SENADO FEDERAL

Instituto Legislativo Brasileiro – ILB

Denilson Monteiro Rocha

Descaracterização de Informações Sensíveis nos Ambientes de Desenvolvimento e Homologação do Senado Federal

Brasilia

2019

Denilson Monteiro Rocha

Descaracterização de Informações Sensíveis nos Ambientes de Desenvolvimento e Homologação do Senado Federal

Monografia apresentada ao Instituto Legislativo Brasileiro – ILB como pré-requisito para a obtenção de certificado de conclusão do Curso de Pós-Graduação *Lato Sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo.

Orientador: Prof. Me. Pabblo Cardelino Ghobad

Brasilia

2019

Rocha, Denilson Monteiro.
Descaracterização de informações sensíveis nos ambientes de desenvolvimento e homologação do Senado Federal / Denilson Monteiro Rocha. -- 2019.
60 p.

Orientador: Pabblo Cardelino Ghobad.

Trabalho de Conclusão de Curso (especialização) -- Curso de pós-graduação *lato sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo – Instituto Legislativo Brasileiro, 2019.

1. Dados pessoais, armazenamento, aplicação por computador. 2. Segurança de dados. 3. Brasil. Congresso Nacional. Senado Federal. I. Título.

CDD 005.8

Denilson Monteiro Rocha

Descaracterização de Informações Sensíveis nos Ambientes de Desenvolvimento e Homologação do Senado Federal

Monografia apresentada ao Instituto Legislativo Brasileiro – ILB como pré-requisito para a obtenção de certificado de conclusão do Curso de Pós-Graduação *Lato Sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo.

Aprovada em Brasília, 12 de setembro de 2019 por:

Prof. Me. Pabblo Cardelino Ghobad
Orientador

Prof. Me. André Luiz Bandeira Molina
Avaliador

Sou grato a Deus, que em nenhum momento me deixou fraquejar ou desistir desse trabalho.

Agradecimentos

A Deus por ter me criado e por me dar saúde e disposição para superar os desafios.

Ao meu orientador, Prof. Me. Pabblo Cardelino Ghobad, pelo comprometimento, direcionamento e envolvimento com o tema; pelas correções e incentivo.

Ao meu pai Firmino (in memoriam) pelo apoio, esforço e extrema dedicação para a minha formação acadêmica

A minha mãe Elia pelo amor, incentivo e apoio incondicional; por estar sempre presente.

A minha esposa Giovane Mary por estar sempre ao meu lado e por apoiar meus projetos e desafios.

A minha filha Larissa por ter me ajudado neste trabalho, principalmente nas referências bibliográficas e na formatação do trabalho; a minha filha Letícia pela sua dedicação e companheirismo.

Aos meus colegas de sala, por terem apresentado um elevado senso de colaboração durante todo o curso.

Aos colegas do Prodasen que idealizaram esse curso de pós-graduação, especialmente ao Diretor Alessandro Pereira de Albuquerque e seu adjunto à época do início, Fabrício Fernandes Santana.

Aos professores do curso, pela dedicação e qualidade dos assuntos ministrados. Em especial agradeço ao Lauro Cesar por ter me incentivado a participar do curso e a Telma Venturelli pelo seu comprometimento e dedicação.

Ao Coordenador-Geral do curso, Yuri Morais, pela sua efetiva participação durante todo o período do curso.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

"A melhor maneira que o homem dispõe para se aperfeiçoar é aproximar-se de Deus."
(Pitágoras)

Resumo

O Senado Federal exerce um papel de destaque em nosso país; suas ações têm impacto sobre os rumos da nação e sobre a vida do povo brasileiro. Em consequência disso a atuação dos senadores recebe atenção especial por parte da mídia e da sociedade. No entanto, apesar do enfoque estar voltado para a atividade política do órgão, diversas atividades administrativas são executadas para garantir o funcionamento da casa. Na era atual em que o avanço da tecnologia da informação e dos meios de comunicação produziu mudanças significativas na forma que as atividades são executadas, a informação possui um papel preponderante no funcionamento da casa. Apesar da convergência das informações nos meios digitais ser imprescindível, esse modelo demanda um aumento na preocupação com a segurança da informação, cujos pilares são a disponibilidade, a integridade, a confidencialidade e a autenticidade. Além disso, ao longo do tempo foram criados diversos normativos para garantir a proteção dos dados pessoais. A Lei Geral de Proteção de Dados, prevista para entrar em vigor em agosto de 2020, enfatiza ainda mais essa necessidade. Alguns sistemas do Senado requerem especial atenção por armazenarem dados reais de produção em suas bases de desenvolvimento e homologação. Muitas dessas bases podem ser acessadas por servidores do Senado Federal, por parceiros contratados e por estagiários vinculados à área de TI. O presente estudo analisou o sistema de pessoal do Senado Federal para desenvolver um modelo de descaracterização dos dados pessoais nos ambientes de desenvolvimento e homologação. A partir da revisão teórica sobre o assunto, da legislação e das normas pertinentes a esse tema, foram propostas soluções para mitigar o risco associado ao acesso indevido a essas informações. Este estudo levou em consideração também os normativos internos do Senado Federal que estão relacionados ao tratamento desse problema. Por fim, um estudo sobre o mascaramento de dados deu origem a um modelo de proteção de dados sensíveis capaz de atender aos diversos requisitos da segurança da informação. Vislumbrando a possibilidade de expandir a solução para outros sistemas do Senado que possuem dados pessoais em suas bases, foi criado um modelo genérico de descaracterização derivado do modelo elaborado para o sistema de pessoal.

Palavras-chave: Dados pessoais; descaracterização; segurança da Informação.

Abstract

The Senate plays a prominent role in our country; Their actions have an impact on the course of the nation and on the lives of the Brazilian people. As a result, the work of senators receives special attention from the media and society. However, although the focus is on the political activity of the agency, several administrative activities are performed to ensure the functioning of the house. In the present age when the advancement of information technology and the media has produced significant changes in the way activities are performed, information plays a major role in the functioning of the house. Although the convergence of information in digital media is essential, this model demands an increase in concern for information security, whose pillars are availability, integrity, confidentiality and authenticity. In addition, various regulations have been created over time to ensure the protection of personal data. The General Data Protection Act, due to take effect in August 2020, further emphasizes this need. Some Senate systems require special attention because they store actual production data in their development and approval bases. Many of these bases can be accessed by Senate servers, contract partners, and IT-related trainees. The present study analyzed the Federal Senate personnel system to develop a model of decharacterization of personal data in development and homologation environments. From the theoretical review on the subject, the legislation and the relevant norms on this subject, solutions were proposed to mitigate the risk associated with improper access to this information. This study also took into consideration the Federal Senate's internal regulations related to the treatment of this problem. Finally, a study on data masking has given rise to a sensitive data protection model capable of meeting the diverse requirements of information security. Looking at the possibility of expanding the solution to other Senate systems that have personal data in their bases, a generic model of decharacterization derived from the model developed for the personnel system was created.

Keywords:Personal data; decharacterization; information security.

Lista de ilustrações

Lista de abreviaturas e siglas

	Lista de Siglas
APF	Administração Pública Federal
CEPESC	Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações
GSI/PR	Gabinete de Seguança Institucional/Presidência da República
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	*General Data Protection Regulation*
PCSI	Política Corporativa de Segurança da Infomação do Senado Federal
PGTI	Política de Governança de Tecnologia da Informação
PNSI	Política Nacional de Segurança da Informação
Prodasen	Secretaria de Tecnologia da Informação Prodasen
SEGP	Secretaria de Gestão de Pessoas
SF	Senado Federal
SGSI	Sistema de Gestão de Segurança da Informação
SIC	Sistemas de Informação e Sistemas de Comunicação
TIC	Tecnologias da Informação e Comunicação
SegCiber	Segurança Cibernética
SGBD	Sistema de Gerenciamento de Banco de Dados

Sumário

1 Introdução

A sociedade passou por diversas formas de organização ao longo do tempo. Segundo Bioni (2019), desde o estágio inicial, onde a economia era baseada na agricultura, até os dias atuais, em que a informação é o elemento central para o desenvolvimento econômico, houve mudanças significativas na forma de organização social. A transformação que estamos vivenciando é alavancada pela evolução tecnológica recente, a qual cria mecanismos capazes de processar e transmitir informações em quantidade e velocidade cada vez maiores. Essa transformação é tão evidente, que a era atual é conhecida como sociedade da informação.

A obra de Bioni (2019) ainda enfatiza que ao longo da era atual, a informação vem substituindo gradativamente recursos que estruturavam as sociedades agrícola, industrial e pós-industrial; passou-se a reconhecer cada vez mais a centralização da informação como fator de otimização do desenvolvimento econômico.

De acordo com Werthein (2000), a expressão "sociedade da informação" passou a ser utilizada nos últimos anos do século passado, substituindo o conceito de "sociedade pós-industrial", transmitindo mais precisamente o conteúdo do "novo paradigma técnico-econômico". Nesse modelo, a informação é a matéria-prima. As tecnologias permitem que o homem atue sobre a informação propriamente dita, criando implementos novos ou adaptando-os a novos usos. A informação passou a ser parte integrante de toda atividade humana.

Apesar dessa nova forma de organização não se resumir ao ambiente virtual, a computação eletrônica e a Internet são ferramentas fundamentais no processo de transformação digital. A informação que antes era materializada e armazenada fisicamente por meio da escrita, mudou seu padrão para uma linguagem compreensível pela máquina, a qual é constituída por bits (BIONI, 2019).

Essa mudança expandiu significativamente o potencial da informação, que por sua vez se tornou um elemento fundamental desse novo modelo econômico. Em virtude da mudança de paradigma, os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

A partir do aumento exponencial da capacidade de organizar os dados, criou-se um mercado baseado na extração e codificação das informações pessoais. Atualmente existem entidades que se dedicam a reunir informações que estão pulverizadas em inúmeras fontes, tais como bases de dados públicas e privadas, para vender e revender os dados pessoais dos cidadãos (BIONI, 2019).

O modelo de negócios foi se especializando de tal maneira que se criou uma rede

de organizações que atuam colaborativamente para produzir uma publicidade direcionada, potencializando esse mercado. Em consequência dessas ações, cada vez mais as atividades de processamento de dados têm ingerência na vida das pessoas (BIONI, 2019).

A preocupação com a proteção dos dados pessoais e sigilosos não é algo novo. A nossa Constituição Federal (1988), por exemplo, em seu artigo 5º, inciso XII, estabeleceu princípios para garantir a inviolabilidade do sigilo da correspondência e das comunicações telegráficas ou telefônicas. No entanto, dada a relevância da informação na sociedade atual, a proteção dos dados pessoais é de extrema importância para transmitir segurança a todos os envolvidos na economia digital, quer sejam organizações públicas ou privadas. Os dados pessoais devem receber tratamento especial para evitar que sejam acessados e utilizados de maneira indevida (MALDONADO; BLUM, 2018).

O trabalho de Fontes (2006) chama nossa atenção para essa questão. Segundo ele, a utilização de informações privilegiadas acontece constantemente na vida real. Para evitar que isso aconteça, as organizações devem adotar medidas para evitar que haja vazamentos de informação, sejam eles oriundos de descuido ou de má fé. Esse cuidado deve permear todo o ciclo de vida da informação, desde sua coleta, passando pelo seu uso e armazenamento, até sua exclusão.

