# PROTEÇÃO DE CONHECIMENTO RELACIONADO AO DESENVOLVIMENTO DE SOFTWARE EM ORGANIZAÇÃO PÚBLICA

***Abstract.*** *The objective of this article is to identify the knowledge that requires protection in the process of software development, in a public information technology organization. The research adopted the Case Study strategy, descriptive purpose and level of organizational analysis. For data collection, a documental analysis and interviews were carried out. The results point out the knowledge that requires protection and the protected knowledge assets. The research contributes to a better understanding of "what" to protect in the provision of public services in the area of information technology.*

***Keywords:*** *knowledge protection; knowledge sharing; knowledge management; software development process; information technology.*

***Resumo.*** *O objetivo deste artigo é identificar os conhecimentos que requerem proteção no processo de desenvolvimento de software, em uma organização pública de tecnologia da informação (TI). A pesquisa adotou a estratégia de Estudo de Caso, finalidade descritiva e nível de análise organizacional. Para a coleta de dados foi feita análise documental e realizadas entrevistas. Os resultados apontam os conhecimentos que requerem proteção e os ativos de conhecimento protegidos. A pesquisa contribui para a melhor compreensão de "o que" proteger na prestação de serviços públicos na área de tecnologia da informação.*

***Palavras-Chave:*** *proteção de conhecimento; compartilhamento de conhecimento; gestão do conhecimento; processo de desenvolvimento de software;tecnologia da informação.*

# 1 INTRODUÇÃO

A respeito das capacidades de proteção dos conhecimentos valiosos relativamente pouco se sabe (Faria & Sofka, 2010). A necessidade de rever os processos sobre como avaliar o conhecimento, qual conhecimento deve ser classificado como propriedade intelectual e o valor do conhecimento identificado é apontado por Little (2011). Estudos qualitativos e quantitativos são necessários para desvendar a interação entre o tamanho da empresa, inovação e o dilema do compartilhamento e proteção de conhecimento (Olander, Hurmelinna-Laukkanen & Mahonen, 2009). Pesquisas indicam que é importante o uso de forma eficiente da proteção de conhecimento. Novas pesquisas podem revelar mais detalhes sobre este fenômeno ao oferecer aos gestores meios de proteção de conhecimento para a inovação relacionada à colaboração (Hurmelinna-Laukkanen, 2011). Assim, as lacunas apontadas pela literatura científica indicam a importância do assunto proteção de conhecimento entre acadêmicos e profissionais.

Quanto à distinção entre organizações públicas e organizações privadas, Heisig (2009) aborda, em estudo de abrangência global, 160 *frameworks* sobre gestão do conhecimento a partir de dados de empresas industriais e organizações públicas, sem mencionar qualquer diferenciação. O autor afirma que a gestão do conhecimento é influenciada por elementos fundamentais: cultura, organização e papéis, estratégia e liderança, habilidades e motivação, controle e medição, e tecnologia da informação. E, em seu artigo, nota-se que a proteção do conhecimento pouco se evidencia em organizações públicas.

É suscitada a observação de que nem sempre está claro, para empregados de empresa de tecnologia da informação, conhecimento que pode ser compartilhado daquele que deve ser protegido no trabalho diário, em especial na engenharia de *software*, uma disciplina de engenharia relacionada a todos os aspectos de produção de software. Sommerville (2007) aborda as preocupações quanto à engenharia da proteção em tecnologias emergentes. Trata o que se refere à proteção de aplicações e proteção de infraestrutura. A proteção de aplicações é um problema dos engenheiros de *software*, que devem assegurar que o sistema esteja projetado para resistir a ataques, enquanto a proteção de infraestrutura é um problema dos gerentes de sistemas, que devem assegurar que a infraestrutura esteja configurada para resistir aos ataques. Isto significa tratar das vulnerabilidades quando o *software* é utilizado e a necessidade de atividades que envolvem usuários e permissões, monitoração de *software*, detecção e recuperação de ataques. Este tipo de proteção trata das ameaças a um *software*

quanto à confidencialidade (acesso não autorizado), integridade (dano aos dados) e disponibilidade (restrição ao acesso), elementos pertinentes à segurança da informação (Sommerville, 2007). Contudo, esta abordagem não trata da proteção de conhecimento em si, dos processos não tecnológicos relacionados ao conhecimento pertinente ao negócio de um cliente, que demanda uma solução tecnológica, resultante de um processo de desenvolvimento de *software*.

Nesse contexto, este artigo tem por objetivo identificar os conhecimentos que requerem proteção no processo de desenvolvimento de *software*, em uma organização pública de tecnologia da informação (TI). A adequada compreensão faculta a adoção ou revisão de políticas e mecanismos pertinentes. A ausência destas possibilidades representa implicações desfavoráveis a um apropriado ambiente colaborativo de tecnologia da informação.

