FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO
MESTRADO PROFISSIONAL EM GESTÃO E POLÍTICAS PÚBLICAS

William Thomaz

PROCESSOS DIGITAIS NA PREFEITURA DE SANTOS: A CERTIFICAÇÃO DIGITAL E A SEGURANÇA DA INFORMAÇÃO

SÃO PAULO
2015

William Thomaz

Processos digitais na Prefeitura de Santos: a certificação digital e a segurança da informação

Artigo individual apresentado à Escola de Administração de Empresas de São Paulo, da Fundação Getulio Vargas, como requisito para obter o título de Mestre em Gestão e Políticas Públicas.

William Thomaz

Processos digitais na Prefeitura de Santos: a certificação digital e a segurança da informação

Artigo individual apresentado à Escola de Administração de Empresas de São Paulo, da Fundação Getulio Vargas, como requisito para obter o título de Mestre em Gestão e Políticas Públicas.

Campo do Conhecimento: Gestão Pública
Data de Aprovação: ___/___/2015

Examinador:

_____

Prof. Dr. Eduardo de Rezende Francisco

FGV-EAESP

DEDICATÓRIA

Dedico este trabalho àquela que nos momentos mais difíceis de minha vida pessoal e profissional jamais se furtou a estar ao meu lado e sempre acreditou que os objetivos seriam – e são – sempre plausíveis e alcançáveis: minha amiga, esposa, parceira de trabalho e companheira de muitas viagens, Camila Bricatte Thomaz.

Resumo

O presente trabalho tem como principal objetivo a descrição da sistemática de certificação digital a ser implementada na Prefeitura de Santos, como parte de um processo maior, a implementação dos Processos Digitais naquele município através da verificação e o acompanhamento dos principais desafios que a Prefeitura Municipal de Santos, por intermédio de sua Secretaria de Gestão, encontrou para a contratação e implantação da fé pública exigida para o correto enquadramento legal do programa de digitalização dos processos administrativos da Municipalidade.

Para tanto, tem-se como base a pesquisa de material legal, especialmente do Decreto do Prefeito de Santos e da Portaria Municipal da Secretaria de Gestão que criou efetivamente a obrigação para que todos os servidores do Município elaborem determinados processos administrativos de maneira unicamente digital. Ainda, a MP 2001-02/2001 que trata da certificação digital é retratada. Angariar informações, desde as básicas, como quais são os equipamentos necessários, até o modelo de licitação (pregão eletrônico) para que outros entes públicos busquem a digitalização de seus processos e a consequente licitação para a certificação digital são os desafios deste artigo.

PALAVRAS-CHAVES: Processos Digitais, Certificação Digital, Políticas Públicas, Indicadores Públicos, Santos.

Abstract

This paper has as the main objective the description of digital certification to be implemented in the City of Santos, as part of a larger process, the implementation of Digital Processes. Through verification and monitoring of the main challenges that the Municipality of Santos, through its Secretary of Management, took for the hiring and deployment to digital certification laws for administrative processes of the Municipality.

It has based on the research of laws, especially the Decree of the Mayor of Santos and Municipal Management Bureau Ordinance that effectively created an obligation for all public servers to create certain administrative processes uniquely digital way. The law MP 2001-02 / 2001 which deals with digital certification is discussed. Gather information, from basic as what are the models needed to the bidding to other public entities that seek digital processes and the subsequent alternatives for the digital certification are the challenges of this article.

KEYWORDS: Digital Process, Digital Certification, Public Policy, Public Indicators, Santos.

LISTA DE ABREVIATURAS E SIGLAS

AC – Autoridade Certificadora

DETIC – Departamento de Gestão e Tecnologia da Informação e Comunicações

FAMS – Fundação Arquivo e Memória de Santos

GSI-PR – Gabinete de Segurança Institucional da Presidência da República

ICP – Infraestrutura de Chaves Públicas

ITI – Instituto Nacional de Tecnologia da Informação

MARE – Ministério da Administração Federal e Reforma do Estado

MP – Medida Provisória

SSHD – (“Solid State Hybrid Disc”, em inglês) ferramenta eficaz de armazenamento de dados cuja performance assemelha-se aos ótimos resultados de desempenho

Sumário

Introdução

> Na semana de 4 de Julho, diversos sites da Coreia do Sul e dos Estados Unidos sofreram ataques *denial of service*[1], e culparam a inimiga histórica – Coreia do Norte. Um dos resultados foi o anúncio de uma nova unidade militar na Coreia do Sul especializada em defesa digital. Em 25 de Junho o site do Telegraph do Reino Unido (http://www.telegraph.co.uk) publicou notícia sobre a acusação, por parte de um alto funcionário do governo daquele país, de que a China, Russia e a Al-Qaeda estavam promovendo ataques contra a infraestrutura digital do país, e que o governo britânico estava lançando uma nova estratégia para defesa digital, incluindo ataques terroristas que poderiam ser lançados no futuro. Coincidência ou não, o governo dos Estados Unidos anunciou há algumas semanas um novo plano de defesa contra ataques e uma nova estrutura organizacional, com pesados investimentos e um claro aviso de que pode revidar ataques cibernéticos militarmente, com forças convencionais, para deixar bem claro. De qualquer forma, os países anunciaram que o contra-ataque faz parte da estratégia[2].

A reportagem acima descrita está hospedada no sítio eletrônico do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República do Brasil (GSI-PR), órgão público que é responsável pela segurança da informação (para fins de defesa nacional) no Brasil, o que demonstra a importância do tema para o governo brasileiro, visto que o GSI é diretamente ligado à Presidente da República.

Da matéria e da importância da discussão presente em órgão máximo do Poder Executivo surgem alguns questionamentos que serão tratados posteriormente: existe segurança digital no Brasil suficiente para tornar os processos de entes públicos completamente digitais? Há necessidade de manutenção de arquivos físicos por motivos de segurança para garantir a publicidade dos atos da Administração Pública? Qual é a regulamentação legal em vigor no Brasil atualmente? Em suma, digitalizar processos pode tornar a Gestão Pública mais vulnerável?

Este trabalho busca complementar assunto tratado em uma perspectiva um pouco diferente na monografia apresentada na Fundação Getulio Vargas sobre os Processos Digitais na Prefeitura de Santos. De maneira mais aprofundada e detalhada, buscou-se verificar a

[1] Ataques chamados de *denial of service* podem ser entendidos como atos criminosos para retirar do ar determinados sites, ou ainda prejudicar o bom funcionamento da página, excedendo os limites de acesso da página no servidor onde o serviço é hospedado.

[2] O referido ataque deu-se no ano de 2009. Disponível em http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq. Acesso em 19 de agosto de 2015.

solução que a Prefeitura de Santos procurou para obter a certificação digital e o necessário alcance da fé pública[3] determinada pela legislação brasileira, como será visto adiante.

O Instituto Nacional de Tecnologia da Informação (ITI), órgão brasileiro responsável pela emissão da certificação digital assim a define:

> O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso. A certificação digital é uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demanda identificação clara da pessoa que a está realizando pela intranet[4].

Na prática, o certificado digital da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a *web*. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

Os certificados contêm os dados de seu titular, como nome, número do registro civil, assinatura da AC que o emitiu, entre outros, conforme especificado na Política de Segurança de cada AC.

Ao mesmo tempo em que há necessidade de que a Administração Pública se adeque aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência determinados pela Carta Magna do Brasil, em seu artigo 37, a segurança cibernética é assunto cada vez mais recorrente e alvo de preocupação tanto de servidores públicos quanto de instituições privadas. Desta forma, o projeto de uma Prefeitura 100% digital, como a Municipalidade de Santos se propõe atualmente, deve obrigatoriamente ter na segurança da informação e na legitimidade dos processos digitais um dos pilares para o bom funcionamento do sistema.

[3] Os documentos públicos devem estar de acordo com os ditames legais.
[4] Disponível em http://www.iti.gov.br/certificacao-digital/certificado-digital. Acesso em 07 de setembro de 2015.

Assim, como os outros trabalhos individuais que complementam o trabalho em grupo[5] sobre o tema, este artigo pode constituir e complementar a experiência de Santos, para que outros entes públicos busquem fundamentação para a obtenção pública da certificação para os processos digitais.

Com o aval do Município de Santos, a licitação para a aquisição da certificação digital está anexada a este relatório, bem como as regras de uso do correio eletrônico e governança da informação.

[5] O trabalho citado, Processos Digitais na Prefeitura de Santos, foi apresentado no Mestrado Profissional em Gestão e Políticas Públicas da EAESP/Fundação Getulio Vargaspelos mestrandos Ana Carolina Caldas Bahia Falcão, João Roberto Fernandes de Lima e William Thomaz e aprovado em 11 de setembro de 2015.

1. A certificação digital no Brasil e as bases legais

A passagem temporal dos processos físicos para os processos digitais no Brasil (e a consequente certificação digital de tais processos) é extremamente nova se comparada ao início da criação da chamada "assinatura digital". Esta surgiu na década de 70:

> A legislação vigente que delimita a utilização da certificação digital e assinatura eletrônica é recente se comparada ao início do termo assinatura digital que começou no ano de 1976, quando Whitfield Diffie e Martin Hellman, dois Matemáticos, publicaram um artigo descrevendo uma forma de enviar mensagens criptografadas por chave pública; dois anos mais tarde, Rivest, Adi Shamir e Leonard Adleman desenvolveram um sistema de assinatura digital[6].

A legislação que trata da certificação digital e seus regramentos em âmbito nacional data de 2001[7]. A medida provisória de número 2.200-2/2001 criou a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Tal letra legal iniciou o regramento em âmbito nacional do reconhecimento e organização das chaves digitais e a sua consequente organização por um ente público exclusivamente dedicado ao assunto.

