ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

DIVISÃO DE ENSINO

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

ARTHUR SOUZA RODRIGUES DA COSTA, Cap Av

Estratégias e Soluções de Prevenção de Perda de Dados Sensíveis do COMAER

Rio de Janeiro

2024

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

ARTHUR SOUZA RODRIGUES DA COSTA, Cap Av

Estratégias e Soluções de Prevenção de Perda de Dados Sensíveis do COMAER

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: Guerra Cibernética
Orientador: Márcio Henrique Teixeira de Souza, Ten Cel Av

Rio de Janeiro
2024

ARTHUR SOUZA RODRIGUES DA COSTA, Cap Av

Estratégias e Soluções de Prevenção de Perda de Dados Sensíveis do COMAER

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

Aprovado por:

_____

Márcio Henrique **Teixeira** de Souza, Ten Cel Av
EAOAR

_____

Alexandra Vidal Pedinotti Zuma, Maj Farm
EAOAR

Rio de Janeiro

2024

RESUMO

No cenário contemporâneo de avanços tecnológicos e crescente digitalização, o Comando da Aeronáutica (COMAER) enfrenta desafios na proteção de uma vasta quantidade de dados críticos e pessoais. A perda ou comprometimento desses dados não só ameaça a soberania nacional, como também expõe informações sensíveis de militares, servidores e dependentes, evidenciando a necessidade imperativa de robustecer a segurança cibernética. Este ensaio defende a tese de que o COMAER deve adotar políticas de Prevenção de Perda de Dados, do inglês *Data Loss Prevention* (DLP), com o objetivo de assegurar a integridade, confidencialidade e disponibilidade dos dados. Argumenta-se que a implantação de medidas de DLP facilita a conformidade com normativas legais vigentes, como a Lei Geral de Proteção de Dados (LGPD), e aumenta a capacidade de controle de informações críticas sob gestão do COMAER, como solução de segurança cibernética focada no dado, prevenindo vazamentos e espionagem. A DLP emerge como solução estratégica, não apenas para cumprimento de regulamentações, mas como medida proativa e inovadora para proteger as operações militares e científicas contra a ameaça de ciberataques e engenharia social. Dessa maneira, a capacidade de proteger informações sensíveis mediante políticas de DLP reforça a posição estratégica do Brasil, promove a confiança pública e sublinha o compromisso do COMAER com a proteção da privacidade e direitos individuais, objetivo comum de todos os entes públicos.

Palavras-chave: Prevenção de Perda de Dados. Segurança cibernética. LGPD. Soberania Nacional.

1 **INTRODUÇÃO**

No contexto atual de acelerada inovação tecnológica e expansão da conectividade, um volume significativo de dados circula e é operado nos sistemas, servidores e redes do Comando da Aeronáutica diariamente. Estes dados, acumulados e aprimorados ao longo de décadas de atividades operacionais e pesquisa científica, representam um ativo estratégico fundamental, destacando a necessidade crítica de sua gestão eficaz e proteção.

Pertencem, também, à Força Aérea Brasileira (FAB) informações cruciais que versam sobre o funcionamento de sistemas de defesa e de controle do espaço aéreo. Tais dados são vitais para a soberania nacional, cujo comprometimento poderia resultar em desvantagens militares, científicas e econômicas significativas, além de impactar os usuários das infraestruturas críticas gerenciadas pela Aeronáutica.

Além dos dados críticos, cabe ao COMAER a custódia de informações pessoais afetas à Administração do Pessoal e à Saúde. Tais informações despertam interesses de pessoas mal-intencionadas que desejem fazer uso delas para Engenharia Social ou com intenções financeiras. O vazamento desses dados tem potencial de expor militares, servidores e pensionistas sob a administração da FAB, bem como seus dependentes.

Por isso, à medida que as tecnologias avançam, torna-se imperativo implantar protocolos inovadores de proteção, visando robustecer a segurança. Deve-se adotar práticas e estratégias que garantam a integridade, a confidencialidade e o controle de acesso a esses dados sensíveis. Dentre essas soluções se destacam as compreendidas nas estratégias de Prevenção de Perda de Dados.

