



ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA  
DIVISÃO DE ENSINO  
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

FELIPE **ANDRÉ ALVES** DE PADUA, Cap Av

**Aplicação da Segurança da Informação na alavancagem da Gestão do  
Conhecimento**

Rio de Janeiro  
2024

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA  
DIVISÃO DE ENSINO  
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

FELIPE **ANDRÉ ALVES** DE PADUA, Cap Av

**Aplicação da Segurança da Informação na alavancagem da Gestão do  
Conhecimento**

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação Lato Sensu em Liderança com Ênfase em Gestão no COMAER.

Linha de Pesquisa: Ciência, Tecnologia e Inovação

Orientadora: Robertha Lima da Silva Matias,  
Cap Av

Rio de Janeiro  
2024

FELIPE **ANDRÉ ALVES** DE PADUA, Cap Av

**Aplicação da Segurança da Informação na alavancagem da Gestão do  
Conhecimento**

Trabalho de conclusão de curso apresentado  
no Curso de Aperfeiçoamento de Oficiais da  
Aeronáutica.

Aprovado por:

---

Edvaldo Pires de **Figueiredo**, Ten Cel Esp Sup Tec  
EAOAR

---

**Robertha** Lima da Silva Matias, Cap Av  
EAOAR

Rio de Janeiro  
2024

## RESUMO

A atividade de Gestão do Conhecimento no âmbito dos projetos de Pesquisa e Desenvolvimento em prol da aquisição e manutenção de capacidades militares da FAB tem enfrentado vários desafios. Dentre esses desafios está a perda de conhecimentos decorrente da rotatividade dos militares e baixa dos civis envolvidos em tais projetos. Visando reduzir essa perda de conhecimentos e a correspondente degradação das capacidades adquiridas, este trabalho defende a utilização das ferramentas de Segurança da Informação em prol da Gestão do Conhecimento, tese esta que se apoia em dois pilares. O primeiro pilar é a existência de uma relação entre as políticas de Segurança da Informação de uma instituição, sua cultura organizacional, e as práticas de Gestão do Conhecimento, em um processo que se retroalimenta. O segundo pilar consiste na promoção da formalização dos conhecimentos tácitos promovida por políticas de SI em organizações altamente sensíveis à informação, favorecendo a perpetuação dos conhecimentos por meio da externalização. Da argumentação apresentada, conclui-se que diversas ferramentas em uso na Segurança da Informação no âmbito do COMAER podem ser também aplicadas visando potencializar os processos de Gestão do Conhecimento no ramo de Ciência, Tecnologia e Inovação em prol da obtenção e manutenção de capacidades militares da FAB, podendo levar a maior efetividade na consecução dos objetivos institucionais.

**Palavras-chave:** Gestão do Conhecimento. Segurança da Informação. Cultura Organizacional. Disponibilidade da Informação. Pesquisa e Desenvolvimento.

## **1 A GESTÃO DO CONHECIMENTO NO COMAER**

Diante do atual cenário de rápido desenvolvimento tecnológico, a informação e o conhecimento estão entre os principais ativos de qualquer instituição. A adequada exploração desses ativos constitui um diferencial competitivo, e a própria sobrevivência de uma companhia pode estar atrelada ao seu bom uso. Nesse contexto, surge a necessidade de se buscar uma efetiva Gestão do Conhecimento (GC). Esta é definida por Gold, Malhotra e Segars (2001) como o processo adquirir, converter, utilizar e proteger os conhecimentos de uma instituição. No âmbito do COMAER, cabe ao DCTA efetuar a GC nas atividades que envolvam a inovação tecnológica voltada à obtenção de novas capacidades da FAB, bem como à manutenção das capacidades existentes.

Dentre os desafios que se apresentam à Gestão do Conhecimento no COMAER, encontram-se a alta rotatividade do pessoal militar envolvido nos projetos, a baixa gradativa dos servidores civis sem perspectiva de reposição, a falta de práticas de transição nas substituições de pessoal e outros. Por vezes, situações como essas têm levado à perda de conhecimentos acumulados na atividade de Pesquisa e Desenvolvimento (P&D), seja durante a condução dos projetos ou mesmo após sua conclusão. Esta perda se traduz na redução das capacidades militares da Força.