1.1 Problema de Pesquisa

Dentre as atribuições da Secretaria de Tecnologia da Informação (Prodasen) está o provimento, por meio de recursos próprios ou de terceiros, de serviços, soluções, suporte e infraestrutura de tecnologia da informação para atender as necessidades do Senado Federal.

Diversas soluções requerem o desenvolvimento de sistemas que possuem em suas bases informações pessoais sensiveis que precisam ser protegidas contra acesso indevido. A necessidade de aumentar a capacidade de entrega de soluções de tecnologia da informação faz com que o Prodasen utilize a mão de obra de seus parceiros contratados de forma cada vez mais abrangente. Além disso, alguns sistemas que armazenam informações pessoais estão integrados a diversos outros sistemas, o que torna a segurança da informação no ambiente de desenvolvimento um tema bastante importante e complexo.

Para tratar dessas questões adequadamente, uma abordagem eficiente envolve a análise do ambiente interno e da legislação aplicável à proteção dos dados pessoais. É preciso identificar as informações sensíveis e classificá-las adequadamente para possibilitar a elaboração de um modelo de dados que garanta a privacidade das informações pessoais nos ambientes de desenvolvimento e homologação e que seja funcional.

Isso ocorre porque nesses ambientes, desenvolvedores de software e administradores de banco de dados possuem acesso irrestrito a todas as informações contidas nas bases que

eles utilizam em suas atividades. Para contornar esse problema, é preciso descaracterizar as informações que eles têm acesso.

O Senado Federal adquiriu recentemente uma ferramenta de mascaramento de dados. Essa ferramenta, apesar de possuir todas as funcionalidades exigidas no processo licitatório, deve partir de um modelo de descaracterização consistente para produzir os resultados desejados. O sistema de pessoal é bastante adequado para iniciar esse projeto porque concentra em suas bases uma grande quantidade de informações sensíveis.

O modelo a ser criado deve partir da identificação das informações sensíveis e da classificação das mesmas. Essas diretrizes devem servir de base para a elaboração de um fluxo de implantação para o caso específico do sistema de pessoal e também para a criação de um modelo genérico que possa ser aplicado a outros sistemas.

1.2 Objetivos

1.2.1 Objetivo Geral

Propor um modelo de descaracterização dos dados pessoais sensíveis nos ambientes de desenvolvimento e homologação dos sistemas do Senado Federal, utilizando o sistema de pessoal como estudo de caso.

1.2.2 Objetivos Específicos

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

- Revisar a teoria sobre descaracterização de dados e normas aplicáveis;
- Identificar as informações pessoais sensíveis nos ambientes de desenvolvimento e homologação dos sistemas de pessoal do Senado Federal;
- Classificar os dados utilizados nos ambientes de desenvolvimento e homologação dos sistemas de pessoal do Senado Federal como sensíveis ou não;
- Propor diretrizes para a descaracterização das informações reais sensíveis;
- Elaborar um fluxo para implantação das diretrizes estabelecidas nos ambientes de desenvolvimento e homologação no sistema de pessoal do Senado Federal;
- Propor um fluxo geral para implantação em outros sistemas do Senado Federal.

1.3 Metodologia

O estudo de caso é uma metodologia indicada para situações de pesquisa em que o olhar é particularizado. Especificamente para este trabalho de conclusão de curso a abordagem metodológica escolhida foi a de tratar a descaracterização das informações sensíveis disponíveis nos ambientes de desenvolvimento e homologação partindo de um primeiro sistema, o de pessoal.

Yin (2005) define o estudo de caso como estratégia de pesquisa que possui na sua essência esclarecer uma decisão ou um conjunto de decisões, assim como o motivo pelo qual foram tomadas, como foram implantadas e com quais resultados obtidos dentro de uma situação específica. A obra de Sampieri, Collado e Lucio (2013), apresenta a seguinte definição: "estudos que ao utilizar os processos de pesquisa quantitativa, qualitativa ou mista, analisam profundamente uma unidade para responder a formulação do problema, testar hipóteses e desenvolver alguma teoria".

Neste trabalho de conclusão de curso foram tratados de diversos desafios de pesquisa, destacando-se os seguintes:

- Identificação das informações sensíveis nos ambientes de desenvolvimento e homologação do sistema de pessoal do Senado Federal;
- Classificação das informações sensíveis nos ambientes de desenvolvimento e homologação dos sistemas de pessoal do Senado Federal;
- Criação das diretrizes para descaracterização das informações sensíveis;
- Elaboração de um fluxo para a implantação das diretrizes estabelecidas nos ambientes de desenvolvimento e homologação do sistema de pessoal do Senado Federal

Para alcançar os objetivos propostos, ao longo do trabalho foram feitas entrevistas com os todos os coordenadores da Secretaria de Gestão de Pessoas, compreendendo as seguintes áreas: Administração de Pessoal, Pagamento de Pessoal e Benefícios Previdenciários. Esta etapa foi extremamente importante, uma vez que as informações levantadas deram origem à elaboração de uma relação contendo as informações pessoais sensíveis.

Após reunir todas as informações necessárias, foi elaborado um Modelo de Entidade-Relacionamento simplificado contemplando as tabelas do sistema que possuem dados pessoais sensíveis.

Por fim, após análise da revisão da literatura, foram elaborados os modelos que servirão de base para a descaracterização das informações sensíveis.

1.4 Justificativa

Segurança da informação é um tema estratégico para as organizações e não pode ser negligenciado. Os servidores do Senado Federal, estagiários e os parceiros contratados, especialmente aqueles vinculados à área de TI, podem ter acesso a informações sigilosas, que precisam ser resguardadas.

Diante desse cenário, o projeto de descaracterização das informações sensíveis nos ambientes de desenvolvimento e homologação se fundamenta na preocupação com questões que precisam ser analisadas e tratadas com bastante atenção. Atualmente, todos os colaboradores diretamente envolvidos na manutenção de sistemas são obrigados a utilizar dados reais para testar por falta de alternativa. É de suma importância implementar medidas para garantir a segurança das informações pessoais no processo de desenvolvimento. Esse projeto deve partir da identificação das informações pessoais que precisam ser protegidas e dos sistemas que fazem uso dessas informações.

A criação de um modelo de proteção de informações que possa ser aplicado em diversos sistemas certamente será de grande importância para o Senado Federal.

1.5 Principais Contribuições

Este trabalho foi idealizado a partir da necessidade do Prodasen de implementar o processo de mascaramento de dados previsto no PDTI. Apesar de se tratar de um trabalho acadêmico, está voltado para um caso concreto. O estudo de caso do sistema de pessoal do Senado Federal é bastante significativo porque os resultados alcançados poderão ser expandidos para outros sistemas de possuem dados sensíveis em suas bases.

O referencial teórico demonstra a importância do tema, uma vez que aborda as principais leis e normas que dizem respeito ao mesmo. Esse arcabouço foi pesquisado à luz de um caso real e demonstra a necessidade de mascarar as informações.

Além de possuir uma fundamentação teórica consistente, de acordo com os objetivos propostos, os resultados esperados são preponderantemente de ordem prática. O referencial teórico foi concebido de forma que possibilitou sua ligação à parte prática desta obra. Mesmo estando sujeita a ajustes após sua aplicação, os resultados apresentados podem ser de grande importância para iniciar o processo de mascaramento. As diretrizes apresentadas levaram em consideração a ferramenta que o Prodasen dispõe para descaracterizar as informações sensíveis, assegurando assim a viabilidade deste estudo.

1.6 Organização

O presente trabalho está organizado da seguinte forma:

Capítulo 2: revisa os conceitos relacionados aos ambientes operacionais em bancos de dados relacionais e segurança da informação; apresenta a legislação relacionada à proteção dos dados pessoais (desde leis de alcance nacional até normativos internos do Senado Federal); apresenta conceitos referentes à descaracterização de informações.

Capítulo 3: apresenta resultados obtidos a partir da análise do referencial teórico; apresenta informações sobre o sistema de pessoal do Senado Federal e detalha sua arquitetura; apresentação da ferramenta que deverá ser utilizada para implementar a solução; descreve os procedimentos necessários para utilizar essa ferramenta no mascaramento dos dados pessoais; apresentação de um modelo de descaracterização específico para o sistema de pessoal e de um modelo genérico para outros sistemas que armazenam informações sensíveis;

Capítulo 4: traz as conclusões e sugere trabalhos futuros.

2 Referencial Teórico

Neste capítulo apresentamos conceitos importantes que ajudam a compreender os riscos associados ao ambiente operacional do Senado Federal. Para fundamentar este estudo, foi feita uma ampla análise, partindo das normas técnicas que determinam diretrizes gerais, passando por legislações de caráter nacional, até chegar às normas elaboradas pelo Senado Federal.

Além disso, este capítulo apresenta de forma detalhada informações sobre o mascaramento de dados, uma vez que essa técnica é o cerne da solução para tratar do problema de pesquisa.

2.1 Ambientes Operacionais em Bancos de Dados Relacionais

A criação de ambientes operacionais distintos é importante para evitar alterações em arquivos ou sistemas. O ideal é que toda organização que desenvolve seus próprios sistemas conte com ambientes computacionais distintos (MACHADO, 2012).

De acordo com a classificação adotada por Machado, o primeiro desses ambientes, o de desenvolvimento, é o ambiente no qual se geram os códigos dos sistemas; o segundo, o de homologação e testes, é onde o sistema recém-desenvolvido é aprovado; o terceiro ambiente, o de produção, é onde de fato o sistema é utilizado para a realização de atividades relacionadas ao negócio (MACHADO, 2012).

Na maioria dos casos, as organizações mantêm o foco das ações de segurança no ambiente de produção, que é sua principal fonte de informações sensíveis. Isso é justificável, uma vez que este ambiente está mais sujeito a ação de *hackers* e ataques externos.

No entanto, para garantir a confidencialidade, um dos pilares da segurança da informação, os ambientes de desenvolvimento e de testes também devem estar protegidos. Segundo Machado (MACHADO, 2012), um aspecto importante que deve ser levado em consideração é a existência de uma segregação lógica e física dos ambientes, com o intuito de evitar que pessoas responsáveis pelo desenvolvimento e testes dos sistemas tenham acesso aos dados da produção. Isso impede que os dados da produção sejam comprometidos por falhas nos sistemas, bem como impede que essas informações, que são vitais para as atividades do negócio, sejam acessadas por funcionários não autorizados, deixando a organização exposta a fraudes.

Uma premissa importante é que dados reais, que podem conter informações sensíveis,

não devem ser usados para teste. Os sistemas de teste devem utilizar apenas dados fictícios. É importante que esse ambiente seja o mais parecido possível com o de produção, no entanto, por medidas de segurança, os dados críticos, como informações pessoais, não devem fazer parte do ambiente de testes, garantindo assim a privacidade das informações. Permitir que dados confidenciais de produção sejam copiados e usados para ambientes de desenvolvimento e homologação aumenta o potencial de exposição, o que representa um risco para a organização.

2.2 Segurança da Informação

Uma vez que as informações das organizações estão armazenadas no ambiente computacional e elas dependem desse ambiente para realizar seus negócios, o tema segurança da informação tem se popularizado. À organização cabe o papel de definir políticas e regulamentos que explicitam sua filosofia. No entanto, como o acesso ao ambiente computacional está disponível para seus colaboradores, é necessário que todos tenham consciência de sua importância (FONTES, 2006).