Atualmente, o ICP-Brasil (gerido através do ITI – Instituto Nacional de Tecnologia da Informação) faz a emissão, revogação e renovação dos diversos níveis hierárquicos da certificação digital, através de seu Comitê Gestor e suas divisões.

Outro marco jurídico importante para a certificação digital e seus desdobramentos é a Lei Federal nº 12.682, de 9 de julho de 2012:

> Art. 1º - A digitalização, o armazenamento em meio eletrônico, óptico ou equivalente e a reprodução de documentos públicos e privados serão regulados pelo disposto nesta Lei.
>
> Parágrafo único. Entende-se por digitalização a conversão da fiel imagem de um documento para código digital.
>
> Art. 2º - (VETADO).
>
> Art. 3º - O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento

[6] Certificação Digital: importância e aplicabilidade. Tiago Lolato e Evelacio Roque Kaufmann. Unoesc & Ciência - ACET, Joaçaba, v. 5, n. 1, p. 39-52, jan./jun. 2014. Importante destacar que assinatura digital e certificação digital são atos jurídicos diferentes; o valor probatório e autenticado é de responsabilidade da certificação digital.

[7] Embora existam legislações anteriores que façam referência a documentos eletrônicos, como a lei 8935/94, a MP 2200/01 trata-se de um marco da legislação por iniciar o ICP-Gov e criar a Autoridade Certificadora ligada ao Governo do Brasil. Para um estudo detalhado da legislação, o SIGA (Sistema de Gestão de Documentos de Arquivo) possui em seu arquivo eletrônico todo o detalhamento da legislação: http://www.siga.arquivonacional.gov.br/media/iii_encontro_siga_2010/apresetao_jose_henrique_arquivamento_eletronico_de_documentos.pdf. Acesso em 19 de agosto de 2015.

> digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil.
>
> Parágrafo único. Os meios de armazenamento dos documentos digitais deverão protegê-los de acesso, uso, alteração, reprodução e destruição não autorizados.
>
> Art. 4º - As empresas privadas ou os órgãos da Administração Pública direta ou indireta que utilizarem procedimentos de armazenamento de documentos em meio eletrônico, óptico ou equivalente deverão adotar sistema de indexação que possibilite a sua precisa localização, permitindo a posterior conferência da regularidade das etapas do processo adotado.
>
> Art. 5º - (VETADO).
>
> Art. 6º - Os registros públicos originais, ainda que digitalizados, deverão ser preservados de acordo com o disposto na legislação pertinente.
>
> Art. 7º - (VETADO).
>
> Art. 8º - Esta Lei entra em vigor na data de sua publicação.

Nota-se, de pronto, que alguns artigos foram vetados[8], e é exatamente neste ponto que a legislação não auxiliou a certificação digital e consequentemente a efetividade dos processos digitais no Brasil.

O artigo 2º (VETADO) especificava que o documento digital e sua cópia teriam valor legal para todos os fins de direito; previa que após a digitalização os documentos físicos poderiam ser destruídos; por fim, autorizava a produção de documentos públicos e privados por meios ópticos e equivalentes.

Com o veto, perdeu-se a oportunidade de dinamizar os atos administrativos, bem como deixar de arquivar e destruir fisicamente documentos já digitalizados sob alegação de que tal medida iria de encontro à lei arquivista em vigor no Brasil (Lei federal nº 8.159/91).

Assim, a necessidade de registro e certificação, mesmo nos processos digitais (excluindo-se legislação específica para o Processo Judicial, a Lei nº 11.419/06, que garante que as cópias digitalizadas são consideradas originais para os fins legais), ainda perdura.

[8] A mensagem de veto presidencial foi assim informada: "Ao regular a produção de efeitos jurídicos dos documentos resultantes do processo de digitalização de forma distinta, os dispositivos ensejariam insegurança jurídica. Ademais, as autorizações para destruição dos documentos originais logo após a digitalização e para eliminação dos documentos armazenados em meio eletrônico, óptico ou equivalente não observam o procedimento previsto na legislação arquivística. A proposta utiliza, ainda, os conceitos de documento digital, documento digitalizado e documento original de forma assistemática. Por fim, não estão estabelecidos os procedimentos para a reprodução dos documentos resultantes do processo de digitalização, de forma que a extensão de efeitos jurídicos para todos os fins de direito não teria contrapartida de garantia tecnológica ou procedimental que a justificasse".

Isso, na prática, significa que o contribuinte santista que pedir de uma cópia com fé pública de seu processo digitalizado deverá percorrer o enorme caminho burocrático para ter a documentação autenticada (em cartório) e com valor de documento oficial.

A Lei Federal nº 12.682/12, em seu projeto inicial, trazia a equiparação do documento digital ao documento original, prevendo a eliminação do documento produzido por meio eletrônico, após o devido lapso legal de seu arquivamento, tudo conforme legislação pertinente. Entretanto, tais previsões constavam nos artigos 2º e seus parágrafos, artigo 5º e artigo 7º, todos vetados. Ou seja, a Prefeitura de Santos deverá arquivar toda a documentação eletrônica, mesmo após seu prazo legal. Para uma Prefeitura com o porte da cidade de Santos, trata-se de grande capacidade de armazenamento eletrônico a ser investido e mantido.

Mais uma vez, a timidez da lei obriga a Administração Pública a arquivar de maneira permanente toda a documentação produzida mesmo de maneira eletrônica e obriga o munícipe a certificar suas cópias, mesmo provenientes de processos digitais. A tentativa de conceder valor jurídico ao processo digital (mais uma vez, excluindo-se o Processo Judicial que tem legislação específica) reforça a burocrática visão citada desde as tentativas de reformas administrativa no Brasil levadas a cargo por Bresser-Pereira em seu extinto trabalho no Ministério da Administração Federal e Reforma do Estado (MARE), na década de 90.

Além disto, a manutenção do papel e a continuidade da cultura burocrática impedem que o projeto dos Processos Digitais de Santos tenha maior amplitude e benefícios aos cidadãos.

Na legislação local, Santos tem em seu arcabouço jurídico o regramento para a certificação digital, oriundo das normas relativas aos Processos Digitais da Prefeitura de Santos (o regramento específico dos certificados eletrônicos está diretamente ligado à utilização dos processos digitalizados).

O Decreto nº 7.141, de 09 de junho de 2015[9], traz as disposições legais para a implantação dos processos digitais na Prefeitura de Santos. Aqui, buscou-se a regulamentação necessária (norma específica, necessária para a determinação de maneira ampla) para que

[9] A publicação do decreto está disponível em https://egov1.santos.sp.gov.br/do/1316/2015/do10062015.pdf. Acesso em 20 de junho de 2015.

todos os servidores tenham como obrigação legal a elaboração de determinados processos de maneira exclusivamente digital.

Assim, criou-se, automaticamente, a necessidade da certificação para os documentos produzidos.

2. A licitação da certificação digital em Santos

Com as bases legais para a certificação digital definida, desde a medida provisória que regulamentou em âmbito nacional a certificação de documentos eletrônicos até a legislação santista que aprovou o projeto dos processos digitais e consequentemente requeriu oficiosamente a certificação digital legal, o embasamento jurídico para tornar oficiais e válidos os documentos produzidos em meios eletrônicos na Prefeitura de Santos estava devidamente sedimentado.

Surgiu, então, a necessidade da elaboração da licitação pública para a contratação (integralmente transcrita em cópia através do anexo 01).

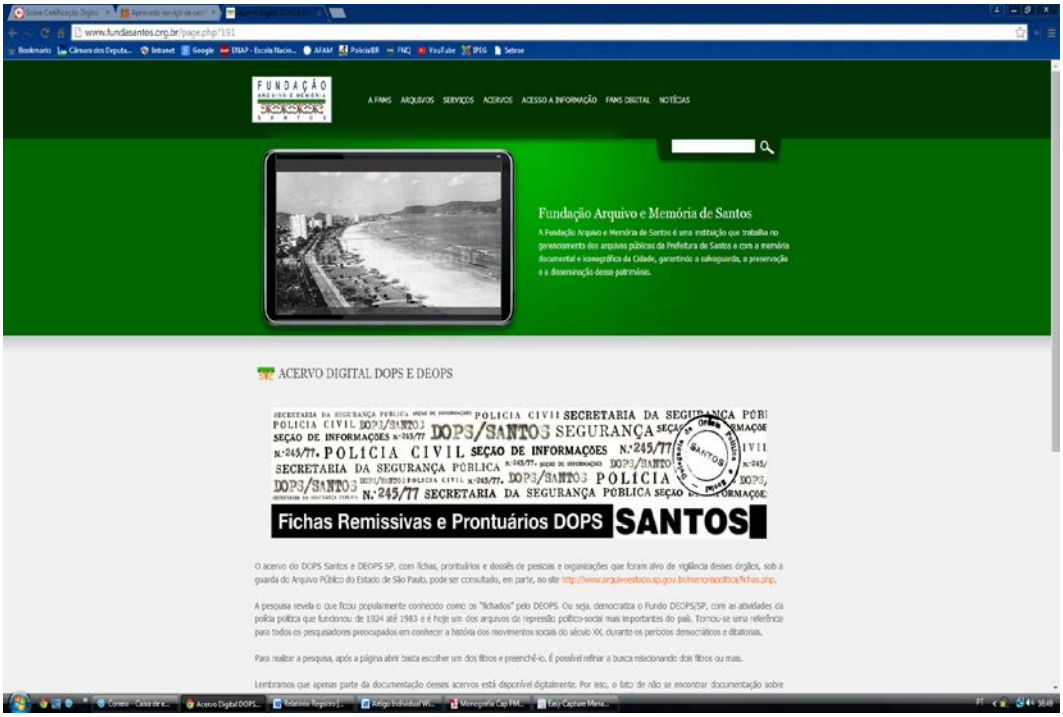
O caso aqui em estudo buscou através de licitação, na modalidade registro de preços, prevista na Lei nº 8.666/93 (Lei de Licitações) a aquisição das certificações com as especificações da ICP-Brasil (regradas pela MP 2200-02/2001).