## 2 SOBRE PROTEÇÃO DE CONHECIMENTO

Estudos sobre proteção de conhecimento envolvem o compartilhamento e elementos associados à inovação (Olander, Hurmelinna-Laukkanen & Mahonen, 2009; Hurmelinna-Laukkanen, 2011; Bogers, 2011). Razões para a escolha entre o compartilhamento de conhecimento e proteção, ou combiná-los, são difíceis para pequenas e médias empresas (PMEs) e caracterizam um dilema para as atividades de inovação (Olander, Hurmelinna-Laukkanen & Mahonen, 2009). Em resumo, a criação de valor e de captura exige que as empresas escolham entre o compartilhamento de conhecimento e a proteção, ou tentem encontrar alguma maneira de incorporar as duas alternativas. O Quadro 1 ilustra a necessidade de encontrar o equilíbrio para o dilema em inovação.

Quadro 1 – Compartilhamento de conhecimento versus proteção de conhecimento – dilema da inovação

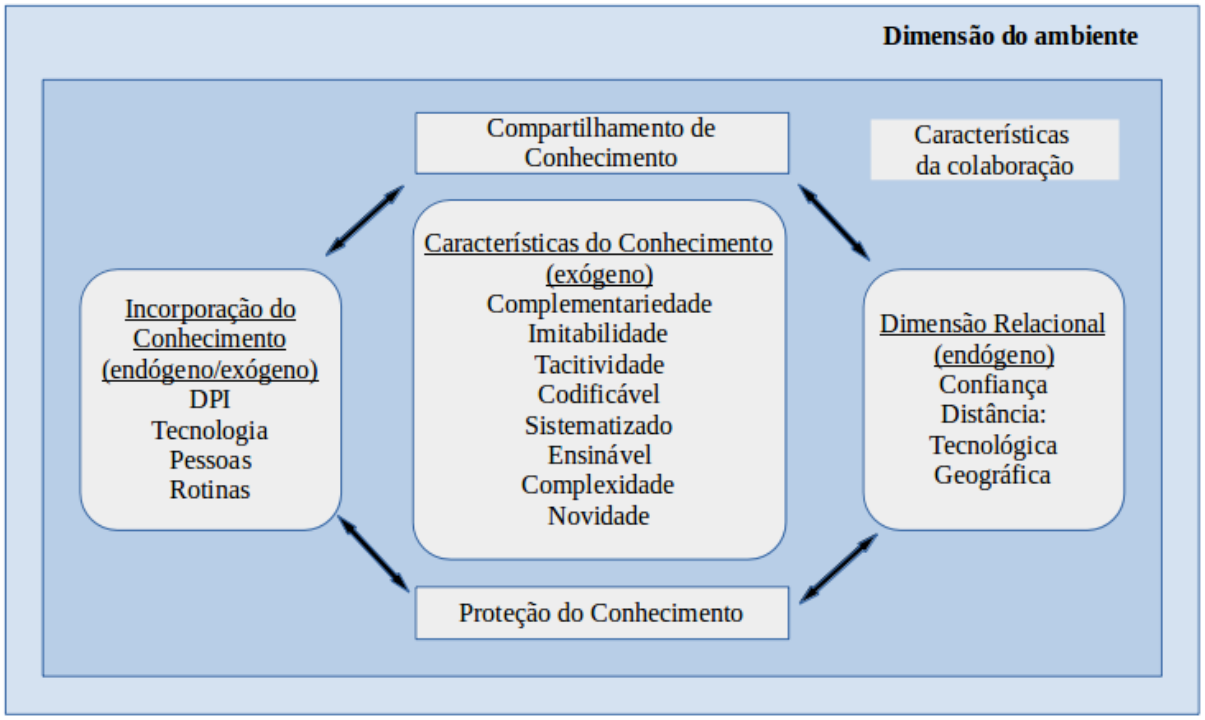
| | Valor e Criação de Inovação | Capturar e Lucrar Valor com a Inovação |
|---|---|---|
| Compartilhamento de conhecimento | Necessário para a criação de novas combinações e ideias inovadoras; pode causar perda de ativos de conhecimento essenciais para os rivais. | Necessário para obter acesso a mercados; pode causar perda de vantagem competitiva. |
| Proteção de conhecimento | Necessário para divulgação segura de conhecimento existente; pode impedir adequado fluxo de conhecimento. | Necessário para proteger os investimentos em inovação, necessário para a divulgação seguro; pode causar difusão mais lenta da inovação. |

Fonte: adaptado de Olander, Hurmelinna-Laukkanen & Mahonen (2009)

