IPECE INSTITUTO DE PESQUISA E ESTRATÉGIA ECONÔMICA DO CEARÁ

GOVERNO DO ESTADO DO CEARÁ
Secretaria do Planejamento e Gestão

Boletim de GESTÃO PÚBLICA

Nº 06 – Janeiro/Fevereiro de 2018

Boletim de Gestão Pública – Nº 06 – Janeiro/Fevereiro de 2018

Unidade Responsável:
Diretoria de Estudos de Gestão Pública – DIGEP

Editoração:
Cláudio André Gondim Nogueira

Colaboração:
Aprígio Botelho Lócio
Tiago Emanuel Gomes dos Santos

O **Instituto de Pesquisa e Estratégia Econômica do Ceará (IPECE)** é uma autarquia vinculada à Secretaria do Planejamento e Gestão do Estado do Ceará. Fundado em 14 de abril de 2003, o IPECE é o órgão do Governo responsável pela geração de estudos, pesquisas e informações socioeconômicas e geográficas que permitem a avaliação de programas e a elaboração de estratégias e políticas públicas para o desenvolvimento do Estado do Ceará.

Missão: Propor políticas públicas para o desenvolvimento sustentável do Ceará por meio da geração de conhecimento, informações geossocioeconômicas e da assessoria ao Governo do Estado em suas decisões estratégicas.

Valores: Ética e transparência; Rigor científico; Competência profissional; Cooperação interinstitucional e Compromisso com a sociedade.

Visão: Ser uma Instituição de pesquisa capaz de influenciar de modo mais efetivo, até 2025, a formulação de políticas públicas estruturadoras do desenvolvimento sustentável do estado do Ceará.

Instituto de Pesquisa e Estratégia Econômica do Ceará (IPECE) -
Av. Gal. Afonso Albuquerque Lima, s/n | Edifício SEPLAG | Térreo - Cambeba | Cep: 60.822-325 |
Fortaleza, Ceará, Brasil | Telefone: (85) 3101-3521
http://www.ipece.ce.gov.br/

Sobre o **Boletim de Gestão Pública**

O Boletim de Gestão Pública do Instituto de Pesquisa e Estratégia Econômica do Ceará (IPECE) tem como objetivo principal a difusão de melhores práticas e inovações na área de gestão e de políticas públicas. É uma publicação bimestral, formada por artigos sintéticos (descritivo-analíticos), elaborados pelo corpo técnico do Instituto e ou por técnicos convidados de outros órgãos do Governo do Estado do Ceará e de outras organizações. Em linhas gerais, os artigos buscam: (i) difundir melhores práticas, com a análise de casos específicos locais, estaduais, nacionais ou internacionais; (ii) apresentar avanços na gestão pública do Ceará, com as principais inovações em gestão e políticas públicas no Estado; (iii) discutir avanços teóricos nas áreas de gestão e de políticas públicas e como esses conhecimentos podem ser postos em ação; (iv) analisar desafios para a gestão e para as políticas públicas; ou (v) verificar inovações no âmbito do setor privado, indicando como elas podem servir de inspiração para o setor público.

Instituto de Pesquisa e Estratégia Econômica do Ceará – **IPECE** 2018

Boletim de Gestão Pública / Instituto de Pesquisa e Estratégia Econômica do Ceará (IPECE) / Fortaleza – Ceará: Ipece, 2018.

ISSN: 2594-8709

Nesta Edição:

2. Transparência e segurança da informação: um fator preponderante para a integridade e credibilidade dos dados disponibilizados ao cidadão para um efetivo acompanhamento da gestão pública

Autores: *Carlos Rubens Moreira da Silva*[25] *e Luis Borges Gouveia*[26]

A Constituição Federal do Brasil assegurou a toda população o princípio da transparência na administração pública e com a nova Lei da Informação já em vigor, esta estabelece em seu artigo 5º que "*É dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão"*. Então qualquer interessado pode apresentar pedido de acesso a informações aos órgãos públicos, sendo necessário apenas conter a identificação do requerente e especificação da informação requerida, sendo vedado à administração exigir do cidadão os motivos de tal solicitação.

No entanto a informação[27], para qualquer entidade, seja ela um órgão governamental ou uma empresa privada, é de importância fundamental e dependendo de seu valor para a organização, a sua integridade deve ser preservada. Na esfera pública ela tanto pode estar guardada para uso restrito como pode ser exposta ao público para consulta, obedecendo ao que determina à lei de acesso à informação, de acordo com a sua classificação de confidencialidade, indispensável à segurança do Estado e da sociedade.

Atualmente o cidadão pode obter qualquer informação sobre o gasto público através da Internet e isso gera uma enorme responsabilidade para os diversos órgãos que compõem as diferentes esferas governamentais do poder público. Desse modo, além da probabilidade de haver inconsistência na informação, também pode ocorrer o tratamento impróprio dos dados, especialmente no que tange à segurança da informação.