O caso de Santos, contudo, tem uma peculiaridade sobre arquivos públicos que merece ser destacada. Por ser uma cidade histórica e abrigar documentos de interesse nacional, o Município conta com uma Fundação própria para o gerenciamento de arquivos públicos. Trata-se da Fundação Arquivo e Memória de Santos (Fams), assim definida em seu sítio eletrônico:

> Fundação Arquivo e Memória de Santos (Fams) é uma instituição que trabalha no apoio à administração municipal no que se refere ao gerenciamento dos arquivos públicos processados pela Prefeitura de Santos, além da memória documental e iconográfica da cidade, garantindo sua salvaguarda, preservação e disseminação. A sede da Fams está localizada na rua Amador Bueno, nº 22, Centro Histórico, desde dezembro de 2012. Antes disso, a diretoria da instituição ocupava a casa acastelada do Outeiro de Santa Catarina (rua Visconde do Rio Branco, 48, Centro Histórico), no mesmo sítio que fora, no século XVI, o marco inicial da Vila de Santos[10].

[10] Disponível em http://www.fundasantos.org.br/page.php?118. Acesso em 15 de agosto de 2015.

Figura 1 - O sítio eletrônico da Fams e um de seus importantes arquivos: Fichas remissivas do DOPS - Santos



Fonte: http://www.fundasantos.org.br/page.php?191.

Criada através da Lei municipal 196/95[11], a Fams também tem autorização emitida pelo ITI desde 2013 para emitir certificados digitais para pessoas físicas, jurídicas e poder público, em esfera nacional, o que não fez com que a Prefeitura de Santos, cumprindo a Lei de Licitações em vigor no Brasil, efetivasse a contratação de sua própria Fundação através de inexigibilidade de licitação.

Manteve o processo licitatório, que resultou, ao final do certame, na oportunidade de contratação pela Prefeitura de Santos de empresa com especialização, viabilizando o cumprimento do edital proposto de forma eficaz e com os custos adequados.

[11] A justificativa para a criação da Fundação está no sítio eletrônico da Fams: "Por conta das experiências bem sucedidas no desenvolvimento de metodologias para organização na área de arquivos, a Prefeitura Municipal de Santos decidiu conferir ao Centro de Memória maior autonomia administrativa, assim como dispositivos que garantissem maior agilidade para a contratação de recursos humanos e técnicos, além de facilidade para a busca de recursos financeiros. Nascia, desta forma, em 1995, a Fundação Arquivo e Memória de Santos (Fams)". Disponível em http://www.fundasantos.org.br/page.php?119 . Acesso em 21 de agosto de 2015.

A Fams, como Fundação legitimamente credenciada para o certame, concorreu assim como as outras empresas que atenderam os requisitos do edital. Entretanto, ao final do certame, após o devido cumprimento do edital, a empresa vencedora foi devidamente informada através do Diário Oficial do Município de Santos em 28 de julho de 2015, vencendo a empresa SERASA S/A:

Figura 2 - O cumprimento do princípio constitucional da publicidade dos atos da Administração Pública através da informação da empresa vencedora do certame: SERASA S.A.

ATOS DA COMISSÃO PERMANENTE DE LICITAÇÕES IV

COMUNICADO

A Comissão supramencionada, situada na Rua XV de Novembro nº 195 - 8º andar – Centro - Santos/SP, comunica que a Sra. Secretária Municipal de Gestão (em substituição) HOMOLOGOU o procedimento licitatório realizado através do Pregão Eletrônico nº 16.035/2015, Processo nº 22.182/2015-20, que tem como objeto a seleção de propostas para REGISTRO DE PREÇOS visando à prestação de serviços de emissão de Certificados Digitais A3 no padrão ICP-Brasil, com emissão dos certificados nas instalações da Prefeitura Municipal de Santos e o fornecimento do cartão (smart card) e da respectiva leitora de cartão, sob gerenciamento do Departamento de Gestão da Tecnologia de Informação e Comunicações (DETIC), da Secretaria Municipal de Gestão - SEGES, à empresa, conforme a seguir:

LOTE 01 – SERASA S/A.

ITEM	DESCRIÇÃO	UNID.	QUANT.	VALOR UNITÁRIO R$	VALOR TOTAL R$
1.1	Emissão de Certificados Digitais, nível A3, no padrão ICP-Brasil, com validade de 3 (três) anos, contados a partir da data do aceite definitivo do certificado, emitidos sob a hierarquia V2, Tipo: e-CPF; fornecimento do cartão (smart card) e da respectiva leitora para "smart card" contendo Certificação Digital e-CPF do tipo A3 e entrada USB; compatível com os sistemas operacionais Windows 7, XP, Windows Vista ou superior; possuir compatibilidade com navegadores web: Microsoft Internet Explorer versão 6.0 e superiores, Mozilla Firefox versão 35.0.1 e superiores e Chrome 38.0.2125.1 e superiores.	UNID.	1.000	129,99	129.990,00

Valor Total estimado do Lote 01: R$ 129.990,00 (cento e vinte e nove mil, novecentos e noventa reais).
Valor Total estimado da despesa: R$ 129.990,00 (cento e vinte e nove mil, novecentos e noventa reais).
Santos, 27 de julho de 2015.

AUGUSTO ONESIO FICK
PRESIDENTE DA COMISSÃO PERMANENTE DE LICITAÇÕES IV – COMLIC IV
PREGOEIRO

Fonte: https://egov1.santos.sp.gov.br/do/1316/2015/do28072015.pdf

Mesmo habilitada para o certame, a Fams não teve homologada sua proposta ao final do processo licitatório. Os valores das certificações são devidamente apresentados no Capítulo 4 e na conclusão deste trabalho. Pontualmente, cada certificação custará anualmente R$ 43,33 ao erário santista.

3. A certificação digital e a segurança da informação: a operacionalização da certificação no projeto de Santos

A tecnologia digital e todos os seus desdobramentos podem tanto facilitar o dia-a-dia de todos os habitantes do planeta como também têm a capacidade (como visto no texto introdutório deste trabalho) de suscitar possibilidades de ataques cibernéticos entre países e maciços investimentos em segurança e contraespionagem virtuais.

Para a administração pública as possibilidades são as mesmas: as novas formas de tecnologia podem transformar-se em formas de melhor interação com os cidadãos ou expor dados e informações cruciais de forma desnecessária e irresponsável.

Nesse sentido, alguns exemplos podem ilustrar tais fatos.

O primeiro deles, ocorrido no ano de 2007 no Reino Unido, revelou os dados de mais de 25 milhões de registro do programa britânico de transferência de renda *Child Benefit:*

> On Saturday morning my better half received a letter from the acting chairman of HM Revenue and Customs (HMRC) personally apologising for the loss of our family's Child Benefit data. In the past few days 7.25 million such letters have been sent out. Little wonder that the post seems slower than usual. This unprecedented apology comes as a result of recent events which culminated in the resignation of the then chair of HMRC and an emergency statement to Parliament by Alistair Darling. The Chancellor was forced to admit that his department had managed to lose 25 million Child Benefit records. The lost (or stolen) information included the names, addresses, dates of birth, National Insurance numbers and, where relevant, bank details of claimants. According to the BBC, two password-protected discs containing the data were sent by HMRC in Newcastle to the National Audi Office in October. The package was sent by courier and it appears that it did not arrive at its destination. A further package was sent by recorded post which did arrive. The Police have been called in but, at the time of writing, nothing has been found[12].

[12] Texto em tradução livre: No sábado pela manhã a minha melhor metade recebeu uma carta do presidente em exercício *da HM Revenue and Customs (HMRC)*, pessoalmente, desculpando-se pela perda de dados do programa Benefício Infantil de nossa família. Nos últimos dias 7,25 milhões de tais cartas foram enviadas. Não é de admirar que o lugar parece ser mais lento do que o habitual. Este pedido de desculpas sem precedentes vem como resultado dos recentes acontecimentos que culminaram na renúncia do então presidente do *HMRC* e uma declaração de emergência ao Parlamento feito pelo Sr. Alistair Darling. O chanceler foi forçado a admitir que seu departamento conseguiu perder 25 milhões de registros de abono de família. As informações perdidas (ou roubadas) incluíam os nomes, endereços, datas de nascimento, números de Seguro Nacional e, se pertinente, os dados bancários dos requerentes. De acordo com a BBC, dois discos protegidos por senha contendo os dados foram enviados pelo HMRC em Newcastle para o National Audi Office em outubro. O pacote foi enviado pelo correio e parece que ele não chegou ao seu destino. Um pacote adicional foi enviado por correio registrado. A Polícia foi chamada, mas, nada foi encontrado. Disponível em http://www.informationlaw.org.uk/userimages/LSGDataLoss.pdf. Acesso em 28 de agosto de 2015.

