GOVERNO DO
ESTADO DO CEARÁ
Procuradoria Geral do Estado

PORTARIA Nº 010/2010.

Dispõe sobre o armazenamento, localização e segurança dos dados e documentos digitais da Procuradoria Geral do Estado do Ceará – PGE.

O **PROCURADOR-GERAL DO ESTADO**, no uso de suas atribuições legais, referidas pelo art. 8. da Lei Complementar nº 58, de 31 de março de 2006.

CONSIDERANDO a portaria Nº 005/2010 da PGE, que regulamenta e determina o uso de recursos de certificação digital.

CONSIDERANDO a necessidade de normatizar os procedimentos para gravação, manutenção, recuperação e segurança dos documentos digitais, de forma que toda a solução possa ser segura e auditável, fundamentada na Medida Provisória Nº 2.200-2, nos decretos, resoluções, instruções normativas e portarias da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil do Instituto Nacional de Tecnologia da Informação – ITI.

CONSIDERANDO a necessidade de adequação as novas tendências de Governança de Tecnologia da Informação e ao uso de documentos eletrônicos assinados digitalmente, permitindo auditorias baseadas em padrões internacionais como *Control Objectives for Information and related Technology - COBIT* e *Information Technology Infrastructure Library - ITIL*.

RESOLVE:

Art. 1º Regulamentar os procedimentos para classificação de segurança, definições do ciclo de vida, gravação, manutenção e recuperação dos dados e documentos digitais no âmbito da Procuradoria Geral do Estado do Ceará.

Art. 2º Definições gerais

§ 1º Considera-se **Repositório Digital**, um ambiente o qual serão armazenados todos os registros e documentos originados dos sistemas de informação da PGE, criado com o objetivo de normatizar e padronizar as formas de armazenamento, manutenção e recuperação de informações por meio eletrônico.

§ 2º Considera-se **Dado**, a menor representação de um fato, que associado a outros dados e processados, geram informações.

§ 3º Cada dado deverá ter uma classificação de segurança.

§ 4º Considera-se **Sistema de Atividade Funcional - SAF**, pequenos sistemas que somados a outros, formarão a função que os colaboradores deverão executar através de meio eletrônico. Cada SAF deverá gerar um produto de dados que serão armazenados em tabelas de banco de dados e arquivos do sistema operacional.

§ 5º Considera-se **Sistema de Repositório Digital - SRD**, pequenos sistemas que deverão implementar serviços de gravação de registros e arquivos.

§ 6º Todos os processos e documentos eletrônicos deverão ser gravados de forma a garantir acessos seguros, facilidade de localização, proteção contra sinistros e procedimentos de auditoria.

§ 7º Para possibilitar a interoperabilidade entre instituições, será adotado formato de arquivo com extensão p7s, conforme padrões ICP-Brasil.

§ 8º Cada **SAF** deverá ter um SRD correspondente que conterá duas formas de armazenamento: 1-Banco de Dados e 2-Sistema de Arquivos (caso seja gerado ou anexado documento).

§ 9º Os **SAF's**, somente deverão implementar rotinas de localização e inserção de registros, não devendo implementar alteração e exclusão. A alteração deverá seguir os seguintes procedimentos: 1-Localizar registro, 2-Carregar página da atividade com os dados do registro localizado, 3-Permitir alteração da cópia, 4-Inserir um registro de banco e de arquivo versionado, mantendo intactos os registros e documentos das inserções anteriores.

§ 10º Cada **SRD** deverá prover serviços de gravação de novos registros e arquivos.

§ 11º As operações de extração, exportação e indexação para banco de dados de informações gerenciais e índices de consulta, deverão utilizar os serviços de acesso oferecidos pelos serviços do **SRD**.

§ 12º No caso de documentos assinados digitalmente deverão ser gravados o documento original e o documento assinado com extensão P7S.

Art. 3º Definições de níveis de acesso a dados e documentos armazenados

§ 1º As informações serão disponibilizadas sob os níveis de segurança listados abaixo na Tabela 3.1, estes níveis de segurança deverão ser atribuídos no momento da análise e especificação do **SAF**.