Como forma de evitar a perda de conhecimentos e consequente redução das capacidades da FAB, este trabalho defende a utilização de ferramentas da Segurança da Informação (SI) em prol da Gestão do Conhecimento no âmbito do DCTA. Esta tese se apoia em dois pilares. O primeiro deles é o fato de que as atividades de Gestão do Conhecimento e a Segurança da Informação possuem forte ligação com a cultura organizacional, sendo influenciados por ela ao mesmo tempo em que a moldam. O segundo pilar reside na promoção da externalização dos conhecimentos tácitos promovida pela SI, a qual permite um maior controle sobre os dados, informações e conhecimentos produzidos.

## **2 A GESTÃO DO CONHECIMENTO E A SEGURANÇA DA INFORMAÇÃO**

A Segurança da Informação, conforme entendida no COMAER (2022b), é constituída de uma gama de medidas que visam assegurar a confidencialidade, a integridade, a disponibilidade, a irretratabilidade e a autenticidade das informações. Conforme exposto por Lundgren e Möller (2019), o conjunto formado pelas três primeiras características,

conhecido como tríade da CIA, é utilizado em todo o mundo. Embora os autores argumentem que essa caracterização careça do rigor necessário para ser considerada uma definição, ela tem balizado normas, leis e padronizações em diversos países, tanto por entes governamentais quanto não-governamentais, pelo que consideramos adequado seguir o entendimento vigente.

Para prover a SI nas Organizações Militares da FAB, diversas ferramentas, técnicas e processos são estabelecidos nos dispositivos normativos internos. Procura-se, neste trabalho, mostrar que várias dessas ferramentas, técnicas e processos podem ser utilizadas em prol da GC nas Instituições de Ciência, Tecnologia e Inovação (ICT) do COMAER, visando a preservação do conhecimentos adquiridos nos diversos projetos de P&D em benefício da obtenção e da manutenção das capacidades operacionais da Força.

## 2.1 A cultura organizacional como potencializadora da SI e da GC

Conforme levantado por Ma, Johnston e Pearson (2008), a importância relativa dos objetivos e práticas da gestão da SI variam de acordo com o nível de sensibilidade das informações de uma organização. Os resultados apresentados demonstram que organizações com média sensibilidade tendem enxergar como objetivo mais relevante a confidencialidade, e como prática mais relevante o controle de acesso. Já as organizações altamente sensíveis tendem a dar grande importância também aos objetivos de responsabilidade e integridade e às práticas de segurança organizacional e política de segurança.

Nessa toada, Tryfonas, Gritzalis e Kokolakis (2000) demonstram que, embora existam alguns *trade-offs* entre os parâmetros da SI, certos contextos críticos requerem um alto nível de exigência sobre todos os parâmetros. Certamente, a criticidade da atividade de determinada organização impacta sua cultura. Esta pode ser entendida como um conjunto de valores, crenças, costumes, normas e outros assuntos compartilhados entre seus membros. Este compartilhamento pode se dar de forma tácita ou expressa, e gera um padrão nas formas de pensar e agir dos indivíduos.

À parte da imensurável variabilidade das culturas em diferentes organizações, Cameron e Quinn (2011 apud Karlsson *et al.*, 2022) baseiam-se numa classificação em duas dimensões para agrupar as diversas culturas organizacionais em quatro quadrantes. Valendo-se dessa classificação, Karlsson *et al.* (2022) apontam que culturas com maior

foco interno apresentam maior conformidade com as políticas de Segurança da Informação.

Os tipos de cultura organizacional com foco predominantemente interno são a cultura de hierarquia e a cultura de clã, nas quais se enquadram a maioria das Organizações Militares da FAB. A predominância do foco interno nas OMs da FAB pode ser relacionado à criticidade de suas atividades, as quais impactam diretamente a Segurança Nacional. Por outro lado, ao mesmo tempo em que a cultura vigente favorece à observância da Segurança da Informação por parte de seus membros, as ferramentas de SI podem ser usadas para moldar essa mesma cultura, num ciclo que se retroalimenta.