Segundo Ghorbanian, Fryklund e Axelsson (2015), a adoção de sistemas DLP permite o monitoramento, detecção e prevenção automática da transferência não autorizada ou do vazamento de informações críticas, tanto em repouso, quanto em trânsito ou em uso. Portanto, esse ensaio defende a tese de que o COMAER deve adotar políticas de Prevenção de Perda de Dados.

Para a sustentação dessa tese, esse ensaio argumenta que a implantação de medidas de DLP colaborará com a adequação do COMAER às leis e normas vigentes, tais como a LGPD, por exemplo.

Além disso, este trabalho também destaca que o uso da DLP aumenta a capacidade de controle de informações críticas de propriedade do COMAER, sendo uma solução de segurança cibernética focada no dado.

Reconhecida a necessidade de adotar estratégias e soluções de Prevenção de Perda de Dados, é essencial compreender como tais tecnologias funcionam e os desafios a superar.

2 **DESENVOLVIMENTO**

Conforme Takebayashi *et al.* (2010), as tecnologias que englobam a DLP possuem uma abordagem focada na informação, ou seja, diferem-se de soluções de segurança convencionais, como antivírus e *firewalls,* que se concentram na proteção de computadores, celulares e servidores contra *malwares* e ataques cibernéticos.

Para isso, Tahboub e Saleh (2014) descrevem que as soluções de DLP atuam identificando conteúdos sensíveis, monitorando seu armazenamento e manipulação por meio da classificação do seu estado: em repouso (*Data-at-Rest*), em uso (*Data-in-Use*) ou em trânsito (*Data-in-Motion*), prevenindo sua exposição fora da Instituição.

Os dados em repouso são aqueles armazenados em dispositivos, computadores e servidores. Medidas DLP são capazes de identificar os conteúdos dos arquivos, classificá-los conforme o fator de risco e ponderar seu correto armazenamento.

Dados em uso são aqueles que estão sendo manipulados pelos usuários ou interagidos de alguma forma. Na política de prevenção de perda de dados, o potencial de vazamento é controlado por meio da identificação e autorização de operações de copiar-colar, impressão ou de captura de tela envolvendo dados identificados como sensíveis.

Dados em movimento dizem respeito aos dados que estão sendo tramitados via uma rede. A DLP atua na detecção de operações envolvendo dados críticos sendo transportados por meio desses canais, identificando e comparando o conteúdo da informação com o protocolo sendo utilizado, evitando por exemplo que um arquivo restrito seja carregado para um site de conversão de arquivos em formato *Portable Document Format* (PDF).

Assim posto, devido à natureza complexa e ao volume dos dados manejados pelo COMAER, deve-se reconhecer que existem uma variedade de possibilidade de

vazamentos, ou ainda, falhas de monitoramento relacionadas a informações pessoais e dados críticos, tornando a FAB alvo atrativo para uma variedade de ameaças cibernéticas, que vão desde vazamentos não intencionais, ataques de engenharia social ou até ações sofisticadas de espionagem cibernética.

2.1 **Uso de DLP como Ferramenta de Adequação Normativa**

A LGPD, promulgada em 2018, abrange o tratamento de dados pessoais, por pessoa jurídica de direito público, com o objetivo de proteger, entre outros direitos fundamentais, o da privacidade. Em seu II inciso do 5º Artigo está definido que dado pessoal sensível, entre outras categorias, é todo aquele sobre origem racial ou étnica, convicção religiosa, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

A LGPD ainda estabelece boas práticas de governança para Administração Pública Federal (APF). No 1º parágrafo do Artigo 50 a lei diz que:

> Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular (Brasil, 2018).

Analisando o atual panorama cibernético do COMAER, identifica-se como ativo importante as informações sensíveis afetas às pessoas que estejam sob controle da administração, sejam elas militares, servidoras civis, pensionistas ou dependentes.