A proteção da produção de inovação que as empresas podem ganhar é menos importante que o conhecimento de base que precisam proteger para compartilhar (Hurmelinna-Laukkanen, 2011). O uso estratégico de mecanismos de proteção de conhecimento melhora o compartilhamento de conhecimento e de inovação. Quando uma empresa faz esforço no sentido de obter forte proteção, o compartilhamento de conhecimento com diferentes parceiros melhora o desempenho de inovação da empresa (uso da proteção de conhecimento de forma eficiente). As correlações do estudo sugerem que a proteção de conhecimento e compartilhamento estão positivamente relacionados ao desempenho da inovação, e que também existe uma relação positiva entre compartilhamento de conhecimento e proteção. Os resultados da análise de regressão apontam que a proteção de conhecimento tem efeito sobre o desempenho da inovação (Hurmelinna-Laukkanen 2011).

Um paradoxo surge quando empresas compartilham e protegem, simultaneamente, seus conhecimentos em alianças com outras organizações, o que requer estratégias para tratar esta tensão no processo de inovação aberta (Bogers, 2011). Este tipo específico de inovação aberta – a colaboração de pesquisa e desenvolvimento (P & D) – utiliza entradas e saídas de conhecimento de parceiros que colaboram. Um modelo da área de tensão do compartilhamento e proteção de conhecimento é desenvolvido, conforme Figura 1.

Figura 1 – Área de tensão do compartilhamento de conhecimento e de proteção




Fonte: adaptado de Bogers (2011)

Com foco na proteção de conhecimento, Norman (2001) afirma que empresas protegem seus conhecimentos essenciais a partir da gestão da alta direção, identificam as capacidades essenciais e sua proteção, e administram seus fluxos de informação. Nas relações entre proteção de conhecimento e propriedade intelectual observa-se a abrangência do capital intelectual e inovação. O capital intelectual é comumente associado aos ativos intelectuais ou ativos de conhecimento de uma organização (Olander, Hurmelinna-Laukkanen & Mahonen, 2009; Little, 2011). A proteção de ativos intelectuais está relacionada ao capital humano e às inovações nas fases das atividades e processos (Olander, Hurmelinna-Laukkanen & Mahonen, 2009). É preciso decidir sobre como proteger o capital intelectual identificado (Little, 2011). É importante evitar a perda de conhecimento da empresa (Ilvonen, 2013).

Observa-se então que a proteção e o compartilhamento de conhecimento são assuntos relacionados entre si, envolvem inovação, e são inerentes às organizações intensivas em conhecimento.

## 3 MÉTODO ADOTADO

Esta pesquisa adota a estratégia de Estudo de Caso (Yin, 2010) com finalidade descritiva sendo a unidade de análise um processo e o nível de análise organizacional. Na definição de termos considera-se o conhecimento realizado pelo indivíduo que também se expressa na regularidade pela qual os membros cooperam em uma comunidade social. Para a proteção de conhecimento foi selecionada a definição de Lin (2007) que considera os processos de aquisição, conversão, aplicação e proteção de conhecimento e envolve organizações de tecnologia da informação. Por isso foi considerada adequada para embasar esta pesquisa. Lin (2007) estabelece que proteção de conhecimento é a capacidade de proteger o conhecimento organizacional do uso ilegal, ou impróprio ou roubo. Por sua vez, entende-se por *software* o conjunto que compreende programa de computador, descrição do programa e material de apoio, também comumente denominado sistema ou solução tecnológica.

A organização pesquisada foi uma empresa pública de tecnologia da informação, o Serviço Federal de Processamento de Dados – SERPRO, vinculado ao Ministério da Fazenda. A empresa atende a administração pública em nível federal, estadual e municipal para a modernização da gestão pública em benefício do cidadão brasileiro. A empresa está distribuída geograficamente pelo país, possui sede localizada em Brasília, 11 regionais, e

escritórios. As soluções tecnológicas desenvolvidas buscam controle e transparência sobre a receita e os gastos públicos (SERPRO, 2013).

O *software* selecionado para a pesquisa trata do assunto "administração financeira" que visa a gestão orçamentária e financeira do país. A versão inicial lançada em 1987 tornou disponível serviços para os gestores públicos e passou a ser referência internacional como ferramenta de controle dos recursos públicos. Em 2009 um novo pólo de desenvolvimento de *software* foi criado na cidade de Florianópolis/SC para desenvolver uma versão renovada desse sistema. A empresa expandiu parcerias com universidades no campo de desenvolvimento de código aberto e em certificação digital. Em 2012 colocou em operação o novo sistema (SERPRO, 2013).