Longe de mostrar-se como um isolado problema de sigilo dos dados virtuais hospedados e sob responsabilidade do governo britânico, no mesmo ano, o *Commonwealth Office (FCO*) encontrou uma falha grosseira na segurança de seus sistemas de solicitação de vistos da Inglaterra:

> The Government doesn't seem to be having much luck complying with its data protection obligations at the moment. On 13th November, the Information Commissioner Office (ICO) announced that he had found the Foreign and Commonwealth Office (FCO) in breach of the Data Protection Act 1998 (DPA) following an investigation into a security breach at the online application facility for UK visas. The breach meant that the personal data of people applying for visas to enter the UK was visible to others visiting the website. The ICO has now obtained a formal undertaking from the FCO agreeing to comply with the principles of the DPA. Failure to do so will result in further enforcement action. More DPA failures were alleged in this week's News of the World. Apparently an ex-contractor at the Department for Work and Pensions (DWP) had two discs with thousands of benefit claimants' details for more than a year. The woman told the News of the World she forgot to return them after she stopped working for the DWP a year ago. The unencrypted discs revealed the type of benefits paid, but a DWP spokesman said they did not contain bank details[13].

Os dois gravíssimos casos de violação da privacidade individual podem questionar a segurança dos dados armazenados de maneira digital pela administração pública, tanto no Brasil quanto no país aqui exemplificado. Naturalmente, a primeira impressão que pode se ter é a de que os processos físicos não teriam tal tipo de problemática, pois perder um processo é completamente diferente de expor os dados de determinado serviço (e de seus utilizadores) na rede mundial de computadores, por tempo possivelmente indeterminado. Ainda, *ad cautela*, seria possível pensar que mesmo com os processos digitalizados haveria a necessidade de criar cópias de segurança, estas físicas.

Seriam então os processos físicos mais seguros que os processos digitais?

---

[13] O Governo não parece estar tendo muita sorte cumprimento das suas obrigações de proteção de dados no atualmente. No dia 13 de novembro, Information Commissioner Office (ICO) anunciou que havia encontrado na Foreign and Commonwealth Office (FCO) uma violação do Data Protection Act 1998 (DPA) após uma investigação sobre uma violação de segurança na instalação de aplicativo on-line para vistos no Reino Unido. A violação significava que os dados pessoais das pessoas que solicitam vistos para entrar no Reino Unido era acessível para os outros que visitavam o site. A ICO obteve um compromisso formal do FCO concordando em cumprir os princípios da DPA. O não cumprimento resultaria em outras medidas coercivas. Mais falhas DPA foram verificadas pela revista News of the World. Aparentemente, um ex-empreiteiro no Department for Work and Pensions (DWP) tinha dois discos com milhares de detalhes dos requerentes de benefícios para mais do que um ano. A mulher disse ao News of the World que ela se esqueceu de devolvê-los depois que ela parou de trabalhar para o DWP há um ano. Os discos não criptografados revelou o tipo de benefícios pagos, mas um porta-voz do DWP informou que não continha dados bancários. Disponível em http://www.informationlaw.org.uk/userimages/LSGDataLoss.pdf. Acesso em 28 de agosto de 2015.

Não é o caso. Mesmo que os processos sejam físicos e fiquem depositados em uma sala trancada os riscos existem, como mostra o exemplo abaixo:

> Uma série de volumes e documentos "desapareceu" de dois processos envolvendo a Máfia do Fisco, como ficou conhecido um dos maiores esquemas de desvio de recursos desbaratado no Estado e que funcionava dentro da Secretaria Estadual de Fazenda (Sefaz). O sumiço ocorreu na 6ª Vara Criminal e na 4ª Vara da Fazenda Pública de Cuiabá. Em um dos relatos de escrivães, a suspeita é de que o material teria sido "surrupiado" por uma mulher no próprio balcão da escrivania. O sumiço de documentos foi constatado no fim de junho, primeiramente na esfera criminal. Ao se deparar com a ausência de volumes da ação, uma escrivã recorreu à Vara da Fazenda para copiar partes do início dos autos de processo similar em tramitação. Lá, funcionários se depararam com o mesmo problema: Os dois últimos volumes haviam desaparecido. O relato incluído no andamento processual descreve que o barbante usado para amarrar os volumes estava solto[14].

Com os exemplos negativos explicitados, o contraponto também deve ser registrado.

Um dos maiores sucessos de digitalização dos processos no Brasil[15] em andamento é o caso do Tribunal de Justiça de São Paulo. Com o porte e complexidade para ostentar os maiores número de um Tribunal do Gênero na América Latina[16], com 20 milhões de processos e 23 mil novas ações todos os dias, atualmente, a distribuição de processos físicos já supera a distribuição de processos digitais.

[14] Disponível em http://www.diariodecuiaba.com.br/detalhe.php?cod=291111. Acesso em 25 de julho de 2015.
[15] As vantagens ao meio ambiente saltam aos olhos: dezenas de milhões de folhas de papel são poupadas. Dados do CNJ (Conselho Nacional de Justiça) apontam que são distribuídos mais de 20 milhões de processos novos por ano no Brasil. No formato físico, consumem cerca de 46 milhões de quilos de papel e 690 mil árvores, com o desmatamento de 400 hectares; e, ainda, 1,5 milhão de metros cúbicos de água (suficientes para abastecer uma cidade de 27 mil habitantes durante um ano).
[16] Fonte: http://www.tjsp.jus.br/CemPorCentoDigital/ Acesso em 25 de julho de 2015.

Figura 3 - A distribuição de processos entre físicos e digitais no TJ/SP no ano de 2015

Distribuição processo físico *x* processo digital:
Janeiro/15 = 66,63% físicos – 33,37% digitais
Fevereiro/15 = 62,24% físicos – 37,76% digitais
Março/15 = 58,89% físicos – 41,11% digitais
Abril/15 = 55,68% físicos – 44,32% digitais
Maio/15 = 52,71% físicos – 47,29% digitais
Junho/15 = 48,06% físicos – **51,94%** digitais

Distribuição 2015 - Processos Físicos x Processos Digitais					
Mês	**Processos Físicos (%)**	**Processos Digitais (%)**	**Processos Distribuídos (MovJud)**	**Processos Físicos Distribuídos**	**Processos Digitais Distribuídos**
Janeiro	66,63%	33,37%	343.017	228.540	114.477
Fevereiro	62,24%	37,76%	321.605	200.171	121.434
Março	58,89%	41,11%	385.587	227.066	158.521
Abril	55,68%	44,32%	338.566	188.513	150.053
Maio	52,71%	47,29%	363.341	191.524	171.817
Junho					

Fonte: http://www.tjsp.jus.br/institucional/canaiscomunicacao/noticias/Noticia.aspx?Id=27286

Com exemplos negativos e positivos dos processos físicos e dos processos digitais, conclui-se que nenhum dos meios apresentados é completamente seguro. As vantagens dos processos digitais, contudo, são inegáveis quando comparadas aos processos físicos: somente a economia de papel e a menor área de armazenamento de tais processos (enquanto salas seguras também são custosas e dependem de manutenção, mas podem armazenar milhões de dados, as salas de armazenamento físico demandam de espaço para todos os processos, manutenção e segurança adequadas nos diversos locais em que estão instaladas, com capacidade limitada).

Antes de se falar em certificação digital, a segurança da informação deve ser devidamente assegurada nos processos digitais.

A segurança da informação é subproduto de uma série de medidas adotadas anteriormente à certificação digital.

E como o gestor público pode balizar a segurança de suas informações?

Para tanto, a administração pública do Brasil dispõe de excelente material para orientação e formulação de padrões: “O guia Boas Práticas em Segurança da Informação do Tribunal de Contas da União”, já em sua 4ª Edição (2012), disponível integralmente na

internet[17], trata-se de um verdadeiro guia para orientar o gestor (de qualquer esfera e nível da administração pública) a conduzir seus atos digitais baseados na segurança da informação. O documento torna-se essencial para a correta gestão dos processos digitais em implantação atualmente, como nos casos aqui apresentados do Tribunal de Justiça e da Prefeitura de Santos.

Nesse sentido, a Prefeitura de Santos já possui um robusto sistema de segurança digital, criado pelo Departamento de Tecnologia, reconhecidamente premiado[18]. A normatização do sistema deu-se através das Instruções Normativas[19] nº 01/2012 (que trata do gerenciamento de identidades) e nº 02/2011 (que trata do correio eletrônico institucional), tendo os servidores públicos suas rotinas digitais já balizadas antes mesmo da formulação e implementação dos processos digitais.

Dentre eles, destaca-se o chamado Serviço de Segurança Humana e Digital (SSHD), assim definido na Instrução Normativa 01/2012 – SEGES da Prefeitura de Santos:

> Art. 1º O Gerenciamento de Identidade tem como objetivo controlar todas as movimentações de um servidor ou prestador de serviço, para garantir em uma base de dados única o histórico de todos os serviços de Tecnologia da Informação - TI atribuídos a uma pessoa no âmbito da Prefeitura Municipal de Santos, e rege-se pelas disposições contidas na presente Instrução Normativa.
> Art. 2º Para efeitos desta instrução, são adotadas as seguintes definições:
> I- identificador único: sequencia de caracteres que não se repete, com dígito verificador, que só deve ser utilizada pela pessoa que o recebeu, também conhecida como usuário ou "login";
> II- senha: conjunto de caracteres que apenas o proprietário do identificador único conhece e, quando associado um ao outro, serve como forma de autenticação;
> **III- SSHD: Serviço de Segurança Humana e Digital – Aplicativo de TI desenvolvido pelo DETIC, para gerenciamento de identidades (g.n.);**
> IV- TI: Tecnologia da Informação;
> (...)

[17] Em http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF . Acesso em 01 de setembro de 2015.