Em 2016, o jornal australiano ABC News reportou um grave incidente de violação de segurança de dados envolvendo o vazamento de informações sensíveis de doadores de sangue. Os dados expostos incluíam informações pessoais detalhadas além dos resultados de um questionário que avaliava se o doador seria “pessoa com comportamento sexual de risco”. Esse vazamento, segundo nota de retratação da Lifeblood, empresa envolvida no ocorrido, foi devido à transferência de um arquivo contendo dados pessoais para um ambiente computacional inseguro, tornando-o acessível a indivíduos não autorizados.

O caso demonstra as graves consequências geradas pela exposição de dados privados e destaca a importância da adoção de medidas de segurança robustas no tratamento de dados sensíveis. Soluções de DLP impediriam a movimentação desses arquivos e reportariam o incidente aos operadores do sistema, evitando

consequências legais para a instituição envolvida. Adicionalmente, medidas educativas e preventivas seriam tomadas para reforçar a Segurança Orgânica.

Erridge, em entrevista concedida a Mansfield-Devine (2016), destaca a importância dos dados preservados por lei, como os descritos na *General Data Protection Regulation* (GDPR), regulamento europeu que inspirou a LGPD, considerando-os um ativo crítico, que deve ser adequadamente protegido, com o uso de estratégias DLP.

Reforçando o argumento, a Diretriz do Comando da Aeronáutica (DCA) 16-3, (2018), Plano de Integridade da Força Aérea Brasileira, classifica o uso indevido e o vazamento de informações sigilosas como “quebra de integridade”. Destaca-se, de forma geral, a importância do respeito às legislações vigentes e a proteção de ativos para prevenir prejuízos e danos, por meio de uma eficiente gestão de riscos, que inclui enfrentar riscos legais e operacionais. Como medidas preventivas desses riscos, as estratégias de DLP podem atuar como práticas de controle com resultados evidentes, se classificando no mais alto nível de efetividade de operação de segurança segundo a diretriz.

Dessa forma, qualquer dado sob custódia da Administração que venha a ser divulgado pode trazer insegurança jurídica e riscos à integridade, portanto, reforça-se a tese de que o COMAER deve adotar políticas de Prevenção de Perda de Dados fortalecendo a capacidade de cumprir normas e leis.

2.2 **Uso de DLP para Prevenção dos Riscos de Segurança**

Os conhecimentos doutrinários e tecnológicos produzidos pelo COMAER, mediante a consolidação de anos de pesquisa, desenvolvimento e experiência operacional, constituem um valioso patrimônio intelectual que sustenta as operações da FAB e servem de arcabouço para a indústria de defesa do país. Estes conhecimentos são ativos cruciais que necessitam da proteção das medidas de DLP.

Para Mazzoni (2014), a informação é o bem mais valioso para a administração Pública Federal, sendo que o vazamento de dados sigilosos pode acarretar prejuízos financeiros, danificar a reputação de instituições, expor informações pessoais, revelar dados estratégicos de empresas e comprometer a segurança e a defesa nacional.

A exposição não autorizada de dados críticos não apenas prejudica a vantagem estratégica que tais informações proporcionam, mas também compromete

alianças e a segurança das operações militares. O acesso indevido por entidades ou nações adversárias pode acelerar o desenvolvimento de contramedidas, diminuir a eficácia operacional da FAB e, em última análise, ameaçar a segurança nacional.

Os riscos associados não se limitam apenas às consequências estratégicas ou operacionais, mas estendem-se significativamente no quesito econômico quando envolvem segredos industriais. Conforme Morgan (2022b), o cibercrime tornou-se altamente organizado, incluindo entre muitas outras atividades, as de produzirem danos e destruição de dado, assim como roubo de propriedade intelectual, dados pessoais e financeiros. Segundo Morgan (2022a), o custo global do cibercrime previsto para 2023 foi de US$ 8 trilhões, marcando um aumento de 33% em relação ao ano de 2021. Além disso, a previsão de Morgan é de que os impactos financeiros cresçam cerca de 15% ao ano até 2025, evidenciando a ameaça crescente que o cibercrime impõe para a economia global.