Tendo isso em mente, uma ferramenta bastante eficaz para se moldar uma cultura são os programas educacionais. Nesse sentido, nota-se que o COMAER (2013) estabelece um programa de educação continuada em inteligência, o qual aborda assuntos como a mentalidade de segurança, a prevenção à engenharia social, a segurança em comunicações, entre outros. Tal programa deve ser ministrado em todas as OM, sendo voltado para todo o efetivo. Semelhantemente, Gold, Malhotra e Segars (2001) argumentam que a efetividade da Gestão do Conhecimento depende de aspectos técnicos, estruturais e culturais. Sobre este último grupo, alegam que nele podem se encontrar os maiores obstáculos a uma GC efetiva, de modo que a habilidade da organização em moldar sua cultura é fundamental para viabilizar este objetivo, pois a transmissão do conhecimento se dá primariamente na interação entre seus membros.

Considerando esse aspecto, podemos notar uma relação positiva entre a cultura organizacional na FAB, a Segurança da Informação e a Gestão do Conhecimento. Esta relação pode ser bem explorada no âmbito das ICT do COMAER, sob a coordenação do DCTA, visando a promoção de interações entre o pessoal envolvido nos diferentes projetos, de modo a se preservar e difundir os conhecimentos essenciais à obtenção e manutenção das capacidades militares da FAB, prevenindo a degradação destas capacidades pela perda daqueles conhecimentos.

## **2.2 A externalização do conhecimento e a disponibilidade da informação**

Frequentemente, a perda de informações e conhecimentos de uma organização leva a diversos tipos de prejuízo (Jouini; Rabai; Aissa, 2014). Esses prejuízos podem incluir o retrabalho, a perda de oportunidades, a interrupção de projetos e até mesmo decisões equivocadas. Não por acaso, informações são consideradas um importante ativo

a ser protegido nas corporações (Buogo; Fachinelli; Giacomello, 2019).

No caso das Instituições de Ciência, Tecnologia e Inovação (ICT) do COMAER, uma fonte de risco de perda de conhecimentos é a saída do pessoal envolvido nos diversos projetos de P&D relacionados ao Poder Aeroespacial. Essa saída se dá por conta da alta rotatividade do pessoal militar e da baixa gradativa dos servidores civis sem perspectiva de reposição. Boa parte do conhecimento gerado durante o desenrolar dos projetos é acumulado de forma tácita, ou seja, fica restrito à mente e à memória do pessoal envolvido.

Visando mitigar o risco de perda desses conhecimentos, é importante garantir que eles sejam transmitidos. Segundo a teoria da espiral do conhecimento, proposta por Nonaka e Takeuchi (2008 apud Buogo; Fachinelli; Giacomello, 2019), essa transmissão, ou conversão, pode se dar de quatro formas: socialização, externalização, combinação e internalização. Dessas, a externalização consiste na conversão do conhecimento tácito em conhecimento explícito. Em outras palavras, é o processo em que o conhecimento existente na memória de uma ou mais pessoas é transmitido para meios externos à mente, como mídias físicas ou sistemas digitais, e organizado de forma a se tornar acessível a outros usuários sem a necessidade de interação direta com seu detentor original.

Nota-se no conceito acima uma estreita relação com o conceito de disponibilidade da informação. Esta, segundo Schou (1996 apud Martin; Khazanchi, 2006), consiste no acesso oportuno e confiável por usuários autorizados. Trazendo este conceito para o contexto da FAB, busca-se a “garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário”(COMAER, 2009), ou a “qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados”(COMAER, 2022a). Conforme apresentado por Martin e Khazanchi (2006), para que uma determinada informação atenda aos requisitos de disponibilidade, é necessário que ela atenda a critérios de confiabilidade, acessibilidade e oportunidade. Certamente, tais critérios não podem ser atendidos caso a informação exista apenas na mente humana, de modo que os autores defendem que fatores como políticas de segurança, redundância, *backups* e segurança física são determinantes para a garantia da disponibilidade da informação. Assim, depreende-se que a promoção da SI pressupõe a formalização, ou externalização, de toda informação que se deseja proteger.

