CONTROLADORIA E OUVIDORIA GERAL DO ESTADO *Governo do Estado do Ceará*		
Procedimento: **POLÍTICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**	Código: **N.COTIC.001**	Folha: **1/15**
Processo: **TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**	Primeira Edição: **01/12/14**	
Área: **COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**	Edição: **1ª**	Data: **01/12/2014**

CONTROLE DE APROVAÇÃO

ELABORADO	REVISADO POR	APROVADO
Maurício Mazzanati de Oliveira	Carlos Jorge Lima de Freitas	Paulo Roberto de Carvalho Nunes
		Denise Andrade Araújo
		Anastácia da Silva Santos

HISTÓRICO DE MODIFICAÇÕES

EDIÇÃO	DATA	ALTERAÇÕES EM RELAÇÃO À REVISÃO ANTERIOR
01	01/12/2014	Edição inicial

ÍNDICE

1. OBJETIVO

O objetivo desta Política de Segurança é estabelecer diretrizes e normas gerais para a gestão da segurança da informação dos ambientes de Tecnologia da Informação e Comunicação (TIC) da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE), de acordo com as condições e recursos tecnológicos disponíveis, de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, descrevendo procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

2. ABRANGÊNCIA

A Política de Segurança da Informação deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação, como também às atividades de todos os agentes públicos, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

3. COMPETÊNCIAS

3.1. Compete à Direção Superior da CGE zelar pelo fiel cumprimento ao estabelecido nesta Norma;

3.2. Compete à Coordenadoria Administrativo-Financeira (COAFI) a gestão patrimonial, compreendendo a aquisição de bens de consumo e permanentes necessários ao funcionamento da instituição;

3.3. Compete à Célula de Logística e Patrimônio (COAFI/CELOG) controlar o estoque de bens de consumo e a movimentação física de bens permanentes, compreendendo transferências, empréstimos, comodatos, devoluções, alienações, doações e baixas;

3.4. Compete à Coordenadoria de Tecnologia da Informação e Comunicação (COTIC) implantar, administrar e efetuar a atualização periódica desta Norma;

3.5. Compete aos agentes públicos cumprirem as determinações constantes nesta Norma, independentemente do nível hierárquico ou função, bem como do vínculo empregatício.

4. SIGLAS E CONCEITUAÇÕES

4.1. Agente Público: É toda pessoa que presta um serviço público, sendo funcionário público ou não, sendo remunerado ou não, sendo o serviço temporário ou não. É todo aquele que exerce ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação, ou qualquer forma de investidura, mandato, cargo, emprego ou função pública;

4.2. Ativo: Qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004];

4.3. *Backup*: Cópia de segurança de dados;

4.4. *Backups* críticos: São cópias de segurança de dados críticos;

4.5. *Backups* especiais: São cópias de segurança de dados efetuados sob demanda específica;

4.6. *Backups* históricos: São cópias de segurança de dados efetuados de forma periódica e rotineira;

4.7. CELOG: Célula de Logística e Patrimônio;

4.8. CGE: Controladoria e Ouvidoria Geral do Estado do Ceará;

4.9. COAFI: Coordenadoria Administrativo-Financeira;

4.10. COTIC: Coordenadoria de Tecnologia da Informação e Comunicação;

4.11. Dados críticos: Informações restritas com classificação de sigilo;

4.12. Dispositivos móveis: Qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição como: *notebooks*, *smartphones* e *pendrives*;

4.13. Janela de *backup*: Períodos em que não há qualquer acesso de usuários ou processos automatizados aos sistemas de informática;

4.14. PCN: Plano de Continuidade de Negócios;

4.15. *Restore*: Restauração de cópia de segurança de dados;

4.16. SPAM: O termo *spam* significa *Sending and Posting Advertisement in Mass*, ou "enviar e postar publicidade em massa", ou também: envio de mensagens não-solicitadas, sem propósito específico ao destinatário final;

4.17. TIC: Tecnologia da Informação e Comunicação.

5. NORMAS E PROCEDIMENTOS

5.1. Uso de equipamentos da CGE

No que se refere aos dispositivos móveis

Na utilização dos ativos de TIC, é obrigação do agente público responsável pelo equipamento:

5.1.1. Responsabilizar-se pelo ativo de TIC e por sua adequada utilização, conforme estabelecido no procedimento P.COAFI.004 e nesta Política de Segurança da

Informação, além do comprometimento com a devolução nas mesmas condições físicas apresentadas no momento de seu recebimento, consideradas as alterações decorrentes da utilização adequada do ativo;

5.1.2. Em caso de roubo, furto ou danos do ativo de TIC, somente será exigida a reposição ou manutenção do mesmo, conforme o caso, quando caracterizado que o evento decorreu de conduta dolosa ou de culpa exclusiva do agente público, a ser apurada por meio de sindicância, na forma da legislação vigente;

5.1.3. Nos casos reportados no item 5.1.2, o agente público responsável pelo ativo de TIC deverá apresentar à COTIC:

a. Boletim de Ocorrência (BO) emitido pela autoridade policial competente, somente no caso de roubo ou furto;

b. Declaração de testemunha(s) referente ao fato ocorrido, quando existir;

c. Comprovação da utilização para fins de trabalho do ativo de TIC, através de declaração do gestor imediato.

5.1.4. Em caso de dano, comunicar formalmente à COTIC através do sistema de abertura de chamados da CGE;

5.1.5. Caso seja diagnosticado pela COTIC que o dano é claramente em decorrência de uso continuado do equipamento, ficam dispensados os procedimentos relativos aos itens 5.1.2 e 5.1.3;

5.1.6. Em qualquer situação que implique baixa ou transferência de responsabilidade do ativo de TIC, sempre que se entender necessário ou por simples medida de segurança, poderá ser solicitado diagnóstico técnico sobre as condições físicas do equipamento, a ser emitido pela COTIC.

No que se refere aos demais equipamentos

5.1.7. Fica o usuário responsável por solicitar através do sistema de abertura de chamados da CGE, qualquer movimentação de equipamento/periférico necessária;

5.1.8. Em caso de danos no equipamento, somente será exigida a manutenção do mesmo pelo agente público quando caracterizado que o evento decorreu de conduta dolosa ou culpa exclusiva do agente, a ser apurada por meio de sindicância, na forma da legislação vigente;

5.1.9. Em caso de roubo ou furto do equipamento, o agente público que constatar a ocorrência deverá comunicar o fato ao seu gestor, que solicitará à COAFI a adoção das providências cabíveis.

5.2. Uso da rede da CGE

É obrigação do agente público:

5.2.1. Utilizar os serviços e recursos para as necessidades autorizadas, tais como, desenvolvimento de trabalhos administrativos, gerenciais e afins;

5.2.2. Proteger sua senha de acesso contra uso indevido, responsabilizando-se por todas as atividades originadas a partir de sua identificação;

5.2.3. Acessar somente arquivos e dados referentes ao escopo de trabalho do próprio agente público;

5.2.4. Usar os serviços de forma otimizada e compartilhada, evitando desperdícios tais como utilização inadequada do tempo de rede, *Internet*, de impressão e espaço em disco;

5.2.5. Utilizar somente programas legalizados ou analisados tecnicamente pela COTIC, sendo expressamente proibido o uso/instalação de *software* não licenciado.

É vedado ao agente público:

5.2.6. Divulgar sua senha de acesso à rede para qualquer pessoa, pois a informação é de caráter pessoal e intransferível;

5.2.7. Utilizar arquivos e dados de outro agente público, sem a devida autorização;

5.2.8. Utilizar identidade falsa para uso do correio eletrônico ou outros usos da rede;

5.2.9. Enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação;

5.2.10. Desenvolver, manter, utilizar e divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus, disseminação de *software* não licenciado ou homologado e propagação de mensagens do tipo *spam*;

5.2.11. Utilizar os serviços e recursos da CGE para intimidar, assediar ou difamar qualquer pessoa;

5.2.12. Utilizar os serviços e recursos da CGE para armazenar, divulgar ou transmitir material ofensivo e abusivo;

5.2.13. Acessar, via *Internet*, *sites* que comprometam a segurança, vão de encontro à cultura organizacional, infrinjam a legislação e/ou que comprometam as normas estabelecidas da CGE, a exemplo de *sites* pornográficos e de conteúdo discriminatório;

5.2.14. Participar, no horário do expediente, de listas de discussão, *newsgroups*, sessões de *chat* e redes sociais que não estejam em conformidade com as atividades institucionais da CGE;

5.2.15. Realizar qualquer procedimento que envolva suporte técnico, tais como manutenção de equipamentos, instalação de *software*, alteração nas configurações do sistema e outras similares, sem a devida autorização da COTIC;

5.2.16. Utilizar os serviços e recursos da CGE para fins comerciais, políticos e particulares, tais como mala direta, propaganda política e venda de objetos pessoais e/ou comerciais.