Igualmente importante é a proteção dos dados relacionados à infraestrutura crítica, como aqueles associados aos sistemas de Controle do Espaço Aéreo, dado que o vazamento dessas informações pode introduzir vulnerabilidades com implicações diretas na segurança de voo e na soberania do espaço aéreo.

O aumento do número de dispositivos conectados às redes, a proliferação das redes sociais e ferramentas online cria potenciais pontos de vazamentos de informações, já que “até colaboradores leais estão suscetíveis a cometerem erros” (Lesnykh, 2011, p.18, tradução nossa).

Neste cenário, políticas de DLP são vitais para garantir que tais transferências de dados sejam realizadas de maneira segura. As soluções DLP podem, por exemplo, identificar esses dados sensíveis em movimento, automaticamente criptografá-los no momento do seu *upload,* verificar a segurança do canal de comunicação, ou até mesmo bloquear a transferência caso o destinatário não esteja previamente autorizado a receber tal informação.

Pelo argumento apresentado, reforça-se a tese de que o COMAER deve adotar políticas de Prevenção de Perda de Dados. É importante destacar que tais estratégias devem ser acompanhadas da busca por uma cultura organizacional que valorize a segurança da informação, envolvendo a conscientização de todos os membros da FAB. A adoção das medidas DLP é uma clara evidência da preocupação da Aeronáutica para com a segurança orgânica e por isso pode motivar seu efetivo a adotar condutas mais disciplinadas.

3. **CONCLUSÃO**

A era digital impõe desafios, especialmente no contexto militar e de defesa. As informações geridas pelo COMAER requerem medidas de proteção avançadas para defendê-las tanto de ataques cibernéticos como de vulnerabilidades sistêmicas. A perda da integridade e do controle dos dados tem consequências que podem ser devastadoras tanto em termos de segurança nacional quanto de privacidade individual e imagem institucional.

Para evitar tais consequências, a DLP funciona como uma estratégia de proteção dos dados críticos em um cenário marcado por ameaças cibernéticas em evolução, que demanda uma vigilância contínua e adaptações tecnológicas proativas. Assim, reitera-se a tese de que o COMAER deve adotar políticas de Prevenção de Perda de Dados.

Conforme apresentado, a implantação de medidas de DLP colaborará com a adequação do COMAER às leis e normas vigentes. Ao monitorar, detectar e prevenir a transferência não autorizada ou vazamento de informações pessoais, a DLP assegura que a governança do COMAER esteja em conformidade com exigências legais como a LGPD e a DCA 16-3.

Além disso, o emprego da DLP aumenta a capacidade de controle de informações críticas de propriedade do COMAER, sendo uma solução de segurança cibernética focada no dado, assegurando-os independente de seu estado: em repouso, em uso ou em trânsito. Esta abordagem resguarda a FAB contra a espionagem, falhas de protocolo e ataques cibernéticos, sendo uma barreira eficaz contra ameaças externas e internas.

Portanto, a eficácia das medidas de DLP em proteger informações sensíveis emerge para reforçar a posição estratégica do Brasil e, também, assegurar a confiança dos cidadãos na capacidade do COMAER de salvaguardar dados de forma correta. Com o avanço da era digital, torna-se imperativo para uma Força Armada que almeja permanecer atualizada, a implantação de soluções robustas e inovadoras. Isso não só assegura a manutenção da segurança e da soberania nacional, mas também reflete o compromisso do COMAER no fortalecimento da confiança pública nas instituições brasileiras. Esse é um objetivo partilhado por todas as esferas e entidades do poder público, sublinhando a importância da proteção da privacidade e dos direitos individuais.

REFERÊNCIAS

ÁVILA, Ricardo *et al*. Use of security logs for data leak detection: a systematic literature review. **Security and Communication Networks**, v. 2021, p. 1-29, 2021. Disponível em: https://www.hindawi.com/journals/scn/2021/6615899/. Acesso em: 15 mar. 2024.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica Portaria EMAER nº 1.868/GC3, de 20 de novembro de 2018. Aprova a edição do Plano de Integridade da Força Aérea Brasileira (DAC 16-3). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 202, 21 nov. 2018. Disponível em: https://www.fab.mil.br/Download/arquivos/prestacaodecontas/DCA_16_3%20_2018_Plano_de_Integridade_da_FAB.pdf. Acesso em 15 mar. 2024.