§ 2º A aplicação da segurança de acesso acontecerá no momento em que o cidadão ou colaborador realizar uma atividade de consulta, neste momento serão avaliados: a situação atual do fluxo do processo que gerou o dado ou o documento, a disponibilidade de acesso público e a função do colaborador conectado, de forma que qualquer requisição seja processada e então filtrada conforme os requisitos da Tabela 3.1 listadas abaixo.

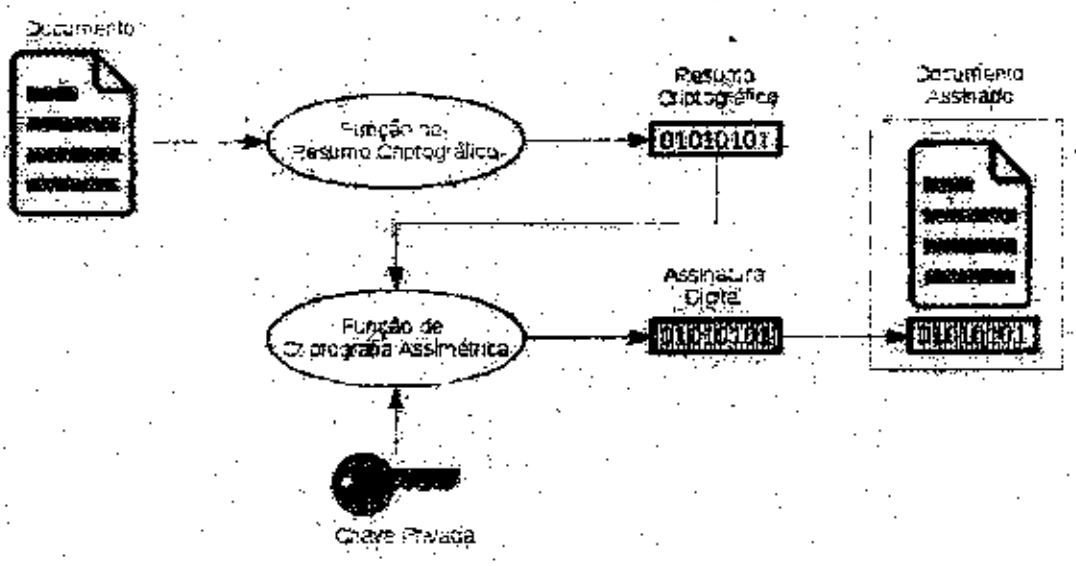
Código do Nível	Visão Externa (Acesso anônimo)	Visão Interna (Acesso Identificado)	Visão Governadoria
ID-SGR-01	Acessível em todo o ciclo de vida do fluxo	Acessível em todo o ciclo de vida do fluxo	Acessível
ID-SGR-02	Acessível após o término do ciclo de vida do fluxo	Acessível em todo o ciclo de vida do fluxo para as funções operadoras do fluxo	Acessível
ID-SGR-03	Sem acesso	Acessível no âmbito da instituição que criou o processo	Acessível
ID-SGR-04	Sem acesso	Acessível no âmbito da área da instituição que criou o processo	Acessível
ID-SGR-05	Sem acesso	Acessível no âmbito da função de uma área da instituição que criou o processo	Acessível

ID-SGR-06	Sem acesso	Acessível no âmbito do colaborador que criou o processo	Acessível

Tabela 3.1 – Níveis de segurança para acesso a dados e documentos.

Art. 4º Fluxos do Repositório Digital

§ 1º O processo criptográfico de criação de uma assinatura digital deve ser como apresentado abaixo:



I - O signatário gera um resumo criptográfico de um documento eletrônico;

II - O signatário cifra o resumo criptográfico com sua chave privada, associada a uma chave pública constante do seu certificado digital, gerando a assinatura digital;

III - O documento eletrônico e a assinatura digital ficam associados para fortura validação.

§ 2º Fluxo de gravação do **SAF** e do **SRD**

I – O **SAF** deverá gravar de forma atômica (todas as operações ou nenhuma) o produto da atividade (Registro e Arquivos) no seu banco de dados e pasta, utilizando o serviço do **SRD** para gravar no repositório digital.

§ 3º Fluxo de indexação de registros e documentos gerados pelo **SAF**

I – Um sistema de indexação de registros e documentos será executado a cada gravação do **SRD**, de forma a garantir pesquisas online dos dados e documentos pelos **SAF's**.