A informação é vital para as organizações atuais. Segundo Fontes, segurança da informação é o conjunto de normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada.

De acordo com a Organização Internacional para Padronização/Comissão Eletrotécnica Internacional (ISO/IEC, 2014), a segurança da informação envolve a aplicação e gerenciamento de medidas de segurança apropriadas, considerando uma ampla gama de ameaças, com o objetivo de garantir o sucesso do negócio bem como a continuidade e minimização dos impactos de incidentes de segurança da informação.

No nível das organizações, muitas medidas vêm sendo adotadas ao longo do tempo para preservar as informações. A preocupação com a segurança não é algo novo, uma vez que ela já era inerente às formas de preservação da informação anteriores à era digital. A diferença é que, enquanto nos modelos de organização social anteriores a segurança física era o elemento principal, na sociedade atual, deve estar associada à segurança de TI para se tornar efetiva.

A segurança da informação pode ser gerenciada. O primeiro passo nesse sentido é identificar os riscos associados ao negócio da organização. Uma avaliação metódica deve focar nas falhas de segurança mais prováveis de ocorrer. Tal avaliação é importante para determinar as ações apropriadas, definir as prioridades para gerenciar os riscos de segurança da informação e implementar controles (HINTZBERGEN et al., 2018).

A segurança da informação é alcançada por meio da implementação de um con-

junto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware (HINTZBERGEN et al., 2018). Ela é importante tanto para os negócios públicos, quanto para o setor privado.

De acordo com a norma ISO/IEC 27000 (2014), a segurança da informação inclui três dimensões principais: confidencialidade, integridade e disponibilidade. Hintzbergen et al. apresenta os seguintes conceitos para essas dimensões (HINTZBERGEN et al., 2018):

- Confidencialidade – assegura que o nível necessário de sigilo seja alcançado, garantindo que a informação seja utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização. Busca também prevenir a divulgação intencional ou não intencional do conteúdo de uma mensagem;

- Integridade – assegura proteção contra modificações não autorizadas ao software, ao hardware e aos dados. O dado deve ser manter internamente e externamente correto e consistente;

- Disponibilidade – garante o funcionamento do sistema quando necessário. Mesmo em caso de falha, a informação deve estar acessível para o funcionamento da organização.

Além dessas dimensões, alguns autores ressaltam a relevância de critérios adicionais para que uma informação seja considera segura. Segundo Laureano e Moraes, esses critérios são os seguintes (LAUREANO; MORAES, 2005):

- Autenticidade – garante que a informação ou o usuário da mesma é autêntico;

- Não repúdio – impede que seja negada a autoria de uma operação ou serviço que modificou ou criou uma informação, pois existem mecanismos que garantem sua autoria;

- Legalidade – o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como pelos princípios éticos seguidos pela organização e desejados pela sociedade;

- Privacidade – não deve ser confundida com confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve estar restrita ao seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas;

- Auditoria – o acesso e uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

O elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas). A melhor forma de garantir a segurança da informação estratégica é atuar junto a todos que manipulam a informação e utilizar termos de confidencialidade.

A adoção das políticas de Segurança da Informação é extremamente importante, uma vez que proporciona a transparência e fornece credibilidade à empresa perante a sociedade. Além disso, as práticas da Segurança da Informação garantem que a informação certa esteja disponível na hora certa, para que a pessoa certa possa tomar a decisão estrategicamente adequada (LAUREANO; MORAES, 2005).

2.2.1 Normas Técnicas

As normas técnicas determinam regras, diretrizes e características mínimas para determinadas atividades e fornecem orientações que ajudam as organizações a se certificarem que estão adotando os procedimentos corretos.

As normas de segurança de informação, em especial, regem a elaboração e aplicação de um Sistema de Gestão de Segurança da Informação. Elas determinam controles, regras e diretrizes para a área e permitem que seja feita uma gestão da informação eficiente, com o objetivo de garantir confidencialidade, integridade e disponibilidades da informação, fatores essenciais para um sistema corporativo seguro.

Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005. As normas da série ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação. Elas abordam Sistema de Gestão de Segurança da Informação (SGSI), gestão de riscos, aplicação de controles, monitoramento, revisões e outros aspectos.

A ISO/IEC 27001 é a norma internacional de gestão de segurança da informação. Ela define requisitos para implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação. Ela não está restrita a empresas de tecnologia, podendo ser aplicada em qualquer organização, independentemente de porte ou setor (ISO/IEC, 2014).

Nessa série encontra-se também a ISO/IEC 27002, norma internacional que estabelece código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações. Baseado em uma avaliação de riscos, ela descreve como os controles podem ser estabelecidos (ISO/IEC, 2005).

Ao focarmos na confidencialidade, um dos pilares da segurança da informação estabelecidos pela ISO 27000, devemos considerar o mascaramento de dados como parte da estratégia de proteção dos dados sensíveis. A ISO 27002, fornece orientações para prevenir o vazamento de informações. De acordo com o guia de implementação desse controle, uma das formas de reduzir esse risco é através do mascaramento. Esse procedimento reduz

a probabilidade de um terceiro obter acesso a informações que devem estar protegidas (ISO/IEC, 2005). Fora do ambiente de produção, os desenvolvedores e testadores de sistemas precisam acessar informações que sejam funcionais para suas atividades, mas não podem ter acesso aos dados reais.

No entanto, a adoção de uma ferramenta não deve ser analisada de forma isolada. Para compreender melhor essa questão e implementar um controle eficiente sobre as informações, é necessário classificá-las para poder gerenciá-las adequadamente. Uma vez que a ISO 27001 não prescreve os níveis de classificação, cabe ao detentor da informação (no nosso estudo, o Senado Federal), baseado nos resultados da análise e da avaliação de riscos, definir seu nível de classificação: quanto maior o valor da informação (quanto maiores as consequências de uma quebra da confidencialidade), maior deve ser o nível de classificação.

A ISO 27001 permite que a organização defina suas próprias regras, e elas geralmente são definidas na política de classificação da informação, ou nos procedimentos de classificação. A ISO 27000 dá liberdade para que a organização implemente uma solução baseada em suas necessidades específicas.

Muitas das medidas de proteção dos dados pessoais assumiram papel ainda mais relevante com a normatização de medidas de proteção aos dados pessoais, dentre os quais destacamos o Regulamento Geral de Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados do Brasil.

De acordo com a Diretiva Europeia sobre Proteção de Dados Pessoais, dado pessoal é qualquer informação relacionada a uma pessoa identificada ou identificável. Uma pessoa pode ser identificada de maneira direta ou indireta, por números de documentos ou por fatores físicos, psicológicos, mentais, econômicos ou culturais. Isso abrange desde informações do documento de identificação até a gravação de imagens e vídeos. Esse conceito nos dá uma visão do universo de informações que requer proteção. Estão excluídos desse escopo apenas dados que não permitam determinar de maneira nenhuma a pessoa a que se referem (Advisera Expert Solutions Ltd, 2019).

O padrão ISO 27001 é arcabouço para a proteção das informações. Mesmo não englobando diretamente todos os requisitos da regulamentação de proteção de dados europeia, a implementação dessa norma permite elencar os dados pessoais como objetos da segurança da informação. A série de normas ISO 27000 fornece diversos padrões que asseguram essa proteção (Advisera Expert Solutions Ltd, 2019).

Existem muitos pontos em que a ISO 27001 ajuda a organização a se adequar à legislação de proteção de dados, dentre os quais se destacam os seguintes:

- Avaliação de risco – um dos novos requisitos da legislação de proteção de dados pessoais é a implementação de avaliações de impacto de proteção de dados; as

organizações terão que analisar os riscos para a sua privacidade. Essa mesma exigência existe na ISO 27001. De acordo com essa norma, as informações devem ser classificadas em termos de requisitos, valor, criticidade e sensibilidade à divulgação ou modificação não autorizada;

- Conformidade – o controle A.18.1.1 (Identificação de legislação aplicável e os requisitos contratuais) obriga a elaboração de uma lista de requisitos legislativos, estatutários, regulamentares e contratuais. Uma vez que as organizações precisam estar em conformidade com a legislação de proteção de dados pessoais, essa regulamentação terá de fazer parte dessa lista;

- Notificação de Violação – de acordo com a legislação de proteção de dados pessoais, as organizações terão que notificar às autoridades a violação de dados pessoais. A implementação do controle ISO 27001 A.16.1 (Gestão de incidentes de segurança da informação e melhorias) garante uma abordagem consistente e eficaz para a gestão de incidentes de segurança da informação;

- Gestão de ativos – o controle ISO 27001 A.8 (gerenciamento de ativos) inclui os dados pessoais como ativos de segurança da informação e permite que as organizações entendam quais são os dados pessoais, onde devem ser armazenados e por quanto tempo. Deve ser identificada também sua origem, quem pode ter acesso a eles e quais são os requisitos da legislação de proteção de dados pessoais;

- Privacidade – a legislação de proteção de dados pessoais torna obrigatória a preocupação com a privacidade no desenvolvimento de produtos e sistemas. O controle ISO 27001 A.14 (aquisição de sistemas, desenvolvimento e manutenção) garante que a segurança da informação é parte integrante dos sistemas de informação em todo o ciclo de vida;

- Relacionamentos com fornecedores – o controle ISO 27001 A.15.1 (Segurança da informação no relacionamento com fornecedores) visa a proteção dos ativos da organização que são acessíveis por fornecedores.

Além de promover a adoção de controles técnicos, elaboração de documentação estruturada e monitoramento, a implementação da ISO 27001 promove uma cultura e conscientização sobre incidentes de segurança nas organizações.

2.3 Legislação Aplicável na Administração Pública Federal

Não resta dúvida que a evolução tecnológica contribui para que as organizações automatizem seus serviços a fim de aumentar suas eficiência e eficácia (FERNANDES, 2010). Inserida nesse cenário, a Administração Pública brasileira sofre uma pressão cada

vez maior por aperfeiçoamento, aumentando assim a necessidade de atender, com maior qualidade, as demandas dos cidadãos por seus serviços (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015). No intuito de encontrar meios para alcançar esse objetivo, os sistemas computadorizados, constituídos pelos Sistemas de Informação e Sistemas de Comunicação (coletivamente chamados de SIC's), estão sendo empregados nas mais diversas atividades.

Com a adoção da tecnologia de forma mais abrangente, tem crescido a preocupação com as ameaças e vulnerabilidades de segurança a que estão sujeitos os sistemas de informação e comunicação (FERNANDES, 2010). As ameaças relativas à elevada interconectividade estão entre os maiores desafios da atualidade. Os riscos de ataque às redes e infraestrutura da informação, o aumento dos ataques cibernéticos e os incidentes de fraudes e roubos de dados são cada vez maiores (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015).

No âmbito da Administração Pública Federal (APF), ao longo do tempo, foram tomadas iniciativas e publicados diversos normativos para tratar de assuntos relacionados à segurança da informação. Em 2009, foi elaborado pela Administração Pública o documento intitulado "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0". Este importante instrumento de apoio ao planejamento estratégico governamental complementa a Instrução Normativa GSI/PR 01/2008 (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015).