BRASIL. Gabinete de Segurança Institucional. Portaria da Presidência da República/Conselho de Defesa Nacional/Secretaria Executiva nº 12, de 09 de abril de 2013. Homologa a Norma Complementar 12/IN01/DSIC/GSIPR - Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF); direta e indireta. **Diário Oficial da União**, Brasília, DF. ed. 68, seção 1, p. 6, 09 abr. 2013. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-12IN01DSICGSIPR.pdf. Acesso em: 15 mar. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, DF, n. 157, 15 ago. 2018. Seção 1, p. 1-59. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 mar. 2024.

ERRIDGE, Tim. Data protection: prepare now or risk disaster. Entrevista concedida a Steve Mansfield-Devine. **Computer Fraud & Security**, [s.l.], n. dezembro, p. 5-11, 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S1361372316300987. Acesso em: 07 abr. 2024.

GHORBANIAN, Sara; FRYKLUND, Glenn; AXELSSON, Stefan. **Do data loss prevention systems really work?**. In: Advances in Digital Forensics XI: 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015, Revised Selected Papers 11. Springer International Publishing, 2015. p. 341-357. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-24123-4_20. Acesso em: 15 mar. 2024.

LESNYKH, Alexei. **Data loss prevention: a matter of discipline**. Network Security, v. 2011, n. 3, p. 18, 2011. Disponível em:

https://www.sciencedirect.com/science/article/pii/S1353485811700289?casa_token=-NKkqMMcoh8AAAAA:gllYGxBVWA2gSC11dv4fHfJfeutXwamqTfyP6Z_697ferofJoRXnUGcal_u11MSzRPjfAuvzJ7_Y. Acesso em: 15 mar. 2024.

AUSTRALIAN RED CROSS BLOOD SERVICE. **Blood Service apologises for donor data leak**. Nota à imprensa, 28 out. 2016. Disponível em: https://www.lifeblood.com.au/news-and-stories/media-centre/media-releases/blood-service-apologises-donor-data-leak. Acesso em: 15 mar. 2024.

MAZZONI, Pedro Henrique Morsch. **Prevenção de vazamento de informações na APF:** Os desafios para a redução de riscos de vazamento de informações sensíveis nos órgãos da Administração Pública Federal. 2014. Dissertação (Especialização em Ciência da Computação) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília, 2014.

MORGAN, Steve. Cybercrime to cost the world 8 trillion annually in 2023. **Cybercrime Magazine**, Sausalito, California, 17 out. 2022a. Disponível em: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/. Acesso em: 15 mar. 2024.

MORGAN, Steve. Cybersecurity research: All in one place. **Cybercrime Magazine**, Northport, Nova York, 05 dez. 2022b. Disponível em: https://cybersecurityventures.com/research/. Acesso em: 15 mar. 2024.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Rio de Janeiro, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8697583. Acesso em: 15 mar. 2024.

TAHBOUB, Radwan; SALEH, Yousef. Data leakage/loss prevention systems (DLP). *In*: 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, IEEE. **Anais** […] IEEE, 2014. p. 1-6. Disponível em: https://ieeexplore.ieee.org/document/6916624/. Acesso em: 15 mar. 2024.

TAKEBAYASHI, Tomoyoshi *et al.* Data loss prevention technologies. **Fujitsu Scientific and Technical Journal**, v. 46, n. 1, p. 4, 2010. Disponível em: https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol46-1/paper13.pdf. Acesso em: 07 abr. 2024.

WILLIAMSON, Brett. Red Cross Blood Service admits to data breach. **ABC NEWS**, 28 out. 2016. Disponível em: https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036. Acesso em: 15 mar. 2024.