[18] Neste ponto, a Prefeitura de Santos, através do DETIC (Departamento de Gestão e Tecnologia da Informação e Comunicações) já ganhou os seguintes prêmios, Santos já conquistou os prêmios TI & Governo - Sistema Rede de Informação Social - Plano Editorial (2006); E-Gov (Governo Eletrônico) - Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e da Comunicação – ABEP – Sistema Integrado de Saúde e Administração de Materiais (2007); TI & Governo - Sistema Integrado de Gestão Escolar - Plano Editorial (2007); Inovação em Gestão Educacional - Sistema Integrado de Gestão Escolar - Ministério da Educação - MEC (2008); TI & Governo - Sistema de Informações Geográficas de Santos - Plano Editorial (2009); e TI &Governo - Sistema de Integrado de Atendimento Social - Plano Editorial (2010). Disponível em http://www.santos.sp.gov.br/?q=noticia/26518/santos-fica-entre-os-dez-munic-pios-mais-digitais-no-pa-s. Acesso em 07 de setembro de 2015.

[19] As duas instruções do Secretário de Gestão de Santos estarão anexadas a este artigo, devidamente autorizadas pela Prefeitura de Santos, para consultas e formulações futuras por entes públicos com os mesmos desafios de Santos.

Houve a preocupação dos gestores de Santos em padronizar a acessibilidade de seus sistemas digitais, antes mesmo do projeto de Processos Digitais. Ainda, com a criação das duas normativas aqui já registradas, a segurança da Informação de Prefeitura de Santos possui desenho e regramentos adequados para a acessibilidade segura da rede mundial de computadores, tanto da intranet quanto da internet.

O último ponto aqui analisado é a certificação digital que já está em vigor no projeto de processos digitais da Prefeitura de Santos. A primeira aquisição da certificação ocorreu em 28 de julho de 2015, com mil certificações adquiridas pelo prazo de três anos. Importante destacar a definição de "certificação digital" e suas principais características:

> Pelo estudo realizado, podemos concluir que o uso da criptografia no mundo atual é praticamente imprescindível. Com o uso da internet, surgiram novas aplicações como o comércio eletrônico e o home-banking. Nestas aplicações, informações confidenciais como cartões de crédito, transações financeiras, etc. são enviadas e processadas em meios não confiáveis. Enquanto meios de comunicações suficientemente seguros para proteger este tipo de informação não surgem, a criptografia aparece como uma boa alternativa para proteção de dados. Com a criptografia e assinatura digital, três características importantes para segurança de informações são alcançadas. São elas: privacidade: Proteger contra o acesso de intrusos; autenticidade: Certificar-se de que, quem é o autor de um documento é quem diz ser; integridade: Proteger contra modificação dos dados por intrusos[20].

Por definição, a certificação digital deve proteger a privacidade, a autenticidade e integridade da informação digital. O que deve ocorrer com qualquer documento produzido pelo poder público. A Lei nº 8.159/91 determina que todos os documentos públicos devem ser, por dever do Estado, devidamente protegidos:

> Art. 1º - É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.
> Art. 2º - Consideram-se arquivos, para os fins desta Lei, os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

A mesma Lei traz em seu bojo a possibilidade de sanção pelo prejuízo causado por eventuais danos causados pelo mau uso, arquivamento ou divulgação do documento público ou em poder do Estado, dispondo o seu artigo 6º que "fica resguardado o direito de

[20] Um estudo sobre a criptografia e a assinatura digital. Fernando Antonio Mota Trinta; Rodrigo Cavalcanti de Macêdo. UFPE, 1998. Disponível em http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm . Acesso em 01 de setembro de 2015.

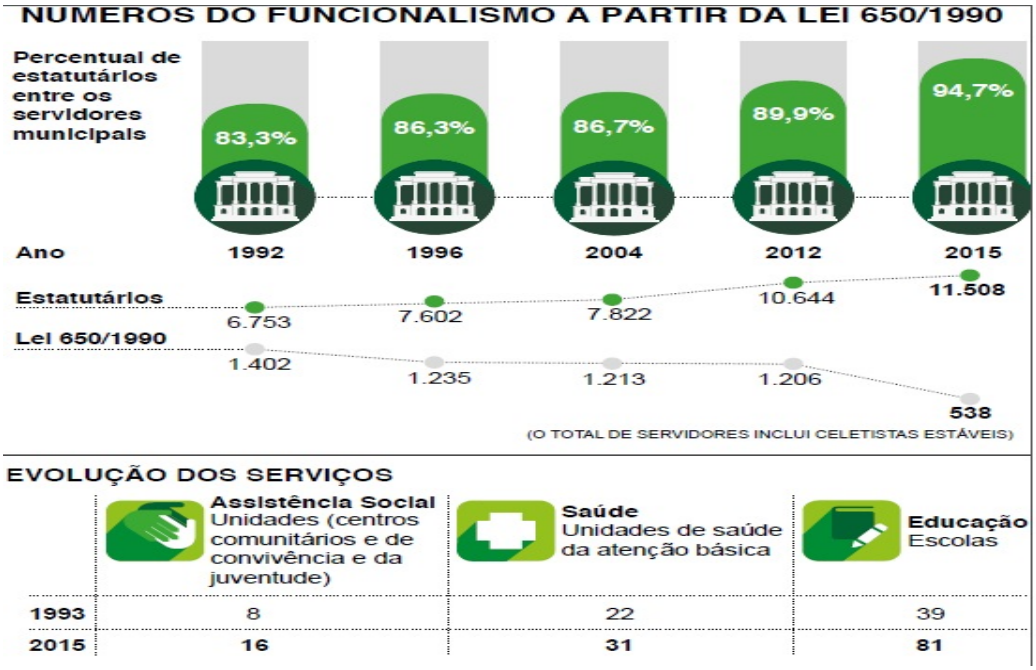
indenização pelo dano material ou moral decorrente da violação do sigilo, sem prejuízo das ações penal, civil e administrativa".

Assim, torna-se obrigacional por força de lei o uso da certificação digital (ou qualquer outro meio seguro de proteção dos documentos públicos elaborados exclusivamente de maneira eletrônica) pelo poder público.

4. Os custos envolvidos na certificação digital no Município de Santos

O caso da Prefeitura de Santos deve ter um ponto a ser destacado quanto ao planejamento e custos empenhados para a aquisição da certificação digital. Atualmente (em 2015), Santos conta com 12.141[21] servidores, de acordo com a figura abaixo:

Figura 4 - Gráfico com a evolução dos servidores públicos de Santos



Fonte: http://www.santos.sp.gov.br/?q=noticia/881331/prefeitura-amplia-servi-os-p-blicos-e-registra-recorde-de-servidores

Na primeira licitação, a certificação adquirida deu-se para mil servidores, ao custo de R$ 129.990,00 para utilização por três anos. Como custo unitário, tem-se o valor de R$ 129,90 (e o custo de cada certidão R$ 43,33 por ano). Consultada sobre os planos de aquisição da certificação, bem como os planos de novas aquisições, a Prefeitura de Santos, através do Departamento de Gestão e Tecnologia da Informação e Comunicações (DETIC), informou

[21] Dados disponíveis em http://www.santos.sp.gov.br/?q=noticia/881331/prefeitura-amplia-servi-os-p-blicos-e-registra-recorde-de-servidores . Acesso em 01 de setembro de 2015.

que a primeira aquisição foi efetivada para os chefes ou encarregados de seção, bem como diretores e secretários.

O que deve ser estudado e acompanhado no caso de Santos é a possibilidade (ou necessidade) de aquisição da certificação digital para todos os mais de 12 mil servidores da cidade.

Os custos de tal aquisição, considerando o mesmo valor praticado pela empresa vencedora do certame aqui analisado (Serasa), estariam em torno R$ 1.558,800. Ao ano, o custo seria de aproximadamente R$ 519.600,00.

Na cidade de Santos, o aluguel de um galpão de 4.000 m^2 na região central, sem qualquer preparação física, de logística e de segurança, foi cotado em pesquisa livre pelo custo mensal médio de R$ 45.000,00 [22]. Anualmente, o custo seria de aproximadamente R$ 540.000,00. Ou seja, apenas a locação de um espaço para guardar os documentos físicos (e mesmo considerando que os espaços já existam como a Fams, os processos públicos continuarão sendo iniciados, encerrados e necessariamente arquivados, demandando mais espaço para armazenamento).

Embora existam diversos custos envolvidos nas duas situações aqui comparadas (de um lado, custos de material como papel, impressão e espaço de armazenamento nos processos físicos e salas seguras, servidores e máquinas de outro lado nos processos digitas, além da necessária presença de servidores e segurança nos dois casos), uma simples comparação permite balizar o gestor para a forma mais econômica, célere e eficaz de armazenamento de processos: os processos digitais.

Assim, mesmo que todos os servidores futuramente tenham a certificação digital (fato que ainda deve ser analisado tendo em vista necessidade, conveniência e custo pelas equipes de Santos), em valores monetários do ano de 2015, o Erário empenharia para a aquisição das chaves digitais aproximadamente o valor do aluguel de um galpão de 4.000 metros quadrados, na comparação de gastos anuais.

A certificação contratada pela Prefeitura de Santos (de acordo com o padrão ICP-Brasil) foi a de fornecimento individual de *smart-cards* (equipamentos que portam

[22] Pesquisa realizada no site Zap Imóveis em http://www.zapimoveis.com.br/oferta/aluguel+galpao-deposito-armazem+centro+santos+sp+4.000m2+RS45000/ID-7477291/?paginaoferta=6 . Acesso em 02 de setembro de 2015.

fisicamente a certificação através de chip, além de seus respectivos leitores) e nível de segurança A3[23].

Os modelos de equipamento (*smart-card*) que a Prefeitura de Santos adquiriu podem ser visto na figura 05:

Figura 5 - Modelo de smart-card e o leitor com cabo usb

Fonte: http://www.comtac.com.br/?url=produto&id=232

Como anteriormente apontado, o nível se segurança escolhido pela equipe técnica de Santos foi o nível A3.

