigilosas independente do órgão ou entidade que produza ou possua a sua guarda. (§ 1º, inciso V, art. 1°, da Portaria CGAI nº 01/2016).
• Referências Legais:
• Lei de Acessibilidade, Lei nº 13.146, de 2015.
• Lei de Acesso a Informação (LAI), Lei nº 12.527, de 2011.
• Marco Civil da Internet, Lei nº 12.965, de 2014, e Decreto nº 8.771, de 2016.
• Lei Antipirataria, Lei nº 9.609, de 1998.
• Lei de Pornografia Infantil, Lei nº 8.069, de 1990.
• Lei de Crimes Cibernéticos, Leis nº 12.735, de 2012, e 12.737, de 2012.
• Lei das Estatais, Lei nº 13.303, de 2016.
• Lei Geral de Proteção de Dados do Brasil (LGPD), Lei nº 13.709, de 2018.
• Norma ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
• Norma ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de segurança – Gestão de Riscos de Segurança da Informação.
Objetivos Estratégicos relacionados as Diretrizes do Princípio 5 - Alinhamento com os aspectos legais:
Objetivo Estratégico: Fortalecer metodologia de classificação de informações e conhecimentos no âmbito do Governo do Estado do Ceará.
Ações Prioritárias
1. Desenvolver processo de classificação da informação para definir níveis e critérios adequados, e
2. Estabelecer normas, padrões e procedimentos relacionados a produção, tramitação, transporte, manuseio, custódia, armazenamento, conservação, eliminação e cessão de documentos no âmbito do Governo do Estado do Ceará.
DOS PROCEDIMENTOS DE AUDITORIA
O Manual de Auditoria, parte integrante da Política de Segurança da Informação e Comunicação dos Ambientes de TIC, será definido sob demanda e em caráter preventivo e especificado em Instrução Normativa própria, a ser expedida pela Controladoria e Ouvidoria Geral do Estado (CGE), mediante parecer favorável do Comitê Gestor de Segurança da Informação, podendo ser atualizado de acordo com a conveniência administrativa, por meio do mesmo instrumento.
O Manual de Auditoria apresentará o procedimento a ser realizado pela CGE para aferir o nível de maturidade nos requisitos de atenção a esta política.
As ações de auditoria sob demanda serão preconizadas a pedido do CGSI, ou do órgão ou entidade que deseje certificar seu nível de maturidade da PoSIC. As ações de auditoria preventiva serão realizadas mediante iniciativa da própria CGE como maneira de zelar pelo devido cumprimento desta Política de Segurança da Informação e Comunicação nos Ambientes de TIC. Em qualquer ação de auditoria, a atuação da CGE poderá culminar em sanção por descumprimento, conforme definido em instrução normativa própria, e/ou reclassificação do nível de maturidade do órgão ou entidade nos controles aferidos.
O Manual de Auditoria definirá, ainda, procedimento inicial de declaração de nível de maturidade, em que o órgão ou entidade, mediante apresentação de documentação mínima da forma especificada na instrução normativa, lhe conferirá interinamente o nível de maturidade pleiteado para o(s) controle(s) até a realização da efetiva inspeção por parte da CGE.
A CGE poderá solicitar apoio técnico da ETICE nos trabalhos de auditoria a serem realizados nos órgãos e entidades. O apoio técnico fornecido pela ETICE se restringirá aos processos de verificação técnica para comprovação de requisitos de segurança que não possam ser aferidos por simples apresentação de documentação.
DAS SANÇÕES
A Definição de Sanções por Descumprimento, parte integrante da Política de Segurança da Informação e Comunicação dos Ambientes de TIC, será especificada em Instrução Normativa própria, a ser expedida posteriormente pelo Comitê Gestor de Segurança da Informação, podendo ser atualizada de acordo com a conveniência administrativa, por meio do mesmo instrumento.
A Política de Segurança da Informação e Comunicação dos Ambientes de TIC possui implicitamente, como sanção preventiva, o condicionamento da prestação de serviços de TIC aos órgãos e entidades à adequação dos mesmos às exigências constantes nas Diretrizes. Contudo, outras sanções poderão ser previstas na Instrução Normativa referida no parágrafo introdutório. Tais sanções levarão em conta as regras do direito administrativo e possuirão caráter preferencialmente educativo e fomentador dos princípios de Segurança da Informação e Comunicação, prevalecendo o interesse coletivo da manutenção da efetiva segurança.

*** *** ***

DECRETO Nº34.101, de 09 de junho de 2021.

