



**INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA**  
**Área Departamental de Engenharia de Electrónica e**  
**Telecomunicações e de Computadores**

## **Network Air Gap Controller**

**Alexandre de Jesus de Sá Amorim**

Trabalho de Projecto para obtenção do grau de Mestre em Engenharia de Electrónica e Telecomunicações

### **Resumo:**

As ameaças à segurança da informação, (INFOSEC) atentam contra a perda da respectiva confidencialidade, integridade e disponibilidade, pelo que as organizações são impelidas a implementar políticas de segurança, quer ao nível físico quer ao nível lógico, utilizando mecanismos específicos de defesa.

O projecto *Network Air Gap Controller (NAGC)* foi concebido no sentido de contribuir para as questões da segurança, designadamente daquelas que se relacionam directamente com a transferência de informação entre redes de classificação de segurança diferenciadas ou de sensibilidades distintas, sem requisitos de comunicação em tempo real, e que mereçam um maior empenho nas condições de robustez, de disponibilidade e de controlo.

Os organismos que, em razão das atribuições e competências cometidas, necessitam de fazer fluir informação entre este tipo de redes, são por vezes obrigados a realizar a transferência de dados com recurso a um processo manual, efectuado pelo homem e não pela máquina, que envolve dispositivos amovíveis, como sejam o CD, DVD, PEN, discos externos ou *switches* manuais.

Neste processo, vulgarmente designado por *Network Air Gap (NAG)*, o responsável pela transferência de dados deverá assumir de forma infalível, como atribuições intrínsecas e inalienáveis da função exercida, as garantias do cumprimento de um vasto conjunto de normas regulamentares. As regras estabelecidas desdobram-se em ferramentas e procedimentos que se destinam, por exemplo, à guarda em arquivo de todas as transferências efectuadas; à utilização de ferramentas de segurança (ex: antivírus) antes da colocação da informação na rede de classificação mais elevada; ao não consentimento de transferência de determinados tipos de ficheiro (ex: executáveis) e à garantia de que, em consonância com a autonomia que normalmente é delegada no elemento responsável pela operação das comunicações, apenas se efectuam transferências de informação no sentido da rede de classificação inferior para a rede de classificação mais elevada.

Face ao valor da informação e do impacto na imagem deste tipo de organizações, o operador de comunicações que não cumpra escrupulosamente o determinado é inexoravelmente afastado dessas funções, sendo que o processo de apuramento de responsabilidades nem sempre poderá determinar de forma inequívoca se as razões apontam para um acto deliberado ou para factores não intencionais, como a inépcia, o descuido ou a fadiga.

Na realidade, as actividades periódicas e rotineiras, tornam o homem propenso à falha e poderão ser incontornavelmente asseguradas, sem qualquer tipo de constrangimentos ou diminuição de garantias, por soluções tecnológicas, desde que devidamente parametrizadas,

adaptadas, testadas e amadurecidas, libertando os recursos humanos para tarefas de manutenção, gestão, controlo e inspecção.

Acresce que, para este tipo de organizações, onde se multiplicam o número de redes de entrada de informação, com diferentes classificações e actores distintos, e com destinatários específicos, a utilização deste tipo de mecanismos assume uma importância capital. Devido a este factor multiplicativo, impõe-se que o NAGC represente uma opção válida em termos de oferta tecnológica, designadamente para uma gama de produtos de baixíssimo custo e que possa desenvolver-se por camadas de contributo complementar, em função das reais necessidades de cada cenário.

**Palavras-Chave** – “Network air gap”, Informação classificada, Segurança da informação, Confidencialidade, Integridade, Autenticação, Controlo, Inspeção de conteúdos, Eventos de segurança, Notificação remota.

**Dezembro de 2010**