Para a investigação empírica deste Estudo de Caso participaram 15 empregados com função gerencial e não gerencial, do nível estratégico e do tático-operacional, localizados em Brasília/DF, na sede da empresa, e na regional Florianópolis/SC. Na linha hierárquica, os empregados do nível estratégico são responsáveis pela negociação e orientação do desenvolvimento de *software*, enquanto os do nível tático-operacional são responsáveis por coordenar e desenvolver o projeto do *software*.

Para a coleta de dados foi feita análise documental (roteiro) e entrevista (roteiro semiestruturado), cujos instrumentos foram revisados por especialistas que fizeram análise semântica e apontaram ajustes para a coerência dos instrumentos. A análise documental explorou documentos formais de instituição e apoio aos mecanismos de proteção de conhecimento e compartilhamento de conhecimento. Para tanto, o roteiro levantou documentos organizacionais (políticas e normas), tipo de documento (breve descrição, vigência, palavras-chave) e comentários. A entrevista explorou aspectos relacionados ao conhecimento. Para essa abordagem foram feitas as seguintes perguntas: Quais são os principais conhecimentos que devem ser protegidos neste processo de desenvolvimento de software? São conhecimentos explícitos ou tácitos? Porque devem ser protegidos? As respostas foram organizadas em planilhas sendo a análise norteada pelo propósito do estudo.

No sentido de garantir a qualidade foram tomadas medidas usuais dos métodos da ciência social – a validade e a confiabilidade (Yin, 2010). Foram dedicados cuidados à validade de construto e à validade das fontes. A confiabilidade foi buscada pelo uso de fontes fidedignas, consultados documentos institucionais na intranet e na *internet* da empresa. Também colaborou para a confiabilidade a elaboração dos passos para a aplicação dos instrumentos e a consequente construção de uma base de dados para a análise dos dados

coletados, importante para pesquisa desta natureza. A triangulação das fontes de evidências foi realizada cruzando-se os dados coletados. Logo, as descrições das interpretações buscaram revelar os achados e atender ao objetivo estabelecido.

## 4 CONHECIMENTOS QUE DEVEM SER PROTEGIDOS NO DESENVOLVIMENTO DE SOFTWARE

Os conhecimentos identificados fazem parte do processo de desenvolvimento de *software*, influenciado pelo método de trabalho (Método Ágil) adotado. A análise das respostas das entrevistas revela dados sobre os conhecimentos envolvidos no processo de desenvolvimento de *software* e alguns aspectos relevantes. A maioria dos respondentes (93%) afirma que existem na empresa documentos que abordam a proteção e o compartilhamento de conhecimento. Alguns respondentes (33%) apontam que existem facilidades e dificuldades na proteção de conhecimento, embora outros (20%) apontem apenas dificuldades. No compartilhamento de conhecimento a maioria dos respondentes (73%) afirma que existem facilidades e dificuldades, enquanto uma parcela (14%) aponta apenas facilidades. Nota-se que o compartilhamento de conhecimento apresenta mais facilidades, enquanto a proteção de conhecimento apresenta mais dificuldades. Pode-se depreender que o compartilhamento de conhecimento é mais evidente na empresa e a proteção de conhecimento um assunto a ser mais tratado.

As entrevistas possibilitaram a identificação dos conhecimentos que requerem proteção na empresa. Observa-se que a maioria dos respondentes (88%) do nível estratégico e alguns (29%) do nível tático-operacional citam conhecimentos de forma explícita. O Quadro 2 mostra em detalhes os conhecimentos identificados.

O nível estratégico aponta conhecimentos e respectivos esclarecimentos que confirmam argumentos de Norman (2001) sobre empresas que protegem seus conhecimentos essenciais a partir da gestão da alta direção, que envolve identificação das capacidades essenciais e sua proteção, além da identificação do conhecimento que pode ser compartilhado.

Os relatos revelam a visão restrita do nível tático-operacional sobre o conhecimento utilizado, ou seja, mais focada no processo de desenvolvimento de *software*, enquanto o nível estratégico tem visão mais abrangente, que envolve a área de negócio – clientes e fornecedores. No nível tático-operacional também se nota que o conhecimento é percebido pelos empregados quanto às características de conhecimento tácito e explícito apontados por

Nonaka e Takeuchi (1997); e principalmente o conhecimento "inacessível" e "acessível", aquele utilizado por meio de senhas de acesso permitido. Desta maneira, os esclarecimentos do nível tático-operacional confirmam argumentos de Norman (2001) quanto aos fluxos de informação e aos conhecimentos limitados, neste Estudo de Caso, pois somente a equipe responsável pelo desenvolvimento de *software* tem acesso ao ambiente de desenvolvimento.