ABRE AOS ÓRGÃOS E ENTIDADES CRÉDITO SUPLEMENTAR DE R$ 286.997.275,31 PARA REFORÇO DE DOTAÇÕES ORÇAMENTÁRIAS CONSIGNADAS AO VIGENTE ORÇAMENTO.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso das suas atribuições que lhe confere o inciso IV, do art. 88, da Constituição Estadual, combinado com os incisos I e III, do § 1º, do art.43, da Lei Federal nº 4.320, de 17 de março de 1964, do art. 5º da Lei Estadual nº 17.364, de 23 de dezembro de 2020 – LOA 2021, do art. 37 da Lei Estadual nº 17.278, de 15 de setembro de 2020 – LDO 2021, da Lei Complementar nº 230, de 07 de janeiro de 2021 e da Lei Complementar nº 239, de 09 de abril de 2021. CONSIDERANDO a necessidade de realocar dotações orçamentárias da ASSEMBLEIA LEGISLATIVA – AL, entre projetos e atividades, para atender despesas com desenvolvimento de ações de saúde e assistência social, realização de concurso público e manutenção da área de tecnologia da informação e comunicação. CONSIDERANDO a necessidade de suplementar dotações orçamentárias dos ENCARGOS GERAIS DO ESTADO – EGE, para atender a contribuição PREVCOM/CE, pagamento de sentenças judiciais e pagamento do programa Sua Nota Tem Valor. CONSIDERANDO a necessidade de suplementar dotações orçamentárias da CONTROLADORIA E OUVIDORIA GERAL DO ESTADO – CGE, para aquisição de equipamentos que serão usados para equipe de tecnologia da CGE, capacitações em avaliação e gestão de pessoas e em gestão de desempenho, ambas com aulas on line e remotas e contratação de solução para atendimento virtual (chatbot) que será disponibilizada nas plataformas tecnológicas. CONSIDERANDO a necessidade de suplementar dotações orçamentárias da CONTROLADORIA GERAL DE DISCIPLINA DOS ÓRGÃOS DE SEGURANÇA PÚBLICA E SISTEMA PENITENCIÁRIO – CGD, para atender a prestação de serviço de computação em nuvem pública no modelo software como serviço, para o fornecimento de licenças de software, serviços de instalação, migração, customização e integração inicial, treinamento e suporte especializado, a fim de atender as demandas referentes as atividades de videoconferência. CONSIDERANDO a necessidade de suplementar dotações orçamentárias do CORPO DE BOMBEIROS MILITAR DO ESTADO DO CEARÁ – CBMCE, para aquisição de cestas básicas. CONSIDERANDO a necessidade de realocar dotações orçamentárias da FUNDAÇÃO CEARENSE DE METEOROLOGIA E RECURSOS HÍDRICOS – FUNCEME, entre projetos e atividades, para atender despesas de exercícios anteriores referentes a ação judicial. CONSIDERANDO a necessidade de suplementar dotações orçamentárias do FUNDO PREVIDENCIÁRIO – PREVID, pagamento de inativos e pensionistas da administração geral do Poder Executivo, da Assembleia Legislativa, do Tribunal de Justiça do Estado, do Ministério Público e do Tribunal de Contas do Estado. CONSIDERANDO a necessidade de realocar dotações orçamentárias da FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ – CEARAPREV, entre projetos, atividades e modalidades, para atender despesa com manutenção dos serviços administrativos. CONSIDERANDO a necessidade de realocar dotações orçamentárias da FUNDAÇÃO UNIVERSIDADE REGIONAL DO CARIRI – URCA, entre projetos, atividades e modalidades, para atender a manutenção do funcionamento das atividades acadêmicas nos campi da URCA. CONSIDERANDO a necessidade de suplementar dotações orçamentárias da FUNDAÇÃO UNIVERSIDADE VALE DO ACARAÚ – UVA, para atender a decisão judicial para nomeação de docente. CONSIDERANDO a necessidade de realocar dotações orçamentárias do FUNDO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL DO ESTADO DO CEARÁ – FSPDS, entre projetos e atividades, para atender a aquisição de equipamentos, materiais de saúde e medicamentos e aquisição de equipamentos de TI, destinados a assessoria biopsicossocial da SSPDS e suas vinculadas. CONSIDERANDO a necessidade de realocar dotações orçamentárias do FUNDO ESPECIAL DO SISTEMA ÚNICO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES PÚBLICOS CIVIS, DOS AGENTES PÚBLICOS E DOS MEMBROS DE PODER DO CEARÁ – FUNAPREV, entre projetos e atividades, para atender ao pagamento de inativos e pensionistas da Segurança Pública (pessoal civil), pagamento de inativos e pensionistas do ensino básico e pagamento de inativos e pensionistas do ensino superior. CONSIDERANDO a necessidade de realocar e suplementar dotações orçamentárias do FUNDO ESTADUAL DE SAÚDE – FUNDES, entre projetos, atividades e regiões, para atender demandas diversas dos contratos de gestão do Hospital Regional Norte, Hospital Regional do Sertão Central, Hospital Regional do Cariri e UPA da Praia do Futuro, atender demandas de material de consumo, pagamento de serviços de desenvolvimento e manutenção de software, pagamento com serviços de infraestrutura de TIC em nuvem, aquisição de equipamentos para o Centro Integrado de Diabetes e Hipertensão e central de regulação do Estado, pagamento de cooperativas do HGCC, LACEN, HSJ, HGF, HCAS e HMJMA, promoção da assistência à saúde aos usuários do SUS, demandas relativas à Covid-19 para requisições administrativas, atender pagamento de licença de banco de dados no HMJMA,