De acordo com Rangel (2015)[28],

> Na ânsia do cumprimento do dever em prol da transparência, aspectos da SI[29] podem ser desconsiderados. Nesse sentido, é preciso encontrar um equilíbrio entre o que é

[25] Doutorando em Ciências da Informação (Universidade Fernando Pessoa, Porto - Portugal) e Mestre em Políticas Públicas (UECE), Auditor de Controle Interno e Orientador da Célula de Monitoramento da gestão para Resultados e Gestão Fiscal da Controladoria e Ouvidoria Geral do Estado (CGE). E-mail: carlos.rubens@cge.ce.gov.br

[26] Agregado em Engenharia e Gestão Industrial pela Universidade de Aveiro, Doutorado em Ciências da Computação pela Universidade de Lancaster, no Reino Unido e Mestre em Engenharia Electrónica e de Computadores, pela Universidade do Porto (FEUP). Professor Catedrático da Universidade Fernando Pessoa.

[27] A informação pode ser entendida como qualquer dado que tenha valor para uma pessoa ou entidade.

[28] RANGEL, A. S. **Transparência versus segurança da informação**: uma análise dos fatores de risco expostos na comunicação entre o governo e a sociedade. 2015. 143 f., il. Dissertação (Mestrado em Ciência da Informação) — Universidade de Brasília, Brasília.

[29] Segurança da Informação.

> transparente e o que é seguro". Então, para resolução de tal problema, a utilização da tecnologia, notadamente as TIC, oferecem soluções para estruturar os imensos quantitativos de documentos existentes nos órgãos da administração pública nas três esferas de poder.

Porém, a utilização da tecnologia pode proporcionar riscos à informação devido à interligação das redes no ciberespaço, ficando assim exposta as incontáveis ameaças existentes no mundo virtual que por sua vez geram incidentes no que tange a segurança da informação disponibilizada nesse meio.

A segurança da informação segundo Gouveia (2016)[30],

> É a proteção de informação, dos sistemas e dos dispositivos (hardware) que usa, armazena e transmite informação. O objetivo da segurança da informação é o de proteger de forma adequada os ativos de informação de modo a assegurar a continuidade de negócio (ou de operação, se for preferido o uso de um termo menos associado à vida empresarial), minimizando potenciais perdas que possam ocorrer (da perda ou destruição de valor desses ativos) e maximizando o retorno de investimento (uma vez que os esforços associados com a proteção de informação têm de ser cobertos pelo seu valor ou pelo valor que deles se possa extrair).

Ainda de acordo com Gouveia (2016), para que essa meta seja atingida, "é necessário preservar três aspetos críticos da informação, que são: a confidencialidade, a integridade e a disponibilidade".

Esses aspectos que segundo Gouveia (2016) estão associados à informação e são utilizados como referência na garantia da sua segurança, podem ser assim conceituados de maneira resumida:

- Confidencialidade – Qualidade de limitar o acesso à informação a somente às que são autorizadas pelo seu proprietário;
- Integridade – Propriedade que garante que a informação mantenha as suas características originais instituídas pelo seu proprietário, incluso o controle de alterações e garantia durante o seu período de validade;
- Disponibilidade – Atributo que garante que a informação permaneça sempre disponível para a utilização legítima, ou seja, por aqueles usuários que são autorizados pelo detentor da informação.

No Brasil, o Departamento de Segurança da Informação e Comunicações – DSCI, do Gabinete de Segurança Institucional, da Presidência da República, é o órgão responsável pela

[30] GOUVEIA, L. **Gestão da segurança da informação**. Livro V.1.1. Porto, 2016.

política de informação no país. Tendo como missão de acordo com o decreto Decreto Nº 8.577, de 26 de novembro de 2015:

I. Orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da administração pública federal;

II. Definir normativos e requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal, no âmbito da Secretaria-Executiva do Conselho de Defesa Nacional;

III. Operacionalizar e manter o centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

IV. Avaliar tratados, acordos ou atos internacionais relacionados ao tratamento e à troca de informação classificada;

V. Exercer, por meio do Núcleo de Segurança e Credenciamento, na qualidade de Órgão de Registro Central, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação classificada; e

VI. Exercer outras atribuições que lhe forem determinadas pelo Assessor Chefe da Assessoria Especial da Secretaria-Executiva do Conselho de Defesa Nacional.