Desta relação entre conceitos, depreende-se que a GC e a SI podem ser pensadas em conjunto. De fato, Eslamkhah e Seno (2019) identificam diversas ferramentas e técnicas

pertencentes ao campo da GC que possuem altíssimo grau de importância na elevação da SI em uma organização. Analisando a política de SI do COMAER (2022b), é possível trilhar o caminho contrário e identificar uma gama de processos afetos à Segurança da Informação que podem ser utilizados em prol da Gestão do Conhecimento visando evitar a perda de conhecimentos decorrente da saída de pessoal afeto à P&D. Dentre esses processos podemos citar o mapeamento de ativos de informação, a gestão da continuidade e a gestão de risco. Estes processos favorecem a formalização, ou externalização, dos conhecimentos tácitos, mediante sua documentação, organização e gestão.

### **3 IMPLICAÇÕES PARA O COMAER**

No contexto hodierno de desenvolvimento tecnológico acelerado, a informação e o conhecimento constituem ativos cuja adequada exploração proporciona um diferencial competitivo às organizações podendo, inclusive, ser determinante para sua sobrevivência. Neste cenário, faz-se necessário buscar uma efetiva Gestão do Conhecimento. Esta consiste no processo adquirir, converter, utilizar e proteger os conhecimentos de uma instituição. No âmbito do COMAER, cabe ao DCTA efetuar a Gestão do Conhecimento nas atividades que envolvam a inovação tecnológica voltada à obtenção e manutenção das capacidades da FAB.

Dentre os desafios que se apresentam à GC no COMAER, encontram-se a rotatividade do pessoal militar, a baixa dos servidores civis, a falta de transição nas substituições de pessoal e outros. Tais situações têm levado, por vezes, à perda de conhecimentos acumulados na atividade de Pesquisa e Desenvolvimento. Esta perda se traduz na redução das capacidades militares da Força. Como forma de evitar a perda de conhecimentos importantes para a manutenção das capacidades da FAB, bem como para a obtenção de novas capacidades, este trabalho defendeu a utilização de ferramentas da Segurança da Informação (SI) em prol da Gestão do Conhecimento no âmbito do DCTA.

Esta tese se apoia, primeiramente, no fato de que a Gestão do Conhecimento e a Segurança da Informação possuem forte ligação com a cultura organizacional, sendo influenciados por ela ao mesmo tempo em que a moldam. O nível de criticidade das atividades de uma corporação, a sensibilidade de suas informações e o foco da instituição (interno ou externo) exercem forte impacto sobre a forma de os indivíduos pensarem e agirem. Ao mesmo tempo, a efetividade da GC depende de aspectos técnicos estruturais e

culturais, e ferramentas como o programa de educação continuada adotado no COMAER podem ser aplicadas para moldar a cultura e potencializar a transmissão dos conhecimentos entre seus membros.

Como segundo apoio à tese apresentada, viu-se que as atividades e políticas voltadas à Segurança da Informação, em especial aquelas voltadas à garantir sua Disponibilidade, pressupõem o registro das informações em meios que possibilitem a acessibilidade, confiabilidade e oportunidade. Tal registro corresponde à fase de externalização apresentada na teoria da Espiral do Conhecimento, de maneira que ferramentas já adotadas na FAB podem ser direcionadas a aumentar a efetividade da GC por meio da formalização dos conhecimentos tácitos existentes na mente de seus pesquisadores.

Embora o foco deste trabalho esteja voltado para os conhecimentos gerados na atividade de Pesquisa e Desenvolvimento, uma vez que as medidas aqui defendidas sejam implementadas nas ICT do COMAER, diversos benefícios devem ser percebidos em outras áreas. Notavelmente, o fomento de uma cultura de compartilhamento de conhecimentos tende a gerar no efetivo uma maior compreensão dos processos de sua OM e da interdependência desses processos, levando a maior integração e cooperação entre os diferentes setores. Esta cooperação deve levar a maior eficiência administrativa, economia de recursos e otimização do tempo em diversas atividades.