Quadro 2 – Conhecimentos (explícitos ou tácitos) detalhados que devem ser protegidos na empresa estudada.

| Conhecimentos detalhados do processo de desenvolvimento de *software* (por nível organizacional) | |
|---|---|
| Nível estratégico | Nível Tático-operacional |
| • Conhecimento do negócio envolvido porque é do cliente, estão explicitados em documentos, inclusive contratos.<br>• Arquitetura de solução para não mostrar as vulnerabilidades que possam permitir ataques.<br>• Regras de negócio e o código fonte (regras de negócio implementadas) embora seja o cliente que decide se é sigilo.<br>• Documentos das regras de negócio.<br>• Código fonte armazenado e versionado.<br>• Documentos gerados pelo processo de desenvolvimento de *software*.<br>• Requisitos, modelo de dados, topologia de hardware, configuração de *software*, devem ser classificados como privado, a não ser que sejam liberados com anuência do cliente.<br>• Arranjos que se faz com a tecnologia por ser o diferencial com os concorrentes.<br>• Conhecimento tácito e explícito sobre os clientes.<br>• Negócio do cliente em contrato, inclusive cláusula específica de sigilo, periodicidade de guarda, segurança da informação dentro da empresa, níveis de serviço, capacidade de recuperação, dentre outros.<br>• Informações do cliente, estruturas estratégicas, códigos, dispositivos de segurança. | • Regras de negócios que são de segurança, como algoritmos e criptografia de senha do sistema que controla o acesso ao sistema do cliente, e subsistema que controla o acesso do cliente.<br>• Código fonte é restrito aos desenvolvedores.<br>• Dados dos sistemas.<br>• Dados trafegados.<br>• Arquitetura e infraestrutura.<br>• Determinadas tecnologias que são usadas não são divulgadas, apesar de não precisarem de proteção.<br>• Informações do cliente são reservadas, cliente é que informa o que deve ser aberto ou não.<br>• Conhecimento de negócio, casos de uso e requisitos de negócio. |

Fonte: Dados da pesquisa

Adicionalmente, a análise documental mostra evidências de que a confidencialidade é garantida por norma da empresa, denominada RC-002 Contrato de Receita, a qual determina que a proposta comercial para os clientes deva estabelecer condições que contemplem os requisitos de segurança e sigilo, de propriedade intelectual e direito autoral, que também garante a proteção de conhecimento legal. A privacidade dos dados também é garantida por norma, TC-002 Licenciamento de *software* livre, que determina que as soluções disponíveis para a sociedade devam considerar a privacidade dos dados dos cidadãos, a segurança dos dados sigilosos e informações de negócio. O compartilhamento e proteção de conhecimento na empresa também são orientados por norma, SG-005 Classificação dos ativos de informação do SERPRO, que adota graus de sigilo. Os documentos que não estiverem

classificados são passíveis de divulgação para fora da empresa. A análise documental também ratifica os relatos dos entrevistados ao demonstrar que as informações do processo de desenvolvimento de *software* estão disponíveis na intranet da empresa para acesso de qualquer equipe, entretanto, os códigos fontes somente podem ser acessados pela equipe cujos desenvolvedores estão dedicados às tarefas do *software* pesquisado.

Desse modo foram identificados os conhecimentos detalhados do processo de desenvolvimento de *software*. No sentido de organizá-los foi feita análise dos termos quanto ao significado e constatou-se que se trata de ativos de conhecimento, pois envolvem um conjunto de dados e informações que agregam valor ao processo na empresa. Ativos de conhecimento segundo Desouza (2007) são conhecimentos que residem na mente dos empregados, estão embutidos nos produtos e serviços, nas redes internas e externas da organização, o que oferece vantagens competitivas e diferenciais perante seus competidores. Os ativos de conhecimentos encontrados são apresentados na próxima seção.

## 5 ATIVOS DE CONHECIMENTO PROTEGIDOS NO DESENVOLVIMENTO DE SOFTWARE

Neste Estudo de Caso observa-se que o conhecimento é tratado desde o contrato com o cliente (antes do início do processo de desenvolvimento de *software*) até a entrega do *software*, o que corrobora Liu e Wang (2011), quando afirmam que organizações de tecnologia da informação são intensivas em conhecimento.

Os conhecimentos identificados se caracterizam por ativos de conhecimento (Desouza, 2007) por agregarem valor ao processo na empresa. A identificação dos ativos de conhecimentos contribui para o melhor entendimento e o aperfeiçoamento das orientações da empresa aos empregados de modo a permitir mais tranquilidade no trato do conhecimento durante as atividades diárias. Os achados da pesquisa revelam que os ativos de conhecimentos que requerem proteção são citados pela maioria dos respondentes do nível estratégico (88%) e minoria dos respondentes do nível tático-operacional (29%). Este fato corrobora Norman (2001) que aponta os gestores da alta direção como responsáveis pela identificação e proteção das capacidades essenciais da organização.