II – As pesquisas serão disponibilizadas através da internet utilizando o sistema **BUSCADOR PGE (www.pge.ce.gov.br)**, que permitirá a localização de processos e documentos utilizando números de identificação, nomes de pessoas ou qualquer dado gravado nos repositórios digitais.

Art. 5º Estrutura do banco de dados e de pastas do repositório digital

§ 1º A arquitetura de armazenamento de registros de banco de dados e arquivos de Sistema Operacional (SO), deverão ser implementadas de forma a garantir: escalabilidade, redundância, backup e performance, organizados da seguinte forma:

I – Banco de dados e Pastas SAF
II – Banco de dados e Pastas SRD
III – Estrutura de indexação
IV – Informações Gerenciais (Dataware house – DW)

§ 2º Especificação das tabelas do repositórios digitais

I – O nome do esquema do repositório da atividade deverá ter o mesmo nome do esquema da atividade sucedido de **rpd** (Repositório Digital). Ex: nome do esquema de atividade – **adm_pgeatv0010**, nome do esquema do repositório digital – **adm_pgeatv0010_rpd**.

II – Definição dos campos e tipos dos repositórios digitais

Campo	**Tipo**
Nome da Instituição	Texto
CNPJ da Instituição	Número
Nome da Área	Texto
Nome da Função	Texto
Nome do Colaborador	Texto
CPF do Colaborador	Número
Número sequencial do Processo	Texto
Resumo do Processo	Texto
Número do Protocolo do Estado	Texto
Código da Atividade	Texto
Descrição da Atividade	Texto
Número do Passo	Número
Descrição do Passo	Texto
Código do Andamento	Número
Número Sequencial de Andamentos do Processo	Número
Número de identificação única do Documento	Texto
Tamanho do Documento	Número
YAML/JSON da Atividade	Texto
Código da Classificação de Segurança	Texto
Data e Hora do Armazenamento	Data/Hora

Tabela 5.1 – Campos de tabelas de repositório digital.

§ 3º Estrutura de pastas do repositório digital

I - O sistema de Repositório Digital deverá obedecer a seguinte estrutura de diretório:

Repositorio Digital → Formula500 → Número sequencial do Processo → Código da Atividade → Número Sequencial de Andamentos do Processo

a) Formula500 = Parte Inteira do "Número sequencial do Processo" dividido por 500.

Art. 6º Ciclo de vida da assinatura digital

§ 1º O ciclo de vida de uma assinatura digital compreende os processos descritos abaixo, conforme Tabela 6.1:

Processo	Descrição
Criação	Criação de um código logicamente associado a um conteúdo digital e a chave criptográfica privada do signatário.
Verificação ou validação	Verificação quanto a validade de uma ou mais assinaturas digitais logicamente associada a um conteúdo digital.
Armazenamento	Guarda da assinatura digital. Compreende os cuidados para conversão dos dados para mídias mais atuais, sempre que necessário.
Revalidação	Processo que estende a validade do documento assinado, por meio da reassinatura dos documentos ou da aposição de carimbos do tempo, quando da expiração ou revogação dos certificados utilizados para gerar ou revalidar as assinaturas, ou ainda quando do enfraquecimento dos algoritmos criptográficos ou tamanhos de chave utilizados.

Tabela 6.1: Ciclo de vida da assinatura digital

§ 2º As assinaturas digitais deverão ser criadas com características apropriadas a finalidade e longevidade esperada. Uma assinatura digital pode incorporar elementos que permitam uma validação confiável a longo prazo.

Art. 7º Ciclo de vida de armazenamento e expurgo de documentos digitais

§ 1º Os documentos armazenados em meio digital na PGE deverão ser mantidos por um período mínimo de 10 (dez) anos e no máximo 20 (vinte) anos a partir do armazenamento no repositório digital, salvo alguma legislação que trate de forma específica determinados documentos.

§ 2º As considerações e as ações relativas ao armazenamento dos documentos institucionais digitais permeiam todo seu ciclo de vida. Esse armazenamento deve garantir a integridade e o acesso aos documentos.