No processo licitatório, a validade solicitada pela Municipalidade foi a máxima permitida pela ICP-Brasil, de três anos. Para melhor entendimento do tipo de certificação que Santos escolheu e as outras opções que estavam disponíveis, a figura abaixo elenca os tipos atualmente disponíveis de certificação digital, regrados pela ICP-Brasil:

[23] Nível de segurança é a capacidade de proteção contra possíveis ataques a que a certificação está homologada. Sua variação inicia-se em A1 até A4, conforme será visto a seguir.

Figura 6 - Tipos de certificação digital

	Chave criptográfica			
Tipo de certificado	Tamanho (bits)	Processo de geração	Mídia armazenadora	Validade máxima (anos)
A1 e S2	1024	*Software*	Arquivo	1
A2 e S2	1024	*Software*	*Smart card* ou *token*, sem capacidade de geração de chave	2
A3 e S3	1024	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave	3
A4 e S4	2048	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave	3

Fonte: Revista Unoesc e Ciência, 2014.

Após a devida contratação e a consequente entrega do material prometido nas certificações contratadas, os primeiros servidores de Santos já operam o sistema de processos digitais com as chaves adquiridas.

Conclusão

O objetivo deste artigo foi complementar o trabalho apresentado[24] no Mestrado Profissional em Gestão e Políticas Públicas da Fundação Getulio Vargas que estudou a política pública de implantação dos processos digitais na cidade de Santos (SP). Enquanto aquele elencou as diretrizes da licitação, a fundamentação como política pública do projeto santista e ainda os indicadores para verificar a eficácia da política, este artigo buscou explicitar um dos temas apresentados no trabalho, contundo sem aprofundamento necessário para balizar outros órgãos públicos com o mesmo desafio enfrentado pelos servidores de Santos. A certificação digital, nos moldes do aplicado pela Prefeitura de Santos, está aqui explicitada.

Os questionamentos apresentados na introdução foram devidamente esclarecidos.

Tanto nos processos físicos quanto nos processos digitais, não se identifica ou busca-se atingir segurança plena. Os processos físicos padecem de dificuldades para armazenamento, possibilidades de fraude e potencial de destruição, furto e roubo dolosos ou culposos em mesma proporção que os meios digitais, apenas em modalidades diferentes. Os casos aqui apresentados demonstraram que mesmo os processos digitais podem ser desastrosos se a segurança da informação não estiver elencada como prioridade no projeto. As grandes vantagens do processo digital, no entanto, surgem ao verificarem-se fatores como economia de papel e impressão, menor espaço de armazenamento físico e maior celeridade nas transações e movimentações entre os diversos órgãos burocráticos de qualquer instituição pública do Brasil. Tais fatores corroboram para o maciço investimento da administração brasileira na digitalização de seus processos.

Com relação à necessidade de utilização de arquivos físicos para manutenção da segurança da informação, mesmo que com os processos completamente digitalizados, o descompasso do Poder Legislativo do Brasil com as modernas formas de gestão infelizmente se mostra ainda presente e impedindo a modernização do serviço público no Brasil. O veto pela Presidente da República de artigos específicos da Lei federal nº 12.682/12 tolheu de maneira expressa grandes medidas de agilidade processual e diminuição dos arquivos físicos,

[24] Processos Digitais na Prefeitura de Santos. Ana Carolina Falcão, João Roberto Lima e William Thomaz. Escola de Administração de Empresas de São Paulo. Fundação Getulio Vargas. São Paulo. 2015.

além dos enormes gastos de papel: somente nos ministérios do Governo Federal, o gasto total estimado com esse insumo é de R$ 4 milhões, ao custo de 20 mil árvores cortadas por ano[25]. O texto original previa a destruição dos documentos físicos após sua digitalização e ainda que as cópias digitais teriam o mesmo valor jurídico das cópias em papel. Sob alegação de conflitos com outras legislações em vigor (como a lei arquivística que impede a destruição de documentos) e, ainda, a falta de padronização para uma possível utilização de cópias digitais com fé pública - no veto da Presidência da República a fundamentação encontrada foi a de que "não estão estabelecidos os procedimentos para a reprodução dos documentos resultantes do processo de digitalização, de forma que a extensão de efeitos jurídicos para todos os fins de direito não teria contrapartida de garantia tecnológica ou procedimental que a justificasse[26]" - impede que, como no caso prático aqui em estudo, a Prefeitura de Santos destrua seus arquivos físicos após sua digitalização. Mesmo com o procedimento digital concluído, haverá necessidade de manutenção dos depósitos, funcionários e estrutura para manter armazenados papeis completamente desnecessários à administração dos diversos órgãos públicos.

Pelo menos o Poder Judiciário, com lei específica para tanto, a Lei nº 11.419/06, tem a garantia da fidedignidade de suas cópias informatizadas.

A regulamentação da certificação digital no Brasil mostra-se bastante moderada. Desde a criação, através da MP (medida provisória) 2.200-2/2001 (com a formação da ICP-Brasil e seu atual gestor o ITI), até a definição e legalização da certificação digital, por lei federal, através da Lei nº 12.686/12, o Estado Brasileiro dispõe de legislação que guia o gestor público na adoção de medidas de certificação digital.

Os passos adotados pela cidade de Santos foram: a criação de *e-mail* funcional com suas regras de uso claras; a criação de um gerenciador de identidade desenvolvido pelo próprio Departamento de Tecnologia da cidade de Santos; a formulação do projeto de implementação dos processos digitais; e por fim a aquisição da certificação digital para a

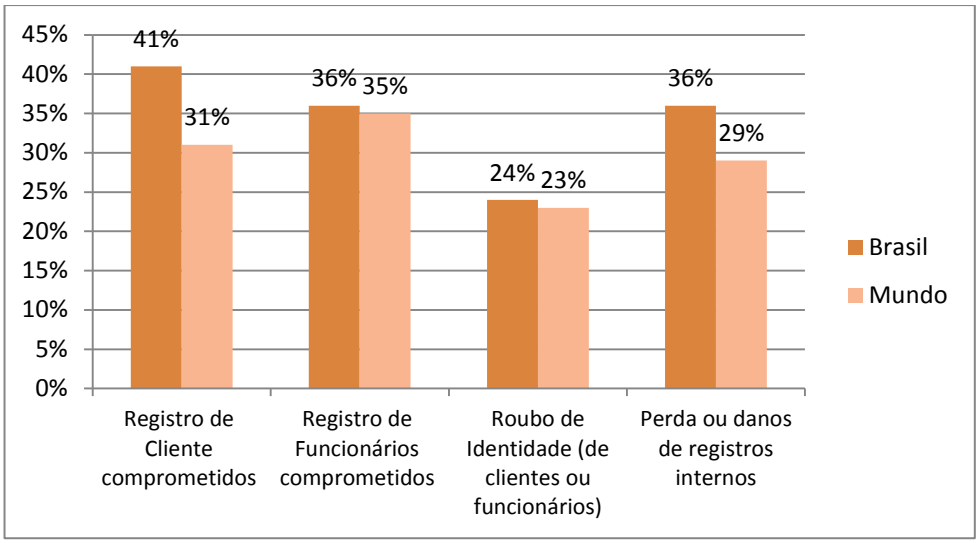
[25] "Estima-se ainda que, apenas com papel, haja um desperdício anual de quatro mil folhas por servidor. E, considerando que os ministérios possuem aproximadamente 50 mil servidores ativos, o uso total por ano pode chegar a 200 milhões de folhas, 400 mil resmas, isto é, pacotes com 500 folhas, quase vinte mil árvores e aproximadamente R$ 4 milhões". Eficiência contra o desperdício na administração pública. Daniela Cambaúva. Revista Desafios do Desenvolvimento/IPEA. Ano 10, edição 73. 2013.

[26] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Msg/VEP-313.htm.

correta fé pública dos documentos digitalizados. Assim, o arcabouço mostra-se moderado, mesmo com falhas, como os vetos da legislação aqui apresentados, e viável para que projetos como o caso de Santos possam se desenvolver com vigor.

Por fim, o questionamento sobre a possível maior vulnerabilidade da Gestão Pública por conta da adoção dos processos digitais não se mostra razoável. Mais uma vez, não existe sistema – físico ou digital – de armazenamento completamente seguro. Nesse sentido, estudo recente[27] da consultoria PwC (PriceWaterhouse Coopers) elenca os impactos dos incidentes de segurança (definidos na pesquisa como ataques cibernéticos contra a estrutura virtual das empresas) em corporações, com consulta entre 1º de fevereiro e 1º de abril de 2013:

Gráfico 1: Impacto dos incidentes de segurança



Fonte: o Autor, com dados da pesquisa da *Uma Defesa Ultrapassada*, da Consultoria PwC[28].

O Brasil encontra-se em patamar parecido com os demais países em termos de segurança da informação, exceto pelo maior número de registro de clientes comprometidos de acordo com o estudo aqui apresentado. Embora não haja pesquisa confiável sobre a vulnerabilidade dos sistemas públicos no Brasil, as empresas privadas possuem similaridade

[27] Uma defesa ultrapassada: Principais resultados da pesquisa global de segurança da informação 2014 – The Global State of Information Security Survey 2014. Disponível em https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf. Acesso em 10 de setembro de 2015.
[28] Idem ao 27.

nas dificuldades e desafios na gestão da informação: enquanto os bancos privados tem o dever de proteger o capital sob sua custódia, os bancos públicos tem o mesmo dever, com as mesmas regras legais.