6. DIRETRIZES GERAIS

6.1. Qualquer violação às normas acima apresentadas sujeitará o infrator a sanções disciplinares, previstas em lei, em especial na Lei nº 9.826/74 – Estatuto dos Funcionários Públicos Civis do Estado, Arts. 174 a 233, além do cancelamento da utilização dos serviços e recursos oferecidos e da adoção das medidas administrativas e judiciais cabíveis;

6.2. Compete à COTIC, na condição de administradora dos ativos de TIC instalados na CGE, por intermédio de técnicos previamente credenciados, acessar quaisquer arquivos residentes na rede ou nos equipamentos da CGE, quando tal medida for indispensável para a manutenção e a segurança do ambiente de TIC;

6.3. O ativo de TIC constitui patrimônio público, devendo ser disponibilizado para os agentes públicos/sociedade que dele necessitem;

6.4. Qualquer falha porventura detectada por qualquer agente público/sociedade na segurança de TIC deverá ser informada à COTIC;

6.5. Aos casos omissos deverá ser aplicada a legislação atinente à responsabilidade por danos ao patrimônio público;

6.6. As questões não expressamente documentadas neste instrumento obedecerão ao disposto no Decreto Estadual nº 29.227, de 13 de março de 2008.

7. CONTROLE DE ACESSOS

Diretrizes específicas e procedimentos próprios de controle de acesso lógico são fixados através do procedimento P.COTIC.004, considerando as seguintes diretrizes gerais:

7.1. O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação da CGE;

7.2. A criação e a administração de contas serão realizadas de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

7.3. O acesso à rede corporativa dar-se-á de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo de 01 (um) ano;

7.4. As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

8. BACKUP

Diretrizes específicas e procedimentos próprios de cópias de segurança de dados (*Backups*) são fixados através do procedimento P.COTIC.002, considerando as seguintes diretrizes gerais:

8.1. O serviço de *backup* deve ser orientado para a salvaguarda e retenção dos dados e o processo de restauração das informações deverá ocorrer quando houver indisponibilidade de serviços que dependam da operação de recuperação;

8.2. O serviço de *backup* deve ser preferencialmente automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas "janelas de *backup*";

8.3. A solução de *backup* deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros);

8.4. A administração das mídias de *backup* deverá ser contemplada nos respectivos procedimentos complementares, objetivando manter sua segurança e integridade;

8.5. As mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres;

8.6. Os *backups* críticos para o bom funcionamento dos serviços da CGE exigem uma regra de retenção especial, a ser prevista no procedimento P.COTIC.002 e devem estar de acordo com as normas de classificação da informação pública, na forma da Lei Estadual nº 15.175, de 28 de junho de 2012, seguindo ainda as determinações fiscais e legais existentes no país;

A execução de rotinas de *backup* e *restore* deverá ser rigidamente controlada, documentada e auditada, nos termos e procedimentos implementados através do P.COTIC.002.

9. PLANO DE CONTINUIDADE DE NEGÓCIOS

Nos termos do procedimento P.COTIC.003, o Plano de Continuidade de Negócios (PCN) busca minimizar os impactos nas atividades da CGE, decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, considerando as seguintes diretrizes gerais:

9.1. O PCN é constituído de documentação com orientações e informações necessárias para que a CGE mantenha seus ativos de informação e a continuidade de suas atividades críticas, num nível previamente definido, em casos de incidentes;

9.2. O Plano acima indicado deverá ser testado e revisado periodicamente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;

9.3. As orientações e informações previstas no PCN deverão ser executadas em conformidade com os requisitos de segurança da informação e comunicação necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, incluindo as pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicação.