Os ativos de conhecimento identificados no processo de desenvolvimento de *software* que requerem proteção são apresentados no Quadro 3. A primeira coluna mostra a denominação do ativo de conhecimento, a segunda coluna descreve onde o conhecimento está

registrado ou contido, ou seja, em que meio está explicitado, e a terceira coluna mostra em que fase do processo o conhecimento é criado e utilizado. Destaca-se que o contrato de cliente, documento criado antes da Fase 1 do processo de desenvolvimento de *software*, influencia diretamente o processo, tendo sido citado pela maioria dos respondentes. O uso dos ativos de conhecimento, imbricados no processo de desenvolvimento de *software*, é corroborado por Choo e Alvarenga-Neto (2010) por afirmarem que o conhecimento pode ser criado, compartilhado e utilizado para a consecução dos objetivos organizacionais.

De acordo com norma da empresa, a SG-005 Classificação dos Ativos de Informação do SERPRO já mencionada, os documentos não classificados, isto é, não citados na norma, são passíveis de divulgação para fora da empresa. Dessa maneira, os conhecimentos que compõem os ativos de conhecimento podem configurar uma tipologia para a disseminação e a não disseminação, conforme Choo (2003).

Quadro 3– Ativos de conhecimento que requerem proteção, evidenciados no Estudo de Caso.

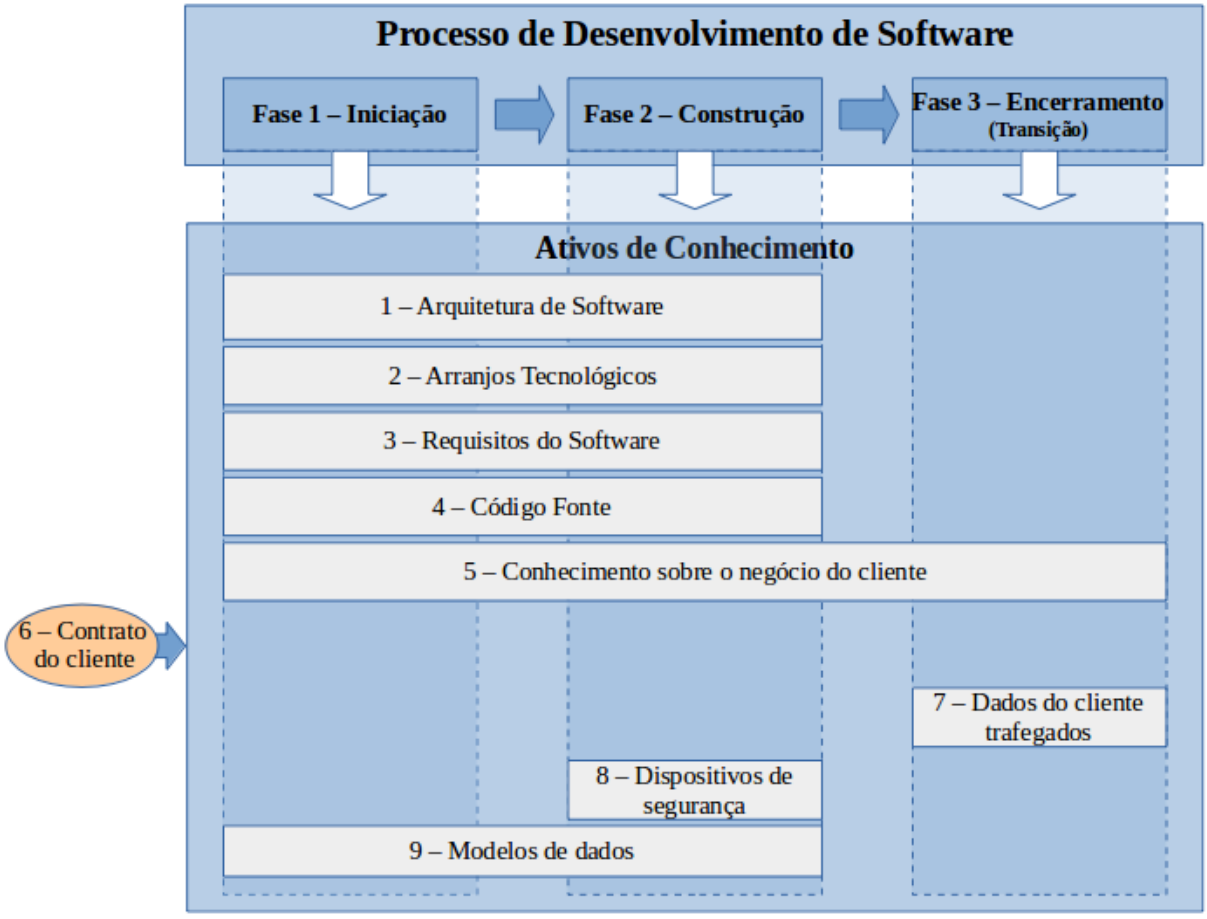
| Ativo de Conhecimento | Descrição | Fases |
|---|---|---|
| Arquitetura do *Software* | Consta no Documento de Arquitetura de *Software*-DAS que estabelece as diretivas para a construção do *software*, por exemplo: sua estrutura em camadas, os padrões de projeto, os componentes, os mecanismos de segurança. | Criado na Fase 1 e utilizado na Fase 2. |
| Arranjos tecnológicos | Consta no documento Configuração de Hardware e *Software*-CHS que estabelece a combinação de hardware e *software*, por exemplos, por meio de bibliotecas, componentes, servidores de aplicação, infraestrutura. | Criado na Fase 1 e utilizado na Fase 2. |
| Requisitos do *software* | Consta em documentação que contém requisitos não funcionais- Fase 1, casos de uso e regras de negócio (requisitos funcionais; envolve algoritmo e criptografia de senha), Documento de Visão-DVS (necessidades e funcionalidades), são atendidos por meio de casos de uso condicionados às regras de negócio. | Criado na Fase 1 e utilizado na Fase 2. |
| Código fonte | É um artefato escrito em linguagem de programação. | Criado e utilizado na Fase 2. |
| Conhecimento sobre o negócio do cliente | Caracterizado na forma tácita e explícita. | Criado e utilizado nas Fases 1,2 e 3. |
| Contrato do cliente | Consta em documentação que contém cláusulas de sigilo, níveis de serviço, periodicidade de guarda, capacidade de recuperação, dentre outros. | Criado antes da Fase 1 e utilizado em todas as fases. |
| Dados do cliente trafegados | Constam no *software* desenvolvido. | Utilizado na Fase 3. |
| Dispositivos de segurança | Constam em documentação do sistema. | Criado e utilizado nas Fases 2 e 3. |
| Modelos de dados | Consta em documentação que descreve como o banco de dados do *software* é organizado quanto aspectos conceitual, lógico e físico. | Criado na Fase 1 e utilizado na 2. |