A Instrução Normativa GSI/PR 01/2008 foi elaborada para atender às seguintes premissas:

- Tratar as informações como ativos valiosos para a eficiente prestação dos serviços públicos;
- Priorizar o interesse do cidadão, que é o beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta;
- Proteger as informações pessoais dos cidadãos;
- Incrementar a segurança das redes e bancos de dados governamentais;
- Orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

De acordo com essa instrução normativa, o GSI/PR tem a missão de coordenar as atividades de segurança da informação do governo. A necessidade de alcançar esse

objetivo deu origem à elaboração da estratégia de Segurança da Informação e Comunicação - SIC, que visa assegurar a execução de ações efetivas para evitar o uso das Tecnologias da Informação e Comunicação – TIC em ações ofensivas e exploratórias, bem como o acesso indevido às redes de computadores de setores e de infraestruturas críticas (FERNANDES, 2010). As ações de Segurança da Informação e Comunicação – SIC e de Segurança Cibernética – SegCiber, seguindo os preceitos da ISO 27002, têm como pilares de ação, a preocupação com a disponibilidade, integridade, confidencialidade e autenticidade.

Na última década, os temas de SIC e de SegCiber se tornaram mais relevantes e assumiram importância estratégica, abrangendo toda a APF, incluindo ações de segurança das infraestruturas críticas da informação.

Demonstrando preocupação com a privacidade, Brasil e Alemanha apresentaram em 2013, na III Comissão da Assembleia Geral das Nações Unidas, a resolução A/RES/68/167. Esse documento foi aprovado em consenso pelos 193 Estados Membros e visa conter a coleta injustificada de informações sensíveis (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015).

Sem desconsiderar importância dos normativos citados anteriormente, atualmente a APF tem o decreto 9.637/2018 como base de sua Política Nacional de Segurança da Informação – PNSI. Essa Política atualizou as normas contidas no Decreto 3.505/2000, bem como revisou e atualizou os princípios e diretrizes que orientam a atuação dos gestores públicos federais. Esse decreto foi instituído com a finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Em seu Art. 2º, o texto da Política estabelece que a segurança da informação abrange a segurança cibernética, a segurança física, a proteção de dados organizacionais bem como as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. No seu Art. 3º são elencados os princípios desta política, dentre os quais se destacam a visão abrangente e sistêmica da segurança da informação e a responsabilidade do país na coordenação de esforços, estratégias e diretrizes que sejam relacionadas ao temas (BRASIL, 2018a).

Visando garantir sua efetividade, a PNSI prevê a criação de planos nacionais que detalhem a execução das ações e os objetivos da Estratégia Nacional, bem como atribuam responsabilidades, definam organogramas e apresentem a análise de riscos e ações que garantam o alcance dos resultados esperados. Baseado nas diretrizes estabelecidas nessa Política, os órgãos da APF devem elaborar suas políticas e normativos internos, as quais devem estar em conformidade com as normas de segurança da informação editadas pelo GSI.

Apesar da adoção de todas as ações em curso, o grau de complexidade das ameaças é um grande desafio para a administração pública, uma vez que a segurança cibernética ainda apresenta muitas fragilidades. O acórdão 3.051/2014-TCU-Plenário demonstra que o

nível de maturidade ainda está aquém do desejado. Nesse documento, o Tribunal de Contas da União – TCU recomendou que o GSI/PR lançasse mão de uma estratégia pautada nos pilares da segurança da informação – disponibilidade, integridade, confidencialidade e autenticidade –, com o objetivo de fortalecer as ações de SIC e de SegCiber na APF (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015).

No intuito de sanar algumas deficiências e garantir o sigilo dos canais de comunicação, o Brasil conta com a Agência Brasileira de Inteligência – ABIN. Esse órgão foi criado em 1982 e está vinculado ao GSI/PR. Possui em sua estrutura o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações – CEPESC. Desde sua criação, a ABIN vem desenvolvendo soluções de segurança da informação e comunicações baseadas em algoritmos criptográficos de Estado, bem como executando trabalhos de pesquisa e desenvolvimento na área da segurança cibernética (BRASIL. Presidência da República. Gabinete de Segurança Institucional, 2015).

2.3.1 Lei Geral de Proteção de Dados

Dada a relevância do tema, diversos países estão preocupados com a proteção dos dados pessoais. No Brasil, foi criada a lei Nº 13.709, de 14 de agosto de 2018, cujo texto foi adaptado do GDPR (Regulamento Geral de Proteção de Dados, do inglês *General Data Protection Regulation*) europeu, que é considerado o padrão mundial nessa matéria.

Conhecida como Lei Geral de Proteção de Dados — LGPD, a norma brasileira tem o objetivo de garantir maior segurança em relação aos dados pessoais que podem ser coletados na internet. Frequentemente esses dados são usados para diversos fins não desejados, como propagandas e *spams* feitos por empresas aos consumidores, bem como são vendidos sem o consentimento dos donos.

Dado que o art. 2º da LGPD, estabelece que o respeito à privacidade é um de seus fundamentos, deve haver uma preocupação crescente com os dados coletados e armazenados pelas organizações. Para garantir a efetividade dessa lei, os órgãos públicos e entidades privadas têm que preservar as informações sensíveis armazenadas em seus bancos de dados.

De acordo com Maldonado e Blum (MALDONADO; BLUM, 2018), apesar de não haver uma definição expressa, tanto a GDPR como a LGPD deixam claro que dados que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, constituem uma categoria especial de dado pessoal. O objetivo da lei é proteger este tipo de informação quando ela está vinculada a uma pessoa natural identificada ou identificável.

Esses dados devem ter um tratamento especial para evitar que sejam publicados de forma indevida. De acordo com o art. 11 da LGPD, o tratamento de dados pessoais

sensíveis somente poderá ocorrer quando o titular ou seu responsável legal consentir de forma específica e destacada, para finalidades específicas (BRASIL, 2018b).

Apesar de ter o foco principal na proteção de dados coletados por meio da Internet, os órgãos públicos e entidades privadas que detêm informações sensíveis devem adotar medidas de segurança e implementar boas práticas para garantir a segurança das informações e o sigilo dos dados. De acordo com o art. 46 da LGPD, os agentes de tratamento devem garantir a proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. As medidas de segurança devem ser observadas desde a fase de concepção do produto ou do serviço, até a sua implementação e produção. Os agentes de tratamento são obrigados a garantir a segurança da informação prevista nesta lei em relação dos dados pessoais.

2.3.2 Lei de Acesso à Informação

A Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2011), conhecida como Lei de Acesso à Informação – LAI, foi criada com o objetivo de regular o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. O primeiro desses dispositivos constitucionais garante a todas as pessoas o direito de acesso a informações de seu interesse particular ou de interesse público, ao passo que o segundo determina que cabe à administração pública estabelecer lei para gerir a documentação governamental e franquear sua consulta a todos que dela necessitem.

A LAI, atendendo a esses preceitos constitucionais, criou mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades. Essa lei tem abrangência geral e vale para os três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Conta e Ministério Público. Até mesmo as entidades privadas sem fins lucrativos são obrigadas a dar publicidade acerca de informações referentes ao recebimento e à destinação dos recursos públicos que recebem.

O objetivo da LAI é estabelecer os procedimentos a serem observados por todos os órgãos públicos, de modo a garantir o acesso de qualquer cidadão ou entidade às informações e documentos públicos dos diversos órgãos integrantes da administração direta e indireta.

De acordo com o inciso I do Art. 3º da LAI, a publicidade passou a ser a regra e o sigilo a exceção. De maneira geral, as pessoas podem ter acesso a qualquer informação pública produzida ou custodiada pelos órgãos e entidades da Administração Pública (BRASIL, 2011).

Destacam-se nessa lei os seguintes princípios:

- Divulgação de informações de interesse público, independentemente de solicitações;
- Utilização de meios de comunicação viabilizados pela tecnologia da informação;
- Fomento ao desenvolvimento da cultura de transparência na administração pública;
- Desenvolvimento do controle social da administração pública.

Apesar de ter sido criada para priorizar a publicidade, a LAI prevê algumas exceções, principalmente nos casos em que a divulgação indiscriminada pode trazer riscos à sociedade ou ao Estado.

De maneira geral, as informações sob a guarda do Estado são públicas, devendo o acesso a elas ser restringido apenas em casos específicos e por período de tempo determinado. A LAI prevê como exceções à regra da ampla divulgação o acesso aos dados pessoais, às informações classificadas por autoridades como sigilosas e às informações sigilosas com base em outras leis, tais como as que garantem os sigilos bancário, fiscal e industrial.

Em seu artigo 31, a LAI prevê restrições ao acesso das informações pessoais, uma vez que seu tratamento deve ser feito de forma transparente e com respeito a intimidade, vida privada, honra e imagem, bem como a liberdades e garantias individuais. As informações pessoais não são públicas e terão seu acesso restrito. Elas só podem ser acessadas pelos próprios indivíduos ou por terceiros nos casos excepcionais previstos na Lei. A LAI prevê a responsabilização pelo uso indevido dessas informações (BRASIL, 2011).

No rol das exceções à publicidade das informações, encontram-se também as que são classificadas como sigilosas, cuja divulgação pode colocar em risco a segurança da sociedade ou do Estado. Por isso, apesar de serem públicas, o acesso a elas deve ser restringido por meio da classificação da autoridade competente. Essas informações são classificadas como ultrassecretas, secretas e reservadas, conforme o risco que sua divulgação pode proporcionar à sociedade ou ao Estado.

Por fim, como exceções à regra da ampla publicidade, o Decreto 7.724 (art. 13), que regulamenta a LAI no Poder Executivo Federal, também prevê que não serão atendidos pedidos de informação que sejam:

(i) genéricos;

(ii) desproporcionais ou desarrazoados; ou

(iii) que exijam trabalhos adicionais de análise, interpretação ou consolidação de dados e informações, ou serviço de produção ou tratamento de dados que não seja de competência do órgão ou entidade.

2.4 Normativos Específicos do Senado Federal

2.4.1 Comissão de Acesso

Em função da vigência da LAI, a partir de 16 de maio de 2012, o Senado Federal, através do Ato nº 9 de sua Comissão Diretora, regulamentou o acesso aos dados, informações e documentos de interesse da sociedade e do Estado, bem como estabeleceu medidas de preservação dos direitos individuais, no que diz respeito ao acervo informacional do Senado Federal (BRASIL. Congresso. Senado, 2012).

Em seu Parágrafo único do Art. 1º, o Ato nº 9 da Comissão Diretora enfatiza o compromisso do Senado Federal de facilitar o acesso aos dados, informações e documentos de interesse coletivo ou geral produzidos internamente ou sob sua guarda. O Art 2º, reafirma alguns dos princípios da LAI, dentre os quais podemos ressaltar a observância da publicidade como preceito geral e o sigilo como exceção. Para isso, o Senado Federal deve utilizar meios de comunicação viabilizados pela tecnologia da informação e adotar procedimentos objetivos e ágeis de forma transparente e clara, utilizando uma linguagem de fácil compreensão (BRASIL. Congresso. Senado, 2012).

Apesar de ser bastante abrangente, uma vez que abarca atos, fatos, documentos e informações de competência do Senado Federal, as informações de natureza pessoal ou sigilosa constituem uma exceção ao princípio da publicidade. Essas restrições são garantidas com base em preceitos legais e constitucionais.

No Art. 28, o Ato determina que o tratamento das informações pessoais deve respeitar a intimidade, vida privada, honra e imagem das pessoas, bem como suas liberdades e garantias individuais. O parágrafo 1º desse artigo assinala que aquele que obtiver acesso a essas informações será responsabilizado por seu uso indevido.