10. TRATAMENTO DA INFORMAÇÃO

São princípios da Política de Segurança da Informação da CGE:

10.1. Toda informação produzida ou recebida pelos agentes públicos, em resultado da função exercida ou atividade profissional contratada, pertence à CGE, e as exceções devem ser explícitas e formalizadas entre as partes;

10.2. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade;

10.3. Todo o acesso à rede do órgão deverá ser feito por meio de *login* de acesso único, pessoal e intransferível;

10.4. A CGE/COTIC pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pelo órgão;

10.5. Cada usuário é responsável pela segurança das informações dentro da CGE, principalmente daquelas que estão sob sua responsabilidade;

10.6. Deverá constar em todos os contratos da CGE, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser cumprida por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na CGE, inclusive provenientes de organismos internacionais;

10.7. Deverá estar prevista, por parte das empresas e dos profissionais prestadores de serviço, entrega do Termo de Compromisso de Confidencialidade e Segurança da Informação e do Termo de Ciência Individual de Confidencialidade e Segurança da Informação (Anexos I e II), como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição;

10.8. Esta Política de Segurança da Informação será implementada na CGE por meio desta Norma e de procedimentos específicos no âmbito do Sistema de Gestão da Qualidade, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como do vínculo empregatício.

11. REVISÃO

Esta Norma será validada anualmente e revisada sempre que necessário, em decorrência do processo de melhoria contínua do Sistema de Gestão da Qualidade.

12. APROVAÇÃO

NOME	FUNÇÃO	ASSINATURA
Paulo Roberto de Carvalho Nunes	Presidente do Comitê da Qualidade	
Denise Andrade Araújo	Coordenadora da Qualidade	
Anastácia da Silva Santos	Secretária do Comitê da Qualidade	
Carlos Jorge Lima de Freitas	Coordenador de Tecnologia da Informação e Comunicação	

13. REFERÊNCIAS BIBLIOGRÁFICAS

- *ABNT ISO/IEC 13335-1: 2004 – Tecnologia da Informação - Técnicas de Segurança - Gestão de Segurança de Tecnologia da Informação e Comunicação - Parte 1: Conceitos e Modelos para o Gerenciamento da Segurança de Tecnologia da Informação e Comunicação;*

- *Decreto Estadual nº 29.227, de 13/03/2008 – Dispõe sobre a Instituição da Política de Segurança da Informação dos Ambientes de Tecnologia da Informação e Comunicação - TIC do Governo do Estado do Ceará e do Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI;*

- *Lei Estadual nº 15.175, de 28/06/2012 – Dispõe sobre o Acesso à Informação no âmbito da Administração Pública do Estado do Ceará;*

- *Lei Estadual nº 9.826/74, de 14/05/1974 – Estatuto dos Funcionários Públicos Civis do Estado do Ceará.*

14. CONTROLE DE REGISTRO DA QUALIDADE

IDENTIFICAÇÃO	ARMAZENAMENTO	PROTEÇÃO	RECUPERAÇÃO		RETENÇÃO	DISPOSIÇÃO
			INDEXAÇÃO	ACESSO		
Registro de *Logs* através do sistema de abertura de chamados da CGE	Registro digital inerente ao sistema de abertura de chamados da CGE	*Backup*	Cronológica	COTIC	1 Ano	Subscrição

15. ANEXOS

ANEXO I – MODELO DE TERMO DE COMPROMISSO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO.

GOVERNO DO ESTADO DO CEARÁ

SEGUNDO TERMO ADITIVO AO CONTRATO Nº XXXX, QUE ENTRE SI CELEBRAM A CONTROLADORIA E OUVIDORIA GERAL – CGE E A EMPRESA XXXX NA FORMA ABAIXO.