Fonte: Dados da pesquisa

Todavia, observa-se que, pelo menos 3 ativos de conhecimento identificados neste estudo constam de forma explícita da norma, a saber: regras de negócio, código fonte, dados do cliente. Os entrevistados comentaram que mais clareza dos itens a serem protegidos auxiliaria na condução da gestão do conhecimento quanto ao que compartilhar e o que proteger, de algum modo, por alguma necessidade. Os achados deste Estudo de Caso corroboram Faria e Sofka (2010) que apontam que pouco se sabe sobre as capacidades para proteger o conhecimento valioso para uma empresa, e Little (2011) que argumenta sobre decidir como proteger o capital intelectual identificado.

Ainda que as normas da organização estudada se refiram à informação também se referem ao conhecimento, pois os termos estão associados. Isto porque existe relação entre dados, informação e conhecimento de modo recursivo conforme o seu uso, grau de organização e interpretação (Bhatt, 2001). A Figura 2 mostra os ativos de conhecimento por fases do processo de desenvolvimento de *software*.

Figura 2 – Ativos de conhecimento no processo de desenvolvimento de *software* do Estudo de Caso




Fonte: Dados da pesquisa

Constata-se neste Estudo de Caso que o conhecimento possui natureza complexa. Dimensões objetivas e subjetivas do conhecimento compõem as atividades diárias da equipe que aprende e cria conhecimento por meio de interações contínuas apontadas por Nonaka e Peltokorpi (2006). Também se verifica que o conhecimento a ser protegido pode ser "de baixo valor" ou "de alto valor", "inacessível" ou "acessível", segundo Heisig (2009).

Os resultados obtidos nesta pesquisa são congruentes com a epistemologia conectivista argumentada por Venzin, von Krog, Roos (1998) que apontam que o conhecimento está nas conexões entre os especialistas que desenvolvem conhecimentos específicos e trabalham para solucionar problemas. Também corroboram Kogut e Zander (1992), pois os envolvidos no processo compartilham conhecimento, frequentemente, por meio de mecanismos com tecnologias, com o intuito de explicitar ou codificar conhecimento para o desenvolvimento do *software*. Portanto, observa-se gestão sistemática e explícita das atividades, práticas e políticas relacionadas ao conhecimento na organização (Wiig, 2000).

## 6 CONSIDERAÇÕES FINAIS

Este artigo apresentou os conhecimentos que devem ser protegidos no processo de desenvolvimento de *software*, em uma organização pública de tecnologia da informação (TI), e os ativos de conhecimento. A motivação decorreu das lacunas na literatura contemporânea que indicam a necessidade de novas pesquisas para revelar meios para a inovação relacionada à colaboração, a partir da proteção e compartilhamento de conhecimento, temas inseridos no contexto da gestão do conhecimento.