Diversos sistemas do Senado Federal armazenam informações pessoais que estão amparadas por essas garantias. No modelo atual, as bases de dados do ambiente de produção são replicadas integralmente para os ambientes de desenvolvimento e homologação, o que representa um risco para a preservação da confidencialidade, uma vez que essas informações são acessadas por equipes de desenvolvedores compostas por servidores do Senado Federal, por técnicos de empresas contratadas e por estagiários.

Seguindo as diretrizes do Ato, o mascaramento dos dados se destaca como uma solução para garantir a proteção das informações sem comprometer a capacidade de entrega das equipes.

2.4.2 Política Corporativa de Segurança da Informação

O Ato da Comissão Diretora Nº 9, de 2017 instituiu a Política Corporativa de Segurança da Informação do Senado Federal – PCSI. Essa política estabelece princípios,

diretrizes estratégicas, responsabilidades, competências e subsídios para a implantação do sistema de gestão de segurança da informação, a fim de viabilizar e assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas (BRASIL. Congresso. Senado, 2012).

De acordo com o Ato, a PCSI está pautada nos seguintes princípios:

- Transparência das informações recebidas, produzidas, processadas, armazenadas e transmitidas pelo Senado Federal;
- Garantia da disponibilidade, da integridade e da autenticidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pelo Senado Federal;
- Garantia da confidencialidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pelo Senado Federal, quando legalmente exigida;
- Planejamento das ações de segurança da informação por meio de sistema de gestão da segurança da informação que considere processos de trabalho e recursos humanos, materiais e tecnológicos.

A classificação da informação, segundo a PCSI, é pressuposto para seu correto tratamento, bem como visa assegurar nível adequado de proteção em relação a suas propriedades. A classificação da informação baseia-se em norma específica. Os controles físicos, administrativos e tecnológicos necessários para assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações deverão ser implementados conforme a classificação a elas atribuída.

O acesso de usuários colaboradores e externos a dados, documentos ou instalações que contenham informações sensíveis, sigilosas ou de acesso restrito deve ser precedido de assinatura de termo de confidencialidade (BRASIL. Congresso. Senado, 2012).

O processo de análise e avaliação de riscos constituem a base para o estabelecimento de controles adequados e para o tratamento dos principais riscos de segurança da informação.

A política, em seu Art. 12, estabelece que os recursos de informação do Senado Federal devem ser utilizados para os fins institucionais, devendo ser respeitados a legislação vigente, a PCSI, as normas complementares de segurança da informação, as obrigações contratuais e os direitos autorais.

Por fim, conforme descrito no Art. 14 do Ato, pode-se ressaltar que a gestão de áreas seguras e instalações físicas críticas tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações do Senado Federal que possam causar perda, roubo ou comprometimento de informações.

2.4.3 Plano Diretor de Tecnologia da Informação

Em maio de 2015, o Senado Federal (SF) aprovou projeto estratégico com o objetivo de instituir a Política de Governança de Tecnologia da Informação (PGTI), publicada em outubro de 2016, por meio do Ato da Comissão Diretora nº 8, de 2016 (BRASIL. Congresso. Senado, 2017).

Foram definidos papéis e responsabilidades relativas à Governança e à Gestão de TI no Senado Federal.

O Plano Diretor de Tecnologia da Informação possui o seguinte escopo:

- Diretrizes de TI;
- Ações estruturantes relacionados às diretrizes de TI;
- Projetos voltados ao tratamento dos principais riscos de TI;
- Projetos voltados ao atendimento das áreas de negócio do SF;
- Indicadores para avaliação do desempenho da TI.

A partir das Diretrizes Estratégicas do Senado Federal para o biênio 2017-2019, foram definidos 17 projetos estratégicos, dentre os quais faz parte a implementação do Plano Diretor de Tecnologia da Informação (PDTI).

As questões relativas à Governança e à Gestão de TI possuem, portanto, estatura estratégica para o Senado Federal, estando materializadas no PDTI/SF e em seu conjunto de projetos e de ações estruturantes.

2.4.3.1 Diretrizes de Tecnologia da Informação

O primeiro item do escopo do PDTI é composto pelas diretrizes de TI. No tema "Formas de Provimento de Serviços de TI", verificamos que uma das diretrizes do plano consiste em explorar a terceirização de serviços de forma a ampliar a capacidade de entrega. Esse direcionamento já está sendo seguido pelo Prodasen, tendo sido alcançados bons resultados até o momento.

Apesar desse incremento na produtividade ser bastante positivo, as boas práticas de segurança da informação prevêm a elaboração de contratos de confidencialidade. Isso é necessário porque os colaboradores internos de uma organização e os terceirizados, especialmente aqueles vinculados à área de TI, no exercício de suas atividades, muitas vezes, têm acesso a informações sigilosas, que precisam ser resguardadas.

Ao tratar da organização da segurança da informação, o Tribunal de Contas da União, em sua publicação sobre boas práticas em segurança da informação, enumera

diversos itens, dentre os quais se encontra parte do texto do Acórdão 1382/2009 Plenário do TCU, que possui a seguinte redação (BRASIL. Tribunal de Contas da União, 2012):

> "(...) envide esforços para que a [Área de TI] do Ministério seja dotada de servidores ocupantes de cargos efetivos em número suficiente, capacitados e treinados para exercer atividades estratégicas e sensíveis, sobretudo as que possam comprometer a segurança da tecnologia da informação do órgão, implantando controles compensatórios quando houver necessidade de que estas atividades sejam executadas por terceiros, à semelhança das orientações contidas na NBR ISO/IEC 17799:2005, item 6.1.3 - Atribuição de responsabilidades para a segurança da informação, e no Cobit 4.1, PO4.13 - Pessoal chave de TI;"

2.4.3.2 Projetos voltados ao atendimento das áreas de negócio do SF

A diretriz de Projetos de TI para atendimento as áreas de negócio engloba iniciativas importantes. Dentre os projetos em execução que envolvem dados pessoais, se destacam os seguintes:

- Automação dos processos da Secretaria de Gestão de Pessoas – SEGP;
- Aquisição de Solução para Auditoria e Proteção de Bancos de Dados;
- Contratação e Implantação do novo sistema SaúdeSF.

A automação da SEGP, bem como o novo sistema, pode envolver o trato direto com dados sensíveis. Já a solução de auditoria indica a preocupação da casa com o tema aqui tratado.

2.4.3.3 Ações Estruturantes

As ações estruturantes garantem que os projetos prioritários sejam conduzidos adequadamente do ponto de vista técnico, minimizando os riscos de execução (BRASIL. Congresso. Senado, 2017).

Essas ações estão agrupadas em dois focos: Realização das Diretrizes de TI e Tratamento de riscos de TI. No primeiro, uma das ações estruturantes é a "Contratação de Serviços de Desenvolvimento de Software – ampliação da capacidade de entrega". Essa ação está relacionado com a diretriz de TI mencionada no subitem 2.4.3.1. No grupo das ações com foco no tratamento de riscos de TI, encontra-se a ação "Política de Segurança da Informação"que deve englobar medidas de proteção às informações pessoais (BRASIL. Congresso. Senado, 2017).

2.4.3.4 Investimentos em infraestrutura de TI

A fim de materializar as ações propostas, o PDTI estabeleceu valores expressivos de investimentos na infraestrutura de TI do SF. Dentre os itens contemplados com esses investimentos, encontram-se os seguintes:

- Software para descaracterização de dados em ambiente de homologação para segurança da informação, com valor estimado de R$ 1.500.000,00;
- Contratação de fábrica de software para manutenções corretivas e evolutivas, com valor estimado de R$670.000,00.

Uma vez que esses investimentos já foram realizados, a etapa seguinte consiste em desenvolver um modelo de descaracterização das informações utilizando o software CA Data Masking adquirido através de processo licitatório.

2.5 Descaracterização e Informações Sensíveis

Atualmente, as organizações precisam estar em conformidade com a política de privacidade dos dados dos clientes e com a legislação de proteção dos dados pessoais. Para atingir esses objetivos, muitas delas estão adotando o mascaramento de dados na transferência de dados de ambientes de produção (normalmente mais protegidos) para ambientes de testes (menos seguros) ou para outros sistemas. O mascaramento de dados desidentifica ou mistura de elementos de dados especificados no seu modelo a fim de protegê-los do acesso não autorizado por seus usuários finais.

A identificação dos dados sensíveis e as medidas necessárias para efetuar o mascaramento precisam estar em vigor quando a informação do cliente é extraída do ambiente de produção. Normalmente, essas informações confidenciais incluem informações pessoais identificáveis, registros de saúde, registros gerais de clientes e quaisquer outros dados corporativos confidenciais que exijam proteção.

As organizações devem estar atentas a essas questões para impedir que suas informações sejam utilizadas para fim diverso do seu objetivo. Dessa forma, o mascaramento de dados se configura como uma medida adequada para evitar que informações sensíveis fiquem expostas nos ambientes de desenvolvimento e homologação. Essa solução fornece um substituto funcional, similar ao original, com as mesmas características do dado real.

Segundo Ajayi e Adebiyi (AJAYI; ADEBIYI, 2014), o Mascaramento de Dados é um processo que tem o objetivo de obscurecer informações específicas armazenadas em bancos de dados. Ele garante que os dados confidenciais sejam substituídos por dados realistas, mas não reais e evita que informações confidenciais estejam disponíveis fora do ambiente autorizado.

O mascaramento de dados deve ser feito no processo de cópia dos dados de produção para outros ambientes, de modo que as cópias criadas para suportar os processos de desenvolvimento e homologação não exponham informações confidenciais, evitando assim riscos de vazamento de informações.

O mascaramento não altera o formato dos dados, e sim, apenas os valores das informações. Esta alteração pode ser feita de diversas maneiras, como por exemplo, por meio da criptografia, do embaralhamento de caracteres e da substituição de caracteres ou palavras. Independentemente do método utilizado, os valores devem ser alterados de tal forma que seja impossível a identificação dos dados ou a aplicação de engenharia reversa (AJAYI; ADEBIYI, 2014).

Existem diversos sistemas no Senado Federal cujos dados nos ambientes de desenvolvimento e homologação necessitam ser atualizados com frequência. O sistema de pessoal é um caso típico, uma vez que as informações disponíveis para testes devem refletir com bastante precisão uma situação real. Para evitar a exposição dos dados confidenciais, o processo de mascaramento deve ser executado de forma automatizada.

No procedimento de mascaramento deve-se levar em consideração o fato que o leiaute do banco de dados está sujeito a eventuais alterações. Para automatizar esse procedimento é recomendável manter uma lista de colunas sensíveis para evitar que o código seja reescrito a cada alteração no leiaute do banco de dados.

Os métodos mais comuns de mascaramento utilizam diversas técnicas. Dentre as mais comuns estão:

- Criptografia / Descriptografia – protege uma informação de modo que apenas o emissor e o receptor consigam compreendê-la. Os dados são criptografados de uma lado e descriptografados do outro;
- Substituição – substitui os dados reais por valores existentes. Ex: substituição do endereço real por informações aleatórias contidas em uma base de endereços;
- Embaralhamento – similar ao método de substituição, mas utiliza informações de outros registros da coluna para substituir o dado real;
- Variação Numérica – aplica uma variação sobre valores dos dados reais. Pode ser utilizado aplicando uma variação percentual aleatória sobre campos numéricos ou variação de dias sobre datas;
- Anular ou Apagar Informações – apaga as informações de um campo;
- Cifragem – variação do método de apagar o dado original. Consiste em substituir parte do dado real por um determinado conjunto de caracteres. Ex: substituição de

parte do número do cartão de crédito por "X"ou parte do número do telefone por "*".