O caminho para uma administração mais célere, em consonância com as modernas formas de gestão e em respeito aos princípios constitucionais do artigo 37 da Constituição Federal de 1988, em especial a publicidade e a celeridade, passam certamente pela digitalização dos processos por todos os órgãos públicos do Brasil.

A experiência de Santos é um alento: deve ser acompanhada de perto e, se mostrar-se vencedora, com certeza deverá ser replicada.

Este trabalho, por sua vez, juntamente com os outros artigos de Ana Carolina Falcão e João Roberto Lima, além do já citado trabalho que analisou os Processos Digitais na cidade de Santos, pretende nortear, com a maior riqueza de dados possível, outros órgãos ou entidades que apontam nessa direção.

Para tanto, os anexos aqui disponibilizados, todos eles com divulgação autorizada pela Prefeitura de Santos, têm como objetivo final o desenvolvimento do Brasil através de uma gestão mais próxima do cidadão e menos lenta e burocrática através dos processos digitais e sua possível certificação.

Anexo I – Instrução Normativa 1/2012: dispões sobre a gerência de identidades da Prefeitura Municipal de Santos (SSDH)

INSTRUÇÃO NORMATIVA Nº 1/2012- SEGES

DISPÕE SOBRE AS NORMAS E PROCEDIMENTOS PARA GERÊNCIA DE IDENTIDADES PROVIDAS PELA PREFEITURA MUNICIPAL DE SANTOS, E DÁ OUTRAS PROVIDÊNCIAS.

O SECRETÁRIO DE GESTÃO, no uso das atribuições que lhe são conferidas pelo inciso III do parágrafo único do artigo 60 da Lei Orgânica do Município, RESOLVE:

Art. 1º O Gerenciamento de Identidade tem como objetivo controlar todas as movimentações de um servidor ou prestador de serviço, para garantir em uma base de dados única o histórico de todos os serviços de Tecnologia da Informação - TI atribuídos a uma pessoa no âmbito da Prefeitura Municipal de Santos, e rege-se pelas disposições contidas na presente Instrução Normativa.

Art. 2º Para efeitos desta instrução, são adotadas as seguintes definições:

I- identificador único: sequência de caracteres que não se repete, com dígito verificador, que só deve ser utilizada pela pessoa que o recebeu, também conhecida como usuário ou "login";

II- senha: conjunto de caracteres que apenas o proprietário do identificador único conhece e, quando associado um ao outro, serve como forma de autenticação;

III- SSHD: Serviço de Segurança Humana e Digital – Aplicativo de TI desenvolvido pelo DETIC, para gerenciamento de identidades;

IV- TI: Tecnologia da Informação;

V- serviços/aplicativos de TI: serviços de tecnologia da informação que englobam a base genérica, os quais necessitam de autenticação (senha) para uso da rede e de arquivos, navegação na "internet", correspondência eletrônica (e-mail) e os sistemas de informação utilizados na Administração Municipal (exemplos: TRIBUS, RIS, SISAM, SIGES, SIAS, SAU, etc.);

VI- SAU: Sistema de Atendimento ao Usuário;

VII- DETIC: Departamento de Gestão da Tecnologia da Informação e Comunicações;

VIII- DEGEP: Departamento de Gestão de Pessoas;

IX- SEGES: Secretaria Municipal de Gestão.

Art. 3º Constituem normas para utilização da Gerência de Identidade: I- normas para cadastro;

II- normas para utilização do identificador único; III- normas para escolha de nova senha;

IV- normas para troca de senha.

Art. 4º Constituem normas para cadastro:

I – cadastro de servidores da Prefeitura Municipal de Santos:

a) o cadastro será realizado pelo DEGEP no sistema de folha de pagamentos;

b) a sincronização dos dados entre os sistemas da folha de pagamentos e o de gestão de identidade (SSHD) serão realizados duas vezes por semana, mantendo atualizadas as situações dos servidores e os seus respectivos acessos aos serviços de TI, bloqueando automaticamente os acessos em caso de desligamento das atividades.

II- cadastro de prestadores de serviço ou terceiros que necessitam de acesso:

a) as chefias de departamento deverão solicitar ao DETIC, via SAU, o cadastramento da pessoa em questão, especificando claramente os serviços de TI aos quais terá acesso;

b) para efetivação do cadastro, serão necessários os seguintes dados:

1- número do CPF/MF com dígito verificador (inclusive para estrangeiros);

2- número do registro de identidade com digito verificador, órgão emissor e UF do emissor;

3- endereço de "e-mail" (preferencialmente profissional);

4- indicação da empresa ou entidade a qual a pessoa é vinculada (Prodesan, CET, COHAB, TCESP, FUNCAMP etc.);

5- unidade organizacional e/ou setor de origem na empresa/entidade em questão;

6- regime de contrato (estatutário, celetista, estável, conveniado, voluntário, municipalizado, terceirizado etc);

7- cargo e/ou função;

8- nome completo sem abreviações; 9- data de nascimento;

10- sexo e estado civil;

11- nacionalidade e naturalidade;

12- endereço residencial completo, incluindo indicação de bairro, cidade, estado, país e CEP;

13 - nome da mãe;

14- número de telefone residencial e/ou celular;

15- identificador único do chefe de departamento responsável pelo cadastro.

§ 1º Quando o acesso for requerido para pessoas vinculadas a outras empresas da municipalidade que venham a utilizar os serviços de TI da Prefeitura, a solicitação deverá ser feita via Ofício;

§ 2º O solicitante será o único e geral responsável pelos dados enviados ao DETIC, bem como o encarregado de comunicar oficialmente o desligamento dos serviços para o bloqueio geral dos acessos aos sistemas informatizados.

Art 5º Constituem normas para utilização de identificador único:

I – cada pessoa receberá uma carta contendo o seu identificador único, que será utilizado como nome de usuário ou "login" nos serviços de TI, e uma senha provisória, que só servirá para que o próprio interessado acesse o sistema SSHD para efetuar a troca da senha e, assim, validar e ativar o acesso.

II – cada pessoa cadastrada terá responsabilidade de aceitar os termos de segurança e acesso do sistema de gestão de identidade (SSHD), mediante as seguintes condições:

a) o acesso aos recursos de TI será concedido a cada usuário de forma pessoal e intransferível;

b) cada usuário será o único e total responsável pela senha de acesso, assim como por todas as ações realizadas através desse código, razão pela qual deverá mantê-lo em sigilo absoluto e nunca fornecê-lo a outra pessoa;

Parágrafo único Caso haja tentativa de acesso com um identificador único por 10 (dez) vezes consecutivas sem sucesso (senha incorreta), este será bloqueado

automaticamente por 24 (vinte e quatro) horas.

Art. 6º Constituem normas para escolha de senha:

I - a nova senha deverá ser escolhida, cadastrada e ativada obrigatória e diretamente pelo responsável do identificador único;

II - a senha deverá conter no mínimo 6 (seis) caracteres, existindo pelo menos 2 (dois) dígitos numéricos e 3 (três) caracteres do alfabeto;

III - a senha não poderá ser fraca ou óbvia, a exemplo daquelas onde se utilizam caracteres de fácil associação com o dono, ou que sejam muito simples ou pequena, tais como:

a) o próprio identificador único ou registro funcional;

b) datas de aniversário, casamento, etc;

c) o próprio nome ou nome de familiares;

d) nomes de animais de estimação;

e) locais favoritos ou frequentados pelo responsável;

f) sequências numéricas simples;

g) palavras e unidades léxicas que constem de dicionários de qualquer língua;

Art. 7º O responsável pelo identificador único trocará a senha:

I - sempre que desejar, através do sistema SSHD, sendo recomendada a troca a cada seis meses;

II – obrigatoriamente, sempre que receber uma senha provisória gerada pelo sistema SSHD, seja na ativação do cadastro ou por motivo de esquecimento;

§ 1º Não haverá perda de acesso aos serviços de TI quando o proprietário efetuar a troca da senha já ativa através do SSHD;

§ 2º Em caso de esquecimento, deverá ser solicitada a emissão de uma senha provisória ao gestor de serviço de TI da unidade ou, na inexistência deste, deverá comparecer pessoalmente ao DEGEP munido de um documento original com foto, sendo aceitos para esta finalidade os seguintes documentos:

a) documento de identidade original emitido no Brasil com até 10 (dez) anos de emissão;

b) carteira de motorista modelo novo, com foto e no prazo de validade;

c) carteira de trabalho;

d) crachá (apenas para servidores da Prefeitura Municipal de Santos).

§ 3º Após a emissão da senha provisória, os serviços de TI ficarão bloqueados para o proprietário até que a troca seja efetuada.

Art. 8º Na gestão de identidade, cada serviço de TI associado à ferramenta de gestão de identidade (SSHD) possuirá no mínimo 1 (um) gestor, com as seguintes atribuições:

I – fazer o controle de quais pessoas (identificadores únicos) terão acesso ao recurso, bem como desativá-las, se for o caso;

II - reemitir senha provisória a qualquer pessoa cadastrada no sistema de gerenciamento de identidade (SSHD);

III - associar um identificador único ao serviço de TI, o que não importará em concessão de privilégios específicos, devendo estes ser atribuídos, se for o caso, diretamente no serviço ou aplicação em questão.

Art. 9º Constituem atribuições e responsabilidades do DETIC: I - manter sigilo das informações gerenciadas;

II - comunicar a SEGES quaisquer irregularidades na gestão de identidade;

III - emitir relatórios sobre as movimentações, manutenções de senhas e tentativas de descoberta das senhas de terceiros quando solicitado;

IV - manter o arquivo de "log" deste recurso definitivamente e íntegro para futura auditoria;

V - identificar e bloquear imediatamente identificadores únicos que venham a ter atitudes suspeitas ou com indícios de fraude, tais como:

a) elevação do próprio privilégio ou concessão de serviço de TI para uma pessoa não autorizada;

b) utilização de ferramentas maliciosas para obter acesso indevido;

c) divulgação da senha do próprio identificador único ou demais senhas para terceiros;

d) utilização de identificador único de terceiros;

e) cadastramento de dados de usuários que sejam falsos ou duvidosos;

f) emissão de carta de identificação única com senha provisória para outra pessoa

que não seja o responsável pelo identificador único.