§ 3º O ciclo de vida dos documentos refere-se as sucessivas etapas pelas quais passam: produção, tramitação, uso, avaliação, arquivamento e destinação (arquivamento permanente, cópias as partes ou eliminação).

§ 4º Seguem abaixo requisitos de armazenamento organizados segundo os critérios de durabilidade, capacidade e viabilidade técnica.

I - Utilizar dispositivos e padrões estáveis no mercado.

II - Avaliar periódicamente a escolha de dispositivos sempre que a evolução tecnológica indicar mudanças importantes.

III - Efetuar migrações preventivas sempre que se tornar patente ou previsível a obsolescência do padrão corrente.

IV - Possuir capacidade de armazenamento suficiente para a acomodação de todos os documentos, metadados e suas cópias de segurança.

V - Prever a possibilidade de expansão da estrutura de armazenamento.

VI - Oferecer ao administrador facilidades para a monitoração da capacidade de armazenamento.

VII - Informar automaticamente ao administrador quando os dispositivos de armazenamento *online* atingirem níveis de alerta e níveis críticos de ocupação.

VII - Manter estatísticas de taxa de crescimento de utilização de memória secundária e terciária para fornecer ao administrador previsões de exaustão de recursos.

VIII - Utilizar técnicas de restauração de dados em caso de falhas.

IX - Utilizar mecanismos de proteção que previnam alterações indevidas e mantenham a integridade dos dados armazenados.

X - A integridade dos dispositivos de armazenamento deve ser periodicamente verificada.

§ 5º A eliminação de documentos institucionais somente poderá ser realizada de acordo normas e padrões da legislação vigente.

§ 6º Os procedimentos para eliminação de documentos institucionais de um Repositório Digital terão de ser executados somente após o vencimento de sua validade e de forma controlada, fazendo-se registro nos metadados e trilha de auditoria.

§ 7º Eliminar significa destruir os documentos que, na avaliação, foram considerados sem valor para a guarda permanente. A eliminação deve ser precedida da elaboração de listagem, do documento de ciência de eliminação e do termo de eliminação, de acordo com a legislação vigente, e deve obedecer aos seguintes princípios:

I - A eliminação deverá sempre ser autorizada por comissões de avaliação e por grupos de trabalho com base em procedimentos definidos conforme a legislação vigente.

II - A eliminação deverá ser realizada de forma a impossibilitar a recuperação posterior de qualquer informação confidencial contida nos documentos eliminados, como, por exemplo, dados de identificação pessoal ou assinatura.

III- Os SAF's deverão informar da eliminação do processo em caso de consulta.

§ 8º Quando se proceder a eliminação de documentos, as memórias de suporte devem ter suas informações efetivamente indisponibilizadas.

§ 9º A eliminação de um documento não implica a eliminação de seus metadados. As informações devem ser eliminadas de forma irreversível, incluindo, no caso de memória terciária, a possibilidade de destruição física das mídias.

Art. 8º Política de backup do repositório digital

§ 1º Será adotada a seguinte política de backup para arquivos e metadados do Repositório Digital.

I - Backup Full - Será realizado às 22:00 horas no dia primeiro de cada mês.

II - Backup Incremental - O primeiro incremental será realizado um dia após ao primeiro full, e os demais serão gerados sempre a partir do seu último incremental. Sempre será realizado ás 22:00 de segunda à sexta.

III - Backup Diferencial - O primeiro diferencial será realizado baseado no primeiro backup full do mês e os demais serão gerados sempre a partir do seu último diferencial. Sempre será realizado aos sábados às 22:00.

Art. 9º Definições de auditoria

§ 1º Deverá ser utilizado o sistema **BUSCADOR PGE** que permitirá localizar de forma rápida qualquer processo, registro ou documento contido nos repositórios, por qualquer dado contido nos mesmos, observando-se a classificação de segurança.

§ 2º Será possível identificar o sequenciamento dos fatos ocorridos, documentados e registrados nos repositórios digitais, através do campo Número Sequencial de Andamentos do Processo.

§ 3º A aplicação de carimbo do tempo será implantada no PGE, segundo os prazos a serem estabelecidos pela ICP-Brasil.

Publique-se. Comunique-se.

Fortaleza, 17 de maio de 2016

José Leite Lopes Filho
PROCURADOR-GERAL DO ESTADO