Cumprindo a sua missão institucional, o Departamento de Segurança da Informação e Comunicações – DSCI elabora instruções normativas que norteiam a política de tratamento da informação nos órgãos e entidades da administração pública federal, sendo este seguido pelos demais entes da federação em suas próprias legislações. A Norma Complementar nº 20 da Instrução Normativa nº 01 GSI-PR (NC20/IN01/DSIC/GSIPR), estabelece diretrizes para o tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal. Em seu interior destacamos o item 6.3 Uso e Disseminação, no qual ressaltamos dentre os 16 subitens que o compõem, os seguintes:

6.3.1 A utilização, o acesso, a reprodução, o transporte, a transmissão e a distribuição à informação devem seguir os princípios da disponibilidade, integridade, confidencialidade e autenticidade, conforme normativos de SIC e legislação vigente, bem como orientações específicas que garantam a salvaguarda de informação sigilosa e pessoal, bem como a divulgação de informação ostensiva;

6.3.2 Nas reuniões em que é tratada informação sigilosa e pessoal, devem ser adotados controles de segurança para acesso ao ambiente, aos documentos, as anotações, as mídias e aos demais recursos utilizados;

6.3.3 A informação deve ser utilizada para atender os interesses dos órgãos e entidades da APF, não devendo ser usada para propósito pessoal de agente público ou privado.

6.3.4 A informação a ser disponibilizada por meio da transparência ativa e passiva deve ser objeto de prévia análise a fim de que se identifiquem parcelas da informação com restrição de acesso.

Observamos que no subitem 6.3.1 além dos três aspectos associados à informação, que são a confidencialidade, a integridade e a disponibilidade, há outro chamado de autenticidade. Este pode ser definido segundo a LAI[31] e o GSI-PR (BRASIL, 2011; GSI-PR, 2008a, p. 2) como sendo "*relacionado à qualidade ou à propriedade da informação que tenha sido produzida, expedida, recebida ou modificada por pessoas, organizações ou sistemas*".

Com base na Norma Complementar nº 20 da Instrução Normativa nº 01 GSI-PR, o DSCI elaborou o chamado Quadro Exemplificativo de Tipos de Informação (ver o Quadro 2.1).

Os ataques e ameaças associados à segurança da informação estão cada vez mais presente após a globalização e a expansão da rede mundial, a Internet. A sua negligência pode ocasionar roubo, perda ou alteração de dados pessoais ou empresariais, e principalmente os dados governamentais, provocando assim prejuízos incalculáveis tantos financeiros quanto ao Estado democrático e à soberania nacional. Essas ameaças estão inteiramente relacionadas com a ruptura de um dos 3 aspectos críticos que são os pilares que garantem a segurança da informação, podendo essas rupturas serem caracterizadas ou exemplificadas da seguinte maneira:

- Quando ocorre quebra de senha de um usuário ou administrador que permitisse expor o sigilo de informações restritas, há **Perda de Confidencialidade**;
- Quando acontece de uma determinada informação ficar exposta a manipulação de pessoa que não tenha autorização para tal, e a mesma realizar modificações sem a permissão do responsável ou proprietário, há **Perda de Integridade** e;
- Quando advém da informação deixar de ser acessível por quem precisa dela devido a ato de pessoa sem autorização com ou sem má fé, ou mesmo erro causado por defeito de equipamento, no caso é **Perda de Disponibilidade.**

[31] Lei de Acesso à Informação.

Quadro 2.1: Exemplos de tipos de informação

TIPO	DESCRIÇÃO
1. OSTENSIVA	Transparência Ativa
	Transparência Passiva
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 Reservada – Prazo máximo de restrição de acesso de 5 anos
	2.2 Secreta – Prazo máximo de restrição de acesso de 15 anos
	2.3 Ultrassecreta – Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 Sigilos Decorrentes de Direitos de Personalidade
	3.1.1 Sigilo Fiscal
	3.1.2 Sigilo Bancário
	3.1.3 Sigilo Comercial
	3.1.4 Sigilo Empresarial
	3.1.5 Sigilo Contábil
	3.2 Sigilos de Processos e Procedimentos
	3.2.1 Acesso a Documento Preparatório
	3.2.2 Sigilo do Procedimento Administrativo Disciplinar em Curso
	3.2.3 Sigilo do Inquérito Policial
	3.2.4 Segredo de Justiça no Processo Civil
	3.2.5 Segredo de Justiça no Processo Penal
	3.3 Informação de Natureza Patrimonial
	3.3.1 Segredo Industrial
	3.3.2 Direito Autoral e Propriedade Intelectual de Programa de Computador
	3.3.3 Propriedade Industrial
4. PESSOAL	4.1. Pessoal – Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.

Fonte: GSI-PR (2014a, p. 12).

De certo modo, a segurança da informação torna-se imperativa nas questões de minimização dos riscos que estão conexos com as atividades do órgão, seja ele público ou privado, assegurando assim a veracidade e legalidade da informação. Portanto, para que a transparência nas informações tenha o seu conteúdo íntegro e confiável nos portais onde são divulgadas, a segurança é um fator preponderante para que a credibilidade seja mantida.