As principais limitações da pesquisa estão relacionadas às características próprias de Estudo de Caso, destacando-se: ética no que se refere às informações sensíveis envolvidas, pois algumas informações não puderam ser registradas a pedido dos entrevistados considerando normas da empresa; não foram entrevistados todos os membros da equipe do nível tático-operacional, mas o suficiente para conhecer o processo de desenvolvimento, pois na terceira entrevista com empregados (sem função gerencial) foi possível perceber a saturação dos dados, ou seja, repetição das respostas. Para futuras pesquisas recomenda-se analisar vários processos de desenvolvimento de *software*, de determinado cliente, de modo a investigar semelhanças e diferenças para a identificação de padrões considerando a cultura que envolve a relação contratual entre a empresa e o cliente.

## REFERÊNCIAS

Bhatt, G. D. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques, and people. *Journal of Knowledge Management*, 5(1), 68-75. doi: 10.1108/13673270110384419.

Bogers, M. (2011). The open innovation paradox: knowledge sharing and protection in R&D collaborations. *European Journal of Innovation Management,* 14(1), 93-117.

Choo, C. W. (2003). *A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões*. São Paulo: Ed. Senac.

Choo, C. W., & Alvarenga Neto, R.C.D. (2010). Beyond the ba: managing enabling contexts in knowledge organizations. *Journal of Knowledge Management*, 14(4), 592-610. doi 10.1108/13673271011059545.

Desouza, K. C. (2007). *Managing knowledge security: strategies for protecting your companys intellectual assets*. London: Koogan.

Faria, P., & Sofka, W.. (2010). Knowledge protection strategies of multinational firms: a cross-country comparison. *Research Policy,* 39(7), 956–968.

Heisig, P. (2009). Harmonisation of knowledge management: comparing 160 KM frameworks around the globe. *Journal of Knowledge Management*, 13(4), 4-31.

Hurmelinna-Laukkanen, P. (2011). Enabling collaborative innovation: knowledge protection for knowledge sharing. *European Journal of Innovation Management,* 14(3), 303-321.

Ilvonen, I. (2013). Knowledge security – a conceptual analysis. Finland: Tampere.

Kogut, B., & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization Science,* 3(3), 383-397.

Lin, H. F. (2007). A stage model of knowledge management: an empirical investigation of process and effectiveness. *Journal of Information Science,* 33(6), 643-665.

Little, T. A. (2011). Knowledge, intellectual capital, and protection: a literature review. *Proceedings Hawaii International Conference on System Sciences, 44th,* (p. 1-7). Hawaii: University of Hawai.

Liu, Z., & Wang. H. (2011). Analysis on factors influencing the knowledge sharing of employee of software enterprises: a case study of shandong, China. *International Journal on Advances in Information Sciences and Service Sciences*, 3(4), 110-116.

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of Management Review,* 23(2), 242-266.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organizational Science, 5(1),* 14–37.

Nonaka, I., & Takeuchi, H. (1997). *Criação de Conhecimento na Empresa*. Campus, Rio de Janeiro.

Nonaka, I., & Peltokorpi, V. (2006). Objectivity and subjectivy in knowledge: a review of 20 top articles. *Knowledge and Process Management,* 13(2), 73-82.

Norman, P. M. (2001). Are your secrets safe? knowledge protection in strategic alliances. *Business Horizons,* 44(6), 51-60.

Olander, H., Hurmelinna-Laukkanen, P., & Mahonen, J. (2009). What's small size got to do with it? protection on intellectual assests in SMEs. *International Journal of Innovation Management,* 13(3), 349-370.

SERPRO. Serviço Federal de Processamento de Dados. Recuperado em: 07 março 2013 de https://www. serpro.gov.br/conteudo-oserpro/estrutura.

Sommerville, I. (2007). *Software engineering*. 8th ed. São Paulo: Pearson Addison-Wesley.

Venzin, M., Von Krog, G., & Roos, J. (1998). Future research knowledge management. In: Von Krog, G., Roos, & J., Kleine, D. (Org.), *Knowing in firms: understanding, managing and measuring knowledge* (pp. 26-66). Califórnia: SAGE.

Wiig, K. M. (2000). Application of knowledge management in public administration: paper prepared for public administrators of the City of Taipei. Arlington: Knowledge Research Institute. Recuperado em: 15 maio 2012 de http://www.krii.com/downloads/km_in_public_admin_rev.pdf.

Yin, R. K. (2010). *Estudo de caso: Planejamento e Métodos*. 4ª ed. Porto Alegre: Bookman.