Com o objetivo de preparar um modelo de mascaramento adequado, Ajayi e Adebiyi (2014) apresentam as seguintes diretrizes, no formato de 5 (cinco) leis do mascaramento de dados:

- O mascaramento não deve ser reversível. Não deve permitir que sejam recuperados os dados sensíveis originais;
- Os dados resultantes devem representar os dados de origem. O objetivo do mascaramento de dados ao invés de simplesmente gerar dados aleatórios é fornecer informações não confidenciais que ainda se assemelhem a dados de produção para fins de desenvolvimento e teste. Isso pode incluir distribuições geográficas, distribuições de cartão de crédito (talvez deixando os primeiros 4 números inalterados, mas embaralhando o restante), ou manter a legibilidade humana de nomes e endereços (falsos);
- A integridade referencial deve ser preservada. Se o número do cartão de crédito é chave primária e é embaralhada como parte do mascaramento, todas as instâncias deste número devem ser embaralhadas de forma idêntica;
- Apenas deve ser mascarado um dado não confidencial se ele puder ser usado para recriar dados confidenciais. A princípio, devem ser mascaradas apenas informações consideradas sensíveis. Por exemplo, se você embaralha a identificação de um prontuário médico, mas o código de tratamento de um registro aponta para um único prontuário, é necessário embaralhar esses códigos também. Esse ataque é chamado de análise de inferência e sua solução de mascaramento deve protegê-lo;
- O mascaramento deve ser um processo repetitivo. O mascaramento único é ineficaz e praticamente impossível de ser mantido. Os dados de desenvolvimento e teste precisam representar os dados de produção. Se o mascaramento não for um processo automatizado, ele será ineficiente, caro e não será efetivo.

O mascaramento de dados deve seguir diversas premissas para que os dados mascarados preservem as características dos dados originais. Ajayi e Adebiyi (2014) apresentam os seguintes requisitos:

- Preservação do Formato – o mascaramento deve gerar dados com a mesma estrutura dos dados originais. Ex: se os dados originais tiverem de 2 a 30

caracteres, o mascaramento deverá produzir dados de 2 a 30 caracteres. Um exemplo comum são as datas, que devem produzir números nos intervalos corretos para dia, mês e ano, em um formato específico. O algoritmo de mascaramento deve identificar o "significado"de dados de origem, como "31.03.2012", "31 de março de 2012"e "31/03/2012", e gerar uma data adequada no mesmo formato;

- Preservação do Tipo do dado – no armazenamento de dados relacionais, deve-se manter os tipos de dados. Bancos de dados relacionais exigem uma definição formal de colunas de dados. Não é possível, por exemplo, incluir texto em uma coluna com formato numérico ou de data. Na maioria das vezes, as máscaras preservam implicitamente o tipo de dados, mas nem sempre isto ocorre. Algumas vezes, os dados podem ser "transmitidos"de um tipo de dados específico para um tipo de dados genérico (por exemplo, varchar);
- Preservação do Gênero – ao substituir nomes, os nomes masculinos devem ser substituídos por outros nomes masculinos e, do mesmo modo, os femininos, apenas por nomes femininos;
- Integridade Semântica – os bancos de dados geralmente impõem restrições adicionais aos dados. Além de garantir a integridade do formato e do tipo de dados, é necessário que o valor armazenado faça sentido para o seu contexto;
- Integridade Referencial – caso um atributo em uma tabela ou arquivo se referira a outro elemento em uma tabela ou arquivo diferente, a referência deve ser mantida de forma consistente. Isto é essencial porque os bancos de dados relacionais otimizam o armazenamento de dados, permitindo que um conjunto de elementos de dados se "relacione"ou se refira a outro. As tecnologias de mascaramento devem manter a integridade referencial quando os dados são copiados entre bancos de dados relacionais, assegurando que o carregamento dos novos dados funcione sem erros e evitando a interrupção de aplicativos que dependem desses relacionamentos;
- Valor Agregado – Os valores total e médio de uma coluna de dados mascarada devem ser mantidos exatos ou aproximados;
- Distribuição de frequência – em alguns casos, os usuários precisam de distribuição de frequência aleatória, enquanto em outros, os agrupamentos lógicos de valores devem ser mantidos para que os dados mascarados possam ser usados. Por exemplo, se os dados originais descrevem localizações geográficas de pacientes com câncer por código postal, códigos postais aleatórios descartariam informações geográficas valiosas. A capacidade

de mascarar dados, mantendo certos tipos de padrões, é essencial para manter o valor dos dados mascarados para análise;

- Exclusividade – os valores mascarados devem ser exclusivos. Por exemplo, os CPFs duplicados não são permitidos quando a exclusividade é uma restrição de integridade obrigatória.

2.6 Conclusão do Capítulo

A descaracterização das informações sensíveis não se limita a questões operacionais da ferramenta adquirida recentemente pelo Senado Federal. Existe um gama de aspectos que devem ser considerados antes de executar o mascaramento dos dados pessoais. Para definir a forma e o objeto desse procedimento, deve se partir da análise do ambiente operacional e pautar as ações nas recomendações das normas de segurança da informação. É importante também conhecer a legislação para adotar as medidas cabíveis antes da vigência da LGPD, prevista para agosto de 2020.

Além disso, diversos outros normativos, como a LAI, a política se segurança da informação e o PDTI do Senado Federal são instrumentos que ajudam a direcionar os esforços para o atendimento de soluções estratégicas do Senado Federal. A observância desses instrumentos terá grande influência sobre os resultados do mascaramento.

3 Resultados

Neste capítulo utilizamos o referencial teórico para tratar de maneira específica do problema de pesquisa. A partir da descrição das características do sistema de pessoal do Senado Federal e de sua arquitetura, foi feito um estudo para identificar a forma como a ferramenta adquirida pelo Senado deve ser utilizada para executar o mascaramento dos dados sensíveis. Para esta finalidade, foi elaborado um modelo de descaracterização para o sistema de pessoal e de um modelo genérico que pode ser utilizado em outros sistemas que possuem dados sensíveis.

3.1 Sistema de Pessoal do Senado Federal

O Sistema de Pessoal do Senado Federal, Ergon, foi adquirido junto à Techne. É um sistema de gestão de pessoas para o setor público que gera automaticamente a folha de pagamento mediante as informações da vida funcional. A interface do sistema foi desenvolvida em Oracle Forms, os relatórios em Oracle Reports e seus dados são armazenadas no Sistema Gerenciador de Banco de Dados – SGBD Oracle. Atualmente sua interface está sendo migrada para Java.

O acesso por meio da interface é destinado principalmente aos servidores lotados nos setores subordinados à Secretaria de Gestão de Pessoas – SEGP. O sistema possui diversos dados pessoais que só podem ser consultados ou alterados por servidores que possuem autorização específica. Essas permissões são concedidas por meio do módulo de controle de acesso, o que garante proteção contra acessos indevidos.

No entanto, como os dados estão armazenados no SGBD Oracle, é necessário adotar medidas de segurança para protegê-los fora do ambiente transacional. Atualmente os dados estão armazenados nas instâncias de produção, de desenvolvimento e de homologação. O acesso às informações na base de produção é bastante restrito, no entanto, os dados de desenvolvimento e de homologação precisam ser protegidos de forma mais efetiva, uma vez que são dados reais, copiados a partir da base de produção.

As bases de desenvolvimento e homologação são acessadas de diversas maneiras. A forma mais usual é através dos analistas do Senado responsáveis pela manutenção e customização do sistema. No entanto, existem diversas outras maneiras.

O Senado possui um contrato com a Techne destinado à prestação de serviços de suporte técnico, manutenção corretiva e manutenção evolutiva específica para o Senado Federal. O atendimento das solicitações feitas à Techne – destinados principalmente à atualização tecnológica, updates e upgrades – pode ser feito remotamente ou presencialmente.

Os consultores e analistas da empresa utilizam as bases de desenvolvimento e homologação da mesma forma que os analistas do Senado.

Outra forma de acesso é por meio das equipes de desenvolvimento da Central de Serviços do Senado Federal e dos sistemas que se integram ao Ergon. Estas equipes são compostas em sua maioria por analistas do Senado, por estagiários e por parceiros contratados.

Além das equipes acima mencionadas, o Senado possui um contrato de desenvolvimento baseado em uma fábrica de software. A empresa contratada para essa finalidade tem atuado de forma cada vez mais efetiva no desenvolvimento de novas funcionalidades para a Central de Serviços (interface utilizada por servidores responsáveis por atividades relacionadas à gestão de pessoas e pelos usuários finais). Segundo Maldonado e Blum (2018), um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios. Uma ameaça é uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização. Vulnerabilidade, por sua vez, é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência ou a fraqueza de uma proteção que pode ser explorada.

A partir dos três conceitos acima, identificamos que os dados armazenados nos ambientes de desenvolvimento e homologação representam um risco à integridade das informações pessoais. O mascaramento de dados é uma forma eficiente de mitigar este risco, pois evita a utilização indevida de dados pessoais dos servidores do Senado Federal. Após realizar entrevistas com todos os coordenadores da área de Gestão de Pessoas, evidenciou-se a necessidade de descaracterizar os dados pessoais sensíveis identificados nesta etapa.

3.2 Arquitetura do Sistema

O sistema de gestão de pessoas e folha de pagamento é direcionado para o setor público e foi desenvolvido pela empresa Techne. Ele adota o modelo relacional e suas informações são armazenadas e acessadas por meio do Sistema Gerenciador de Banco de Dados (SGBD) Oracle.

O sistema possui uma parte que atende as necessidades comuns a todas as instituições públicas e uma específica que pode ser parametrizada para contemplar as particularidades de cada órgão. Para tornar isso possível sua arquitetura contempla quatro esquemas, os quais estão segregados de acordo com a estrutura lógica de suas funcionalidades. Basicamente estão organizados da seguinte forma:

- HADES – agrega as funções básicas para o gerenciamento centralizado do ambiente, desempenhando todas as tarefas comuns a todos os módulos. É peça essencial e

obrigatória do sistema. Implementa diversas funcionalidades, tais como: controle de segurança e acesso às transações; manutenção de tabelas genéricas; manutenção do organograma da instituição;

- C_HADES – permite que as funcionalidades do HADES sejam adaptadas para a realidade do Senado Federal;

- ERGON – agrega funções que têm o objetivo de automatizar as atividades da gestão de pessoas, inclusive as que são voltadas ao processamento da folha de pagamento. É um módulo estratégico, uma vez que implementa todas as regras aplicadas ao setor público. Contempla as funcionalidades do negócio, dentre as quais se destacam: dados pessoais dos servidores; controle de dependentes e pensões alimentícias; cadastro de vantagens pessoais; controle de cargos e funções; controle de frequência; contagem do tempo de serviço; controle de férias, licenças e afastamentos;

- C_ERGON – permite agregar informações e regras específicas do Senado Federal às funcionalidades do esquema ERGON.

O banco de dados do sistema de gestão de pessoas está instanciado de forma similar nos ambientes de desenvolvimento, homologação e produção. A estrutura de informações é idêntica em todos eles e a grande maioria dos dados é replicada integralmente do ambiente de produção para os outros dois.