O Estado do Ceará, por intermédio da Controladoria e Ouvidoria Geral do Estado - CGE, sediada na Av. Gal. Afonso Albuquerque Lima s/n - Ed. Seplag - 1º andar, CEP 60.822-325 - Cambeba - Fortaleza - Ceará, CNPJ n.º [illegible], doravante denominado **CONTRATANTE**, neste ato representada pela sua Secretária de Estado Chefe da Controladoria e Ouvidoria Geral, Sra. Silvana Helena Correia Vidal, [illegible], portadora do CPF nº [illegible], RG nº [illegible], expedido pela SSP/CE e, de outro lado, a «Contratada», sediada em «Endereço Contratada», CNPJ n.º «CNPJ Contratada», doravante denominada **CONTRATADA**, representada neste ato por seu «Diretor/Presidente», Sr.(a) XXXXX, «Qualificações», resolvem aditar o CONTRATO Nº, mediante as cláusulas e condições seguintes:

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Cláusula Primeira – DO OBJETO

Constitui objeto deste ADITIVO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO Nº XXXXX celebrado entre as partes, nos termos da Lei nº [illegible] de [illegible], que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, publicações, compilações, código-fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, ideias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO celebrado entre as partes.

§1º – Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO.

§2º – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO.

Centro Administrativo Governador Virgílio Távora – Av. Gal. Afonso Albuquerque Lima s/n – Ed. Seplag – 2º andar
CEP 60.822-325 – Cambeba – Fortaleza/CE – Fone: (85) 3101-[illegible] – Fax: (85) [illegible]

GOVERNO DO ESTADO DO CEARÁ

Parágrafo Terceiro – As obrigações constantes deste ADITIVO não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente ADITIVO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO, em conformidade com o disposto neste ADITIVO.

§1º – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2º – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO sobre a existência deste ADITIVO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente ADITIVO e dará ciência à CONTRATANTE dos documentos comprobatórios.

§3º – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§4º – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste ADITIVO.

I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

§5º – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO.

§6º – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA DO SIGILO DA INFORMAÇÃO

O sigilo da informação tem natureza irrevogável e irretratável, permanecendo em vigor desde a data da assinatura do CONTRATO até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que tratam desse assunto, conforme Art. 32 da Lei nº 12.527/2012.

Cláusula Sétima – DISPOSIÇÕES GERAIS

As demais cláusulas do CONTRATO permanecem inalteradas.

Centro Administrativo Gov. Virgílio Távora – Av. Gal. Afonso Albuquerque Lima, S/N – Ed. SEPLAG – [illegible] andar
CEP: 60.822-325 – Cambeba – Fortaleza/CE – Fone: (85) [illegible] – Fax: (85) [illegible]

GOVERNO DO ESTADO DO CEARÁ

E, por assim estarem justas e estabelecidas as condições, o presente ADITIVO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

Fortaleza, de de 2014

CONTRATANTE	CONTRATADA
ASSINATURA	ASSINATURA
Nome do Responsável pelo Contratante Cargo / Matrícula Coordenação / Departamento	Nome do Responsável pela Contratada Cargo / Matrícula Coordenação / Departamento

TESTEMUNHAS

ASSINATURA	ASSINATURA
Nome: RG Nº CPF Nº	Nome: RG Nº CPF Nº

VISTO - ASSESSORIA JURÍDICA

ASSINATURA

ANEXO II – MODELO DE TERMO DE CIÊNCIA INDIVIDUAL DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO.

GOVERNO DO ESTADO DO CEARÁ
Controladoria e Ouvidoria Geral do Estado

TERMO DE CIÊNCIA INDIVIDUAL

CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO CONTRATO:

Nº do Contrato	*Digite nº do Contrato*
Nome da Empresa	*Digite Nome da Empresa Contratada*
CNPJ da Contratada	*Informe objeto CNPJ*
Objeto resumido	*Informe objeto resumido*
Vigência Contratual	*Informe vigência*

TERMOS:

O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo nº / , bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.

OBSERVAÇÕES:

Digite observações, se houver.

DE ACORDO:

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

Local, dia/mês/ano	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)	
Nome: **Identidade:** **CPF:** **Função:**	**Assinatura:**
Nome: **Identidade:** **CPF:** **Função:**	**Assinatura:**
Nome: **Identidade:** **CPF:** **Função:**	**Assinatura:**
Nome: **Identidade:** **CPF:** **Função:**	**Assinatura:**
Nome: **Identidade:** **CPF:** **Função:**	**Assinatura:**

Centro Administrativo Gov. Virgílio Távora – Av. Gal. Afonso Albuquerque Lima s/n – Ed. Seplag – 2º andar
CEP: 60.822-352 – Cambeba – Fortaleza/CE – Fone: (85) 3101 3467 – Fax: (85) 3101 3480