Art. 10 O uso indevido do gerenciamento de identidade poderá levar à suspensão temporária do acesso do usuário a todos os serviços ou aplicativos de TI.

Publicada no Diário Oficial de 26 de setembro de 2012.

Anexo II – Instrução Normativa 1/2011: dispões sobre os procedimentos para a utilização dos correios eletrônicos providos pela Prefeitura Municipal de Santos

INSTRUÇÃO NORMATIVA Nº 1/2011 - SEGES, DE 09 DE AGOSTO DE 2011

DISPÕE SOBRE OS PROCEDIMENTOS PARA A UTILIZAÇÃO DOS CORREIOS ELETRÔNICOS ("E-MAIL") PROVIDOS PELA PREFEITURA MUNICIPAL DE SANTOS, E DÁ OUTRAS PROVIDÊNCIAS.

O SECRETÁRIO DE GESTÃO, no uso das atribuições que lhe são conferidas pelo inciso III do parágrafo único do artigo 60 da Lei Orgânica do Município, RESOLVE:

Art. 1º. A utilização dos correios eletrônicos ("e-mail") providos pela Prefeitura Municipal de Santos obedecerá às seguintes premissas:

I – como ferramenta de trabalho, o correio eletrônico deverá ser utilizado somente como apoio ao desenvolvimento das atividades laborais dos usuários, sendo vedada qualquer tipo de utilização para fins particulares;

II – qualquer computador conectado à Intranet ou à Internet tem acesso ao correio eletrônico por meio do "link" disponível no site oficial da Prefeitura Municipal de Santos;

III - os endereços de e-mail e as caixas postais disponibilizadas aos usuários são de propriedade da Prefeitura;

IV - todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

V - a criação de endereços de e-mail para uma unidade organizacional (Secretaria, Departamento) ou para um determinado serviço ou programa poderá ser efetivada mediante solicitação ao DETIC – Departamento de Gestão da Tecnologia da Informação e Comunicações;

VI – contas eventualmente criadas nos moldes referidos no inciso anterior serão de responsabilidade de uma única pessoa, ainda que as mensagens sejam redirecionadas a outras contas de e-mail (listas de distribuição);

VII - devido ao custo de armazenamento, o tamanho das caixas postais poderá ser

limitado de acordo com os recursos disponíveis;

VIII – contas inativas poderão ser bloqueadas devido ao custo de manutenção, caso o DETIC julgue necessário;

IX - todas as mensagens recebidas de origem desconhecida deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, a fim de evitar contaminação por vírus e outros riscos;

X - é proibido usar o correio eletrônico para transmissão e armazenamento de mensagens com conteúdo particular ou considerado impróprio pela Prefeitura, tais como:

a) mensagens que não estejam em conformidade com as regras legais, a moral, a integridade e os bons costumes, relacionadas à pornografia, pedofilia, obscenidades, terrorismo e discriminação racial, sexual, política ou religiosa, etc;

b) mensagens que contenham material que caracterize o incentivo ou a prática de atos ilícitos, lesivos aos direitos e interesses da Prefeitura ou de terceiros, inclusive aquelas cuja finalidade seja molestar, intimidar, assediar ou difamar outras pessoas, etc;

c) mensagens que possam ser caracterizadas como spam (e-mails em massa) ou que divulguem correntes, pedidos de donativos, venda de produtos, boatos, campanhas políticas ou religiosas, jogos, músicas, vídeos, etc;

d) mensagens que possam sobrecarregar um usuário, site ou servidor com e-mails muito extensos ou numerosas partes de e-mail;

e) mensagens que sabidamente contenham vírus eletrônico ou qualquer forma de rotina de programação de computador que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (computadores, servidores e sistemas), bem como aquelas que contenham anexos com as extensões (.bat, .exe, .src, .lnk, .com, .pif, .js,.vbs,.hta, .src, .cpl, .reg, .dll, .inf) ou de quaisquer outros formatos que representem um risco à segurança;

f) mensagens não autorizadas que contenham informações sigilosas e/ou que violem direitos de propriedade.

§ 1º . Caso o DETIC julgue necessário, poderão ser bloqueados, sem aviso prévio, e-mails com arquivos anexos que comprometam o uso de banda, perturbem o bom andamento dos trabalhos ou, ainda, exponham a rede a riscos de segurança.

§ 2º. Serão automaticamente bloqueados arquivos com código executável (.exe,

.com,

.bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) e outras extensões comumente utilizadas por vírus.

Art. 2º. Compete ao DETIC incluir, excluir, bloquear e alterar o perfil dos usuários de correio eletrônico da Prefeitura.

Art. 3º. Cada departamento deve indicar um gestor de correio eletrônico, ou seja, um usuário responsável por solicitar por meio do Sistema de Atendimento ao Usuário (SAU) a criação e exclusão das contas de e-mail de sua unidade.

§ 1º. Contas pertencentes a servidores estatutários ou celetistas serão automaticamente desativadas após seu cadastro no sistema da folha de pagamento ser alterado para inativo.

§ 2º. Cabe ao gestor do correio eletrônico solicitar o bloqueio temporário da conta em função de qualquer tipo de afastamento do usuário, bem como solicitar por intermédio do SAU a desativação de contas quando do rompimento do vínculo do usuário com a Prefeitura.

Art. 4º. O procedimento para a solicitação de contas de e-mail obedecerá aos seguintes parâmetros:

I - O usuário deverá estar previamente cadastrado no Sistema de Segurança Humana e Digital (SSHD);

II - A solicitação da criação da conta de e-mail será realizada através do Sistema de Atendimento ao Usuário (SAU), por usuário habilitado, conforme procedimento descrito no manual do sistema.

Art. 5º. O procedimento para a criação do endereço de e-mail obedecerá aos seguintes parâmetros:

I - A conta de e-mail deverá estar associada ao “login” gerado pelo sistema SSHD;

II - O endereço de e-mail deverá ser um nome amigável para a conta de e-mail acrescido do sufixo @santos.sp.gov.br

Parágrafo único. O endereço de e-mail será composto de nome e sobrenome, ou partes destes, conforme a disponibilidade. A combinação que determinará o endereço deve obedecer à sequencia abaixo:

a) primeiro nome + último sobrenome + sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: mariasilva@santos.sp.gov.br

b) primeiro nome + segundo nome ou sobrenome + sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: mariasantos@santos.sp.gov.br

c) primeiro nome + primeira letra do segundo nome + sobrenome + sufixo @santos.sp.gov.br

Exemplo:

Nome: Maria Santos Silva

e-mail: mariassilva@santos.sp.gov.br

d) primeiro nome sem a última letra + último sobrenome + sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: marisilva@santos.sp.gov.br

e) primeiro nome sem as 2 últimas letras + último sobrenome + sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: marsilva@santos.sp.gov.br

f) primeiro nome sem as 3 últimas letras + último sobrenome + sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: masilva@santos.sp.gov.br

g) primeira letra do primeiro nome + segundo nome+ sufixo @santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: msantos@santos.sp.gov.br

h) primeiro nome sem as 4 últimas letras + último sobrenome + sufixo

@santos.sp.gov.br Exemplo:

Nome: Maria Santos Silva

e-mail: msilva@santos.sp.gov.br

Art. 6º. O DETIC poderá verificar, sempre que julgar necessário, a obediência às normas e aos procedimentos constantes desta instrução normativa.

Art. 7º. O uso indevido dos serviços de correio eletrônico pode levar à suspensão temporária e até definitiva do acesso do usuário, podendo, conforme o caso, caracterizar eventual infração de natureza disciplinar.

Art. 8º. Faz parte desta instrução normativa o Anexo Único, o qual contempla definições de termos técnicos nela referidos.

Art. 9º Esta instrução normativa entra em vigor na data da publicação.

ANEXO ÚNICO

Caixa Postal - Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

Correio Eletrônico / e-mail - Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

Internet - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

Intranet - Rede interna, de uso corporativo.

Spam - Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

Usuários – Pessoas previamente cadastradas e autorizadas a utilizar os serviços de

correio eletrônico.

Vírus Eletrônicos - São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

Referências

BERTOL, V. R. L. Uma Proposta para Regulamentação da Certificação Digital no Brasil. Brasilia, 2009.

FERREIRA, Ana Amélia Menna Barreto de Castro. O sistema de certificação digital brasileiro f rente ao princípio da livre concorrência. Nova Lima, 2010.

FRIEDRICH D, Mostardeiro e Medina, Rosaclea Duarte. "Certificação Digital Acadêmica: Implantação do Sistema de Gerenciamento de Certificados Digitais ICPEDU na UFSM". Revista Novas Tecnologias na Educacao, CINTED-UFRGS. V. 5 Nº 2, Dezembro, 2007.

GUELFI, Airton Roberto. Analise das estruturas jurídico-tecnológicas que compõe a assinatura digital certificada digitalmente pela infraestrutura de chaves públicas do Brasil (ICP-Brasil). São Paulo, 2007.

RAMIRO, M. L. Gestão da Segurança da Informação: Certificação Digital. Rio de Janeiro, 2008.

VALCARENGHI, Emily Vivia. Impactos da adoção da certificação digital ICP-Brasil. Santa Catarina, 2015.