O modelo de descaracterização das informações deverá ser aplicado aos objetos dos esquemas "ERGON"e "C_ERGON", que contemplam a totalidade das informações pessoais.

3.3 Ferramenta de Descaracterização de Dados

O Senado Federal adquiriu a ferramenta CA Test Data Manager. A expectativa é que sua utilização permita a adequação dos ambientes de desenvolvimento e homologação aos níveis de segurança recomendados pelas normas técnicas mantendo a produtividade e eficiência das equipes de desenvolvimento.

Segundo informações de seu fornecedor, CA Technologies (2019), o CA Test Data Manager possui diversas funcionalidades que podem ajudar a melhorar o ambiente de testes. A primeira delas, o provisionamento, tem o objetivo de refinar os dados para gerar informações bem definidas, com dados normalizados que podem ser compreendidos e gerenciados facilmente. A seguir, é destacada a capacidade de a ferramenta criar um rol de informações conciso que abrange todos os casos de testes. Outra importante característica é a possibilidade de a ferramenta criar uma base direcionada para os testes, levando em consideração os requisitos e os casos de testes.

Apesar de não descartar as funcionalidades mencionadas acima, no estudo em questão, vamos enfatizar uma outra que é sua capacidade de tratar os dados sensíveis. Um dos principais desafios encontrados no gerenciamento dos dados de teste é a adoção uma estratégia para lidar com esses dados. É bastante comum encontrarmos situações em que dados privados e informações sensíveis são mantidas sem nenhuma forma de proteção nos ambientes de desenvolvimento. Essa situação representa uma grande vulnerabilidade, uma vez que esses dados podem, por exemplo, ser comercializados no ciclo de testes sem que a organização se dê conta disso.

Dados copiados de um ambiente para outro podem conter informações sensíveis, especialmente quando esta cópia se origina dos dados de produção. Uma solução de proteção adequada deve partir da identificação desses dados. Após essa etapa, é possível definir as regras de mascaramento e aplicá-las aos dados. Essa técnica elimina riscos de vazamento, pois cria dados semelhantes aos de produção, mas que não contêm informações sensíveis (Figura 1).

Figura 1 – Mascaramento – Visão Geral

A base de desenvolvimento do sistema de folha de pagamento e pessoal, assim como alguns outros, necessita ser atualizada com bastante frequência para que os testes considerem a situação real. Para que o procedimento de mascaramento seja viável, é necessário automatizá-lo. O primeiro passo nesse sentido é elaborar um modelo que possa ser atualizado rapidamente, preferencialmente através de um processo automático que pode ser executado periodicamente.

3.4 Procedimentos para executar o mascaramento

Embora o enfoque deste estudo esteja no mascaramento, a ferramenta que o Senado dispõe exige que a primeira etapa seja o provisionamento das informações. Esse procedimento tem o objetivo de varrer os dados, fazer uma análise dos mesmos e extrair seus atributos. Após sua execução, os dados de teste são organizados e catalogados no repositório. É importante observar que não são os dados em si que são copiados. Apenas os metadados ou características dos esquemas e tabelas são extraídos.

Nessa etapa os dados provisionados são analisados. A ferramenta possui uma finalidade destinada a fazer uma identificação prévia dos dados pessoais sensíveis. Ela pode ser bastante útil para situações que o Prodasen necessite dar início ao processo de mascaramento. No entanto, por se tratar de uma ferramenta auxiliar, é importante submeter os resultados obtidos ao proprietário da informação para que seja feita uma revisão e validação dos mesmos.

Existem diversos métodos que podem ser utilizados no mascaramento. No provisionamento são definidas as regras de que devem ser aplicadas aos dados. Esse procedimento pode ser efetuado após a cópia dos dados para o local de destino ou durante o processo de cópia.

Em seguida, quando o dado é mascarado, o repositório armazena o metadado e versiona a ação.

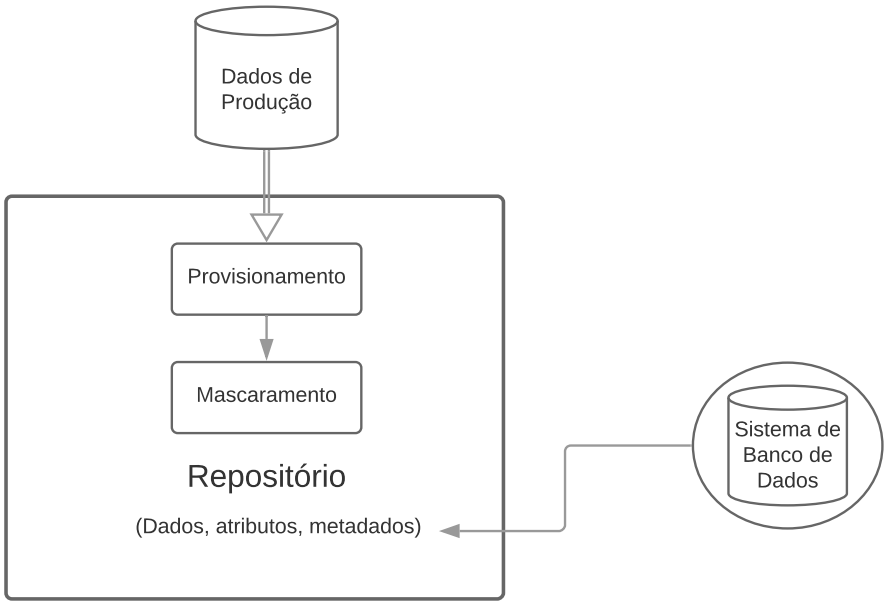

Figura 2 – Mascaramento – Repositório

No modelo apesentado na Figura 2, após os dados serem provisionados, é possível filtrá-los e defini-los como sensíveis. No mascaramento, os dados sensíveis são substituídos

por dados fictícios, evitando assim a exposição dos dados reais. Os dados mascarados são obtidos a partir de uma biblioteca com dados semelhantes aos reais, ou podem ser gerados por *scripts* que utilizam funções de embaralhamento ou de substituição. É possível executar as funções de mascaramento a partir do banco de origem ou criar uma cópia mascarada.

O repositório é um metadado de gerenciamento usado para armazenar critérios de teste reutilizáveis, regras para criar casos de teste e reserva de dados de teste. Esse gerenciamento compreende as seguintes atividades:

1. Os testes são importados para um local central;
2. As equipes compartilham e reusam casos de teste;
3. Usuários podem reservar dados para evitar que estes sejam destruídos por outros cenários;
4. Múltiplas versões são mantidas pelo sistema ao mesmo tempo. A versão é atualizada quando a estrutura de dados é alterada;
5. Mudanças de dados são versionadas, garantindo que os testes são aplicáveis a todas as fases. Informações estatísticas, exemplos de dados e características dos dados também são armazenadas no repositório.

A ferramenta CA Test Data Manager organiza os procedimentos em uma estrutura hierárquica composta pelos objetos que são armazenados no repositório. Cada modelo de teste dá origem a um projeto.

3.5 Modelo de Descaracterização para o Sistema de Pessoal

O modelo de descaracterização se baseia no fluxo descrito na Figura 3.

O primeiro passo para executar o mascaramento é identificar os dados pessoais sensíveis. No estudo em questão, foram realizadas entrevistas com todos os coordenadores da SEGP, englobando as áreas de Administração de Pessoal, de Pagamento e de Benefícios Previdenciários. As informações obtidas nesta etapa permitiram o mapeamento das mesmas nas diversas tabelas do Sistema de Pessoal.

A partir daí, cabe à Comissão de Acesso ratificar as informações para que o Prodasen dê início aos procedimentos técnicos. Nessa fase, a equipe responsável pela administração de banco de dados extrai os dados de produção e cria uma base temporária denominada *Golden Copy*. Os dados sensíveis são incluídos no mapa de transformação de cada uma

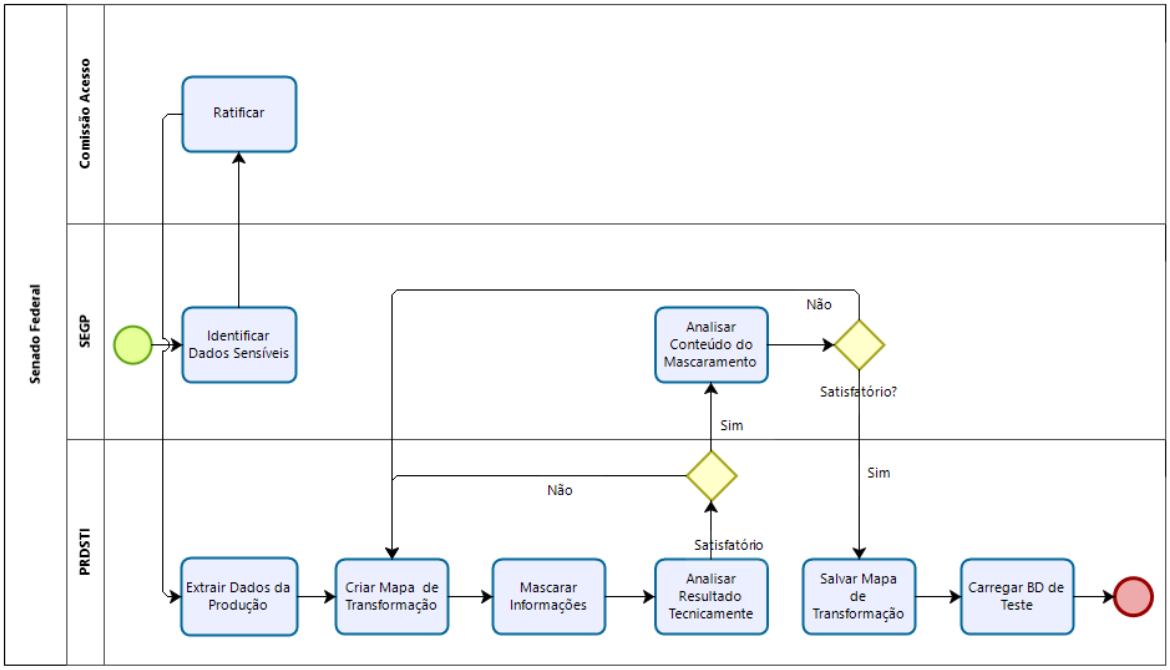

Figura 3 – Modelo de Descaracterização do Sistema de Pessoal

dessas tabelas. Esse é um processo bastante trabalhoso porque deve ser aplicada uma regra de transformação para cada campo.

Antes de executar o mascaramento, é possível executar a rotina no modo de simulação para verificar o resultado. Esse procedimento é importante para evitar a geração de dados mascarados com erro. Os resultados são analisados tecnicamente e, caso não sejam encontrados problemas nesse procedimento, são encaminhados para a Secretaria de Gestão de Pessoas validar as informações.

Após essa etapa, a equipe técnica salva o mapa de transformação que é a base do modelo de transformação. Esse mapa permite que as regras de transformação possam ser aplicadas de forma automatizada todas as vezes que as bases de desenvolvimento e homologação forem atualizadas.

3.6 Modelo de Descaracterização para Sistemas com Informações Sensíveis no Senado Federal

Além do sistema de pessoal, existem alguns outros que possuem informações sensíveis. O modelo proposto a seguir é bastante flexível, podendo servir de base para todos os demais.