Além disso, outro benefício secundário que deve ser observado é uma maior efetividade no assessoramento ao Comandante, decorrente da elevação da disponibilidade das informações e da maior externalização dos conhecimentos. Isso permitirá que os dados, informações e conhecimentos detidos pela OM sejam prontamente acessados de forma confiável sempre que se fizerem necessários, permitindo sua utilização oportuna no processo decisório, possibilitando tomadas de decisão mais acertadas. Assim, será possível obter uma maior efetividade na consecução dos objetivos institucionais, com aumento nos níveis de prontidão operacional, segurança de voo, eficiência no emprego dos meios, dentre outras áreas que impactam diretamente o cumprimento da missão da FAB.

## REFERÊNCIAS

BUOGO, Mateus; FACHINELLI, Ana Cristina; GIACOMELLO, Cíntia Paese. Gestão do conhecimento e segurança da informação. **Revista AtoZ**, v. 8, n. 2, p. 39–59, 2019.

COMANDO DA AERONÁUTICA. Portaria EMAER nº 5/CEMAER, de 23 de fevereiro de 2022: Aprova a reedição da Doutrina de Inteligência da Aeronáutica. **Boletim do Comando da Aeronáutica**, n. 41, 2022.

COMANDO DA AERONÁUTICA. Portaria GABAER nº 273/GC-3, de 18 de abril de 2022: Aprova a Diretriz que estabelece a Política de Segurança da Informação do Comando da Aeronáutica. **Boletim do Comando da Aeronáutica**, n. 74, 2022.

COMANDO DA AERONÁUTICA. Portaria nº 15/CIAER, de 15 de agosto de 2013: Aprova a reedição da Instrução que dispõe sobre Programa Básico de Trabalho Anual e Educação Continuada dos Elos do SINTAER. **Boletim do Comando da Aeronáutica**, n. 154, 2013.

COMANDO DA AERONÁUTICA. Portaria nº 3/CIAER, de 19 de dezembro de 2008: Aprova a edição do Folheto que dispõe sobre Mentalidade de Segurança. **Boletim do Comando da Aeronáutica**, n. 13, 2009.

ESLAMKHAH, Mahdi; SENO, Seyed Amin Hosseini. Identifying and ranking knowledge management tools and techniques affecting organizational information security improvement. **Knowledge Management Research & Practice**, Taylor & Francis, 2019.

GOLD, Andrew; MALHOTRA, Arvind; SEGARS, Albert. Knowledge management: An organizational capabilities perspective. **Journal of management information systems**, Taylor & Francis, v. 18, n. 1, p. 185–214, 2001.

JOUINI, Mouna; RABAI, Latifa Ben Arfa; AISSA, Anis Ben. Classification of security threats in information systems. **Procedia Computer Science**, Elsevier, v. 32, p. 489–496, 2014.

KARLSSON, Martin *et al.* The effect of perceived organizational culture on employees' information security compliance. **Information & Computer Security**, Emerald Publishing Limited, v. 30, n. 3, p. 382–401, 2022.

LUNDGREN, Björn; MÖLLER, Niklas. Defining information security. **Science and engineering ethics**, Springer, v. 25, p. 419–441, 2019.

MA, Qingxiong; JOHNSTON, Allen; PEARSON, John Michael. Information security management objectives and practices: a parsimonious framework. **Information Management & Computer Security**, Emerald Group Publishing Limited, v. 16, n. 3, p. 251–270, 2008.

MARTIN, Andrew; KHAZANCHI, Deepak. Information availability and security policy. **12th Americas Conference on Information Systems, AMCIS 2006**, p. 1247–1258, 2006.

TRYFONAS, Theodore; GRITZALIS, Dimitris; KOKOLAKIS, Spyros. A Qualitative Approach to Information Availability. **Information Security for Global Information Infrastructures: IFIP TC11 Sixteenth Annual Working Conference on Information Security**, p. 37–47, 2000.