O diagrama apresentado na Figura 4 descreve o modelo genérico de mascaramento de informações dos sistemas do Senado Federal. Este modelo foi criado a partir do que foi

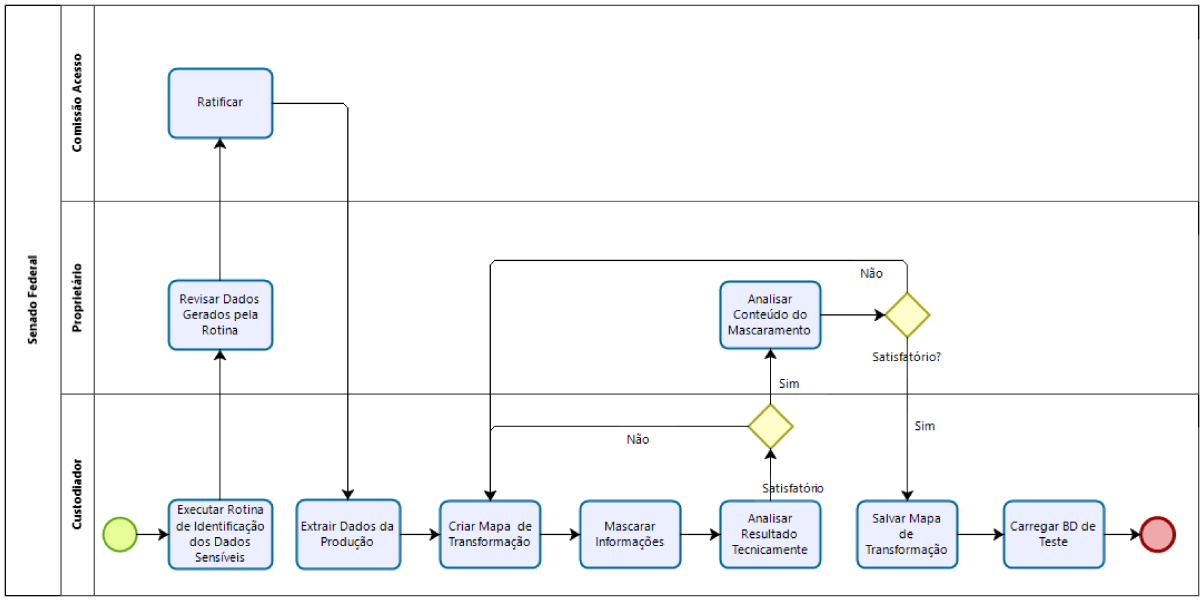

Figura 4 – Modelo de Descaracterização para Sistemas do Senado Federal

elaborado para o sistema de pessoal.

A questão inicial referente à definição do novo modelo envolve a decisão sobre o seu ponto de partida. Apesar de ser possível atribuir ao proprietário da informação essa responsabilidade, sugerimos que essa etapa seja executada pelo custodiador das informações. Entendemos que essa forma de implementação é factível, uma vez que, de acordo com o Regulamento Administrativo do Senado Federal, cabe ao Prodasen, dentre outras atribuições, prover, serviços e soluções, bem como implementar a estratégia de tecnologia da informação. Além disso, como a ferramenta de mascaramento de dados está sob responsabilidade do Prodasen e a mesma possui uma funcionalidade que permite a identificação das informações sensíveis a partir do banco de dados, essa estratégia pode agilizar o processo de proteção das informações sensíveis do Senado Federal. Essa ferramenta pode ser utilizada pela área de TI, uma vez que não exige conhecimento detalhado acerca do conteúdo armazenado. O resultado obtido nessa etapa serve de base para que o proprietário da informação faça uma revisão mais acurada.

Após esta revisão, cabe à Comissão de Acesso ratificar as informações para que o Prodasen dê continuidade aos procedimentos técnicos. Nessa fase, a equipe responsável pela administração de banco de dados extrai os dados de produção e cria uma base temporária denominada *Golden Copy*. Os dados sensíveis são incluídos no mapa de transformação de cada uma dessas tabelas.

Conforme foi mencionado no modelo anterior, antes de executar o mascaramento, é possível executar a rotina no modo de simulação para verificar o resultado e evitar a geração de dados mascarados com erro. Os resultados são analisados tecnicamente e, caso não sejam encontrados problemas nesse procedimento, são encaminhados para o

proprietário das informações validá-las.

Após essa etapa, a equipe técnica salva o mapa de transformação que é a base do modelo de transformação. Esse mapa permite que as regras de transformação possam ser aplicadas de forma automatizada todas as vezes que as bases de desenvolvimento e homologação forem atualizadas.

3.7 Conclusão do Capítulo

O sistema de Pessoal do Senado Federal possui diversos dados pessoais sensíveis. Atualmente suas bases de desenvolvimento e homologação, compostas de dados reais de produção, podem ser acessadas por equipes de desenvolvedores do próprio sistema e de outros sistemas que estão integrados a ele. No rol de pessoas que podem ter acesso a essas informações temos analistas e estagiários do Senado, consultores da empresa que desenvolveu o sistema de pessoal e funcionários da fabrica de software.

Para tratar essa questão de forma eficaz sem prejudicar a produtividade das equipes de desenvolvimento, o estudo analisou detalhes inerentes ao sistema de pessoal do Senado Federal que subsidiaram a elaboração de um modelo de descaracterização dos dados pessoais sensíveis. Esse estudo levou em consideração a arquitetura e as características do sistema, bem como as funcionalidades da ferramenta de mascaramento de dados que o Senado adquiriu recentemente.

As informações obtidas permitiram a elaboração de um modelo de descaracterização para o sistema de pessoal e sua extrapolação para um modelo genérico que pode ser aplicado a outros sistemas que possuem dados pessoais sensíveis.

4 Conclusão

A informação é um ativo extremamente valioso para as organizações atuais. O desenvolvimento da tecnologia da informação e das comunicações transformou sensivelmente a forma como elas realizam seus negócios. A utilização da Internet para realizar suas transações quebra barreiras físicas e abre espaço para um mercado global que é alimentado pela informação. Este mercado é tão abrangente, que muitas vezes envolve pessoas que nem ao menos têm conhecimento sobre a destinação das informações que elas fornecem.

As organizações públicas, apesar de não auferirem lucro com transações comerciais, também precisam gerir suas informações de maneira adequada. A demanda dos cidadãos por serviços informatizados levou a grande maioria delas a utilizar a Internet de forma cada vez mais abrangente em suas relações com os cidadãos. Em decorrência desse processo, a preocupação com a segurança da informação cresceu significativamente. Na tentativa de conter ataques de origem externa, muitos investimentos são direcionados para a proteção dos dados armazenados nos sistemas que estão em produção.

Observa-se, no entanto, que diversos sistemas voltados para organizações públicas são desenvolvidos internamente, o que leva à necessidade da criação de bases de dados de desenvolvimento e homologação. Consoante com esse modelo, o Senado Federal utiliza esses ambientes para devolver suas aplicações. Atualmente a cópia integral dos dados de produção tem sido uma alternativa para prover dados para esses ambientes.

Apesar dessa solução ser bastante satisfatória para as equipes de desenvolvimento, ela cria alguns riscos relacionados à segurança da informação, cujos pilares estão centrados na confidencialidade, integridade e disponibilidade. De acordo com o primeiro desses princípios, a confidencialidade, as informações devem ser utilizadas apenas pelos que necessitam dela para a realização de suas atividades profissionais na organização. Dessa forma, os dados utilizados nesses ambientes devem ser realistas, mas não podem ser reais.

Este estudo foi direcionado para a elaboração de um modelo que trata dos riscos inerentes a essa vulnerabilidade. Foi revisada a legislação e os normativos pertinentes ao tema, bem como os normativos específicos do Senado Federal. O Plano Diretor de Tecnologia da Informação, havia incluído projetos voltados para o tratamento dos riscos de TI e definiu a aquisição de uma solução para proteção de banco de dados como uma de suas prioridades. Essa ferramenta é essencial para mitigar riscos relacionados à segurança da informação nos ambientes de desenvolvimento e homologação e demonstra a relevância desta pesquisa.

Verificamos portanto que a proteção dos dados pessoais é um tema de importância estratégica para o Senado Federal. Neste trabalho o estudo de caso do sistema de pessoal

foi utilizado como base para o modelo de descaracterização das informações sensíveis nos ambientes de desenvolvimento e homologação. Este modelo, pautado nas técnicas de mascaramento de dados, está em conformidade com a ferramenta que o Senado Federal adquiriu recentemente, o que torna sua aplicação bastante factível.

Para chegar a esta conclusão, pesquisou-se a respeito das técnicas de mascaramento de dados e rememorou-se as normas técnicas ligadas à segurança da informação. A partir da definição das informações sensíveis e da análise do relacionamento entre essas informações, foi elaborado um fluxo de informações específico para o sistema de pessoal. Este fluxo serviu de base para a elaboração de um outro mais abrangente que pode ser adaptado para todos os sistemas do Senado Federal que possuem dados sensíveis em suas bases.

Por se tratar do primeiro projeto do Senado Federal relacionado ao mascaramento de dados, é recomendável que após sua implantação sejam criados mecanismos para otimizar os resultados. Uma proposta nesse sentido poderá dar origem a um projeto pautado na definição de métricas e na realização de testes no ambiente, o que poderia ajudar a implementar melhorias.

Referências

Advisera Expert Solutions Ltd. *What is EU GDPR and how can ISO 27001 help*. 2019.

AJAYI, O. O.; ADEBIYI, T. O. Application of data masking in achieving information privacy. 2014.

BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. [S.l.]: Editora Forense Ltda, 2019.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado, 1988.

BRASIL. *LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011*. Brasília, DF, 2011.

BRASIL. *Decreto Nº 9.637, de 26 de dezembro de 2018*. Brasília, DF: Presidência da República, 2018.

BRASIL. *LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF, 2018.

BRASIL. Congresso. Senado. *Ato da Comissão Diretora nº 9 de 2012*. 2012.

BRASIL. Congresso. Senado. *Plano Diretor de Tecnologia da Informação*. 2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018 : versão 1.0*. 2015.

BRASIL. Tribunal de Contas da União. *Boas práticas em segurança da informação*. [S.l.]: TCU, 2012.

CA Technologies. *CA Test Data Manager 4.4 : Foundations 200*. [S.l.: s.n.], 2019.

FERNANDES, J. H. C. *Gestão da segurança da informação e comunicações : volume 1*. [S.l.]: Editora da Faculdade de Ciência da Informação da Universidade de Brasília, 2010.

FONTES, E. L. G. *Segurança da Informação: o usuário faz a diferença*. [S.l.]: Saraiva, 2006.

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL. *ISO/IEC 27000:Information technology — Security techniques — Code of practice for information security management*. 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL. *ISO/IEC 27000:Information technology — Security techniques — Information security management systems*. 2014.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. 2005.

MACHADO, M. J. *Segurança no Desenvolvimento de Sistemas*. 2012. Disponível em: <https://marceljm.com/seguranca-da-informacao/seguranca-no-desenvolvimento-de-sistemas/>.

MALDONADO, V. N.; BLUM, R. O. *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. [S.l.]: Thomson Reuters - Revista dos Tribunais, 2018.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. del P. B. *Metodologia de Pesquisa*. [S.l.]: Mc Graw Hill, 2013.

WERTHEIN, J. A sociedade da informação e seus desafios. 2000.

YIN, R. K. *Estudo de caso: planejamento e métodos*. [S.l.]: